TRABAJOS FIN DE GRADO

Universidad de Jaén

Escuela Politécnica Superior de Jaén

“Implantación de la norma ISO/IEC 27001:2022 de seguridad de la información en una empresa de desarrollo de SaaS con empleados y 100% remoto y servidores en la nube”

Autor: Juan Manuel Galdón Hernández

Grado: Ingeniería Informática

Director: Francisco de Asís Conde Rodríguez
Departamento del director: Departamento de Informática

Fecha: 10/09/2024

Resumen

Este Trabajo de Fin de Grado (TFG) se centra en la implementación y certificación del Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022 en Innovatech Consulting, una empresa ficticia basada en el Instituto de Innovación, Ciencia y Empresa. A lo largo del proyecto, se han desarrollado y documentado exhaustivamente los procesos y metodologías clave necesarios para cumplir con los requisitos de la norma, acotando el alcance a aquellos elementos más directamente relacionados con la titulación de grado en informática.

El trabajo aborda desde la identificación y evaluación de riesgos hasta la elaboración de un Plan de Continuidad de Negocio (BCP) y la definición de una Política de Seguridad de la Información. También se ha llevado a cabo una Declaración de Aplicabilidad (SOA) actualizada a la versión 2022 de la norma, y se han establecido objetivos e indicadores de seguridad para monitorizar y mejorar continuamente el SGSI. Cabe destacar que no se abordan todos los requisitos y recomendaciones de la norma ISO 27001:2022, sino que se acotan a aquellos más relevantes para la formación informática, lo que permite una mayor profundidad en los aspectos técnicos y metodológicos específicos.

Se presentan también los resultados obtenidos de la automatización de controles en Azure, demostrando cómo la integración de tecnologías avanzadas puede optimizar la seguridad de la información en un entorno empresarial dinámico. Finalmente, el TFG propone diversas líneas de trabajo para futuras implementaciones y mejoras, destacando la importancia de la innovación continua en la gestión de la seguridad de la información.

Este TFG no solo ofrece una guía práctica para la implementación de un SGSI, sino que también aporta al campo de la seguridad de la información al explorar nuevas metodologías y herramientas para la mejora continua de la seguridad en las organizaciones.

Abstract

This Final Degree Project (TFG) focuses on the implementation and certification of the Information Security Management System (ISMS) under the ISO 27001:2022 standard at Innovatech Consulting, a fictional company based on the Instituto de Innovación, Ciencia y Empresa. Throughout the project, key processes and methodologies necessary to meet the standard's requirements have been thoroughly developed and documented, limiting the scope to those elements most directly related to the degree in computer science.

The project covers everything from risk identification and assessment to the development of a Business Continuity Plan (BCP) and the definition of an Information Security Policy. An updated Statement of Applicability (SOA) aligned with the 2022 version of the standard has also been conducted, and security objectives and indicators have been established to continuously monitor and improve the ISMS. It is important to note that not all requirements and recommendations of the ISO 27001:2022 standard are addressed; the focus is on those most relevant to the computer science field, allowing for greater depth in specific technical and methodological aspects.

The results of control automation in Azure are also presented, demonstrating how the integration of advanced technologies can optimize information security in a dynamic business environment. Finally, the TFG proposes various lines of work for future implementations and improvements, emphasizing the importance of continuous innovation in information security management.

This TFG not only provides a practical guide for implementing an ISMS but also contributes to the field of information security by exploring new methodologies and tools for the continuous improvement of security in organizations.

Palabras clave:

1. **ISO 27001:2022**: Norma internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), asegurando la confidencialidad, integridad y disponibilidad de la información.
2. **Sistema de Gestión de Seguridad de la Información (SGSI)**: Conjunto de políticas, procedimientos y controles diseñados para gestionar los riesgos de seguridad de la información dentro de una organización.
3. **Innovatech Consulting**: Empresa ficticia utilizada en este TFG para implementar y analizar el SGSI conforme a la norma ISO 27001:2022.
4. **Evaluación de Riesgos**: Proceso de identificación, análisis y evaluación de los riesgos que pueden afectar a la seguridad de la información en una organización.
5. **Declaración de Aplicabilidad (SOA)**: Documento que identifica los controles de seguridad aplicables a una organización, justificando su inclusión o exclusión en función de los riesgos identificados.
6. **Automatización de Controles**: Implementación de controles de seguridad de manera automatizada para mejorar la eficiencia y reducir el riesgo de error humano, en este caso, utilizando Microsoft Azure.
7. **Microsoft Azure**: Plataforma de servicios en la nube de Microsoft, utilizada por Innovatech Consulting para implementar y automatizar controles de seguridad en el SGSI.
8. **Plan de Continuidad de Negocio (BCP)**: Estrategia que describe cómo una organización se preparará y responderá a interrupciones graves de sus operaciones, asegurando la continuidad de los procesos críticos.
9. **Política de Seguridad de la Información**: Documento que define las directrices y principios que rigen la protección de la información dentro de Innovatech Consulting, alineado con la norma ISO 27001:2022.
10. **Gestión de Crisis**: Proceso para identificar, evaluar y responder a situaciones de emergencia que puedan afectar la seguridad de la información y la continuidad del negocio.
11. **Análisis de Impacto en el Negocio (BIA)**: Evaluación de las consecuencias potenciales de interrupciones en los procesos críticos de una organización, con el fin de priorizar las acciones de recuperación.

12. **Controles de Seguridad**: Medidas implementadas para proteger la información y los sistemas de una organización contra amenazas y vulnerabilidades.
13. **Redundancia de Sistemas**: Estrategia de continuidad que implica la duplicación de sistemas críticos para garantizar la disponibilidad en caso de fallo.
14. **Monitorización de Seguridad**: Proceso continuo de supervisión de los sistemas de información para detectar y responder a posibles incidentes de seguridad.
15. **Recuperación ante Desastres (DRP)**: Conjunto de acciones y procedimientos diseñados para restaurar los sistemas de información y operaciones críticas después de un desastre.
16. **NormaPro**: Software o plataforma ficticia mencionada en el TFG para la gestión y automatización de operaciones relacionadas con la seguridad de la información.
17. **Simulacro de Crisis**: Ejercicio práctico realizado para evaluar la eficacia del Plan de Continuidad de Negocio y la respuesta ante crisis de la organización.
18. **Ciclo de Mejora Continua**: Enfoque sistemático para la revisión y mejora constante del SGSI, asegurando que se adapten a los cambios en el entorno operativo y las amenazas emergentes.
19. **Formación en Seguridad de la Información**: Programa de capacitación destinado a mejorar la conciencia y las competencias del personal en relación con la seguridad de la información.
20. **Evaluación Post-Incidencia**: Análisis realizado después de un incidente de seguridad para identificar lecciones aprendidas y mejorar las estrategias de mitigación.

Índice

DOCUMENTO Nº 1: MEMORIA.

Índice de figuras:

Índice de tablas:

DOCUMENTO Nº 1: MEMORIA.

1.INTRODUCCIÓN.

La seguridad de la información en el ámbito SaaS es un desafío multifacético que requiere una estrategia integral y bien estructurada. La implementación de un sistema de gestión de seguridad de la información bajo el marco del estándar internacional ISO 27001 es una respuesta efectiva a estos desafíos, proporcionando a las empresas SaaS las herramientas necesarias para proteger sus activos de información y asegurar la continuidad del negocio en un entorno cada vez más digital y amenazante.

1.1. Contexto de la Seguridad de la Información en empresas SaaS.

Las empresas de Software como Servicio (SaaS) ofrecen soluciones software a través de internet, permitiendo a los usuarios acceder a aplicaciones y servicios sin necesidad de instalarlos localmente en sus dispositivos. Esta modalidad de servicio ha ganado popularidad debido a su flexibilidad, escalabilidad y reducción de costos para los usuarios. Sin embargo, con estas ventajas también surgen desafíos significativos, especialmente en lo que respecta a la seguridad de la información.

Las empresas SaaS manejan volúmenes considerables de datos, a menudo de naturaleza sensible, pertenecientes a sus clientes. Esto incluye datos personales, financieros y operativos que, de no ser gestionados adecuadamente, pueden ser vulnerables a accesos no autorizados, pérdida o alteración. La naturaleza remota de estos servicios, junto con la dependencia de la infraestructura en la nube, amplifica el riesgo de ciberataques y brechas de seguridad. Además, el entorno altamente interconectado de las aplicaciones SaaS, que a menudo interactúan con otros servicios en la nube y APIs, añade capas adicionales de complejidad a la gestión de la seguridad.

En este contexto, la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO 27001 se presenta como una necesidad crítica para las empresas SaaS. La ISO 27001 proporciona un marco sistemático para gestionar la seguridad de la información, garantizando que los riesgos se identifiquen y mitiguen adecuadamente. Además, la norma promueve una cultura de seguridad continua, donde las políticas, procedimientos y controles están alineados con las mejores prácticas internacionales.

El cumplimiento de los requisitos y recomendaciones de esta norma no solo fortalece la postura de seguridad de una empresa SaaS, sino que también ofrece beneficios competitivos. Los clientes actuales y potenciales están cada vez más preocupados por la

seguridad de sus datos y buscan proveedores que demuestren un compromiso claro con la protección de la información. La certificación ISO 27001 actúa como un sello de garantía que puede facilitar la confianza del cliente, mejorar la reputación corporativa y abrir puertas a nuevos mercados.

1.2. Justificación de la implementación de la ISO 27001.

La implementación de la ISO 27001 en una empresa de SaaS no solo es una medida de protección esencial, sino también una estrategia de negocio inteligente. Proporciona un marco comprobado para gestionar la seguridad de la información, cumple con los requisitos regulatorios y mejora la confianza del cliente, lo que en conjunto fortalece la posición competitiva de la empresa en el mercado.

Actualmente los datos son uno de los activos más valiosos y la seguridad de la información se ha convertido en una prioridad crítica, especialmente para las empresas de Software como Servicio (SaaS). Estas empresas, que operan en un entorno completamente digital, manejan grandes volúmenes de información sensible, lo que las convierte en objetivos atractivos para ciberataques y otras amenazas relacionadas con la seguridad de los datos.
La norma ISO 27001 se ha consolidado como el estándar internacional más reconocido para la gestión de la seguridad de la información. Su implementación ofrece un enfoque sistemático y proactivo para identificar, evaluar y gestionar los riesgos asociados con la información. La mencionada norma no solo abarca aspectos técnicos, sino que también se enfoca en la gestión organizativa, incluyendo políticas, procedimientos y controles que aseguran que todas las partes de la empresa contribuyan a la protección de la información.

Se resumen a continuación en 6 argumentos la justificación para implementar la ISO 27001 en una empresa de SaaS:

1. **Protección de información crítica:** Las empresas SaaS manejan datos sensibles de múltiples clientes, lo que requiere un alto nivel de protección para evitar accesos no autorizados, pérdidas o alteraciones. La ISO 27001 proporciona un marco estructurado para proteger la confidencialidad, integridad y disponibilidad de estos datos.
2. **Cumplimiento normativo:** En muchos sectores, el cumplimiento de regulaciones específicas relacionadas con la protección de datos es obligatorio y la norma ISO 27001 ayuda a las empresas SaaS a cumplir con estas regulaciones, como el Reglamento General de Protección de Datos (GDPR) en Europa, al asegurar que se implementen los controles adecuados para la gestión de datos personales.

3. **Mitigación de riesgos:** La norma exige una evaluación continua de riesgos, lo que permite a las empresas SaaS identificar y mitigar potenciales amenazas antes de que se materialicen en incidentes de seguridad. Esto es crucial en un entorno donde las amenazas evolucionan constantemente y pueden tener consecuencias significativas para la empresa y sus clientes.
4. **Confianza del cliente y ventaja competitiva:** Los clientes son cada vez más conscientes de la importancia de la seguridad de sus datos, por lo que contar con la certificación ISO 27001 puede ser un diferenciador clave. Las empresas certificadas demuestran un compromiso con la seguridad que puede aumentar la confianza del cliente y, en consecuencia, mejorar la retención de clientes y atraer nuevos negocios.
5. **Mejora continua y adaptabilidad:** La ISO 27001 fomenta la mejora continua a través de revisiones y auditorías periódicas. Esto asegura que la empresa no solo mantenga, sino que también mejore su postura de seguridad con el tiempo. Además, el enfoque basado en riesgos permite a las empresas SaaS adaptar su SGSI a las amenazas emergentes y a los cambios en el entorno empresarial.
6. **Resiliencia Operativa:** La implementación de un SGSI robusto bajo la ISO 27001 también contribuye a la resiliencia operativa de la empresa. Al estar mejor preparada para enfrentar y gestionar incidentes de seguridad la empresa puede asegurar la continuidad de sus servicios incluso en situaciones adversas, minimizando el impacto en los clientes y en la operación diaria.

1.3. Propósito del trabajo.

El propósito de este Trabajo Fin de Grado (TFG) es demostrar la implementación práctica, de manera parcial, de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001, en una empresa ficticia denominada **InnovaTech Consulting**, dedicada al desarrollo de software como servicio (SaaS). El trabajo se enfoca en desarrollar y aplicar una serie de elementos clave del SGSI que resultan críticos para garantizar la seguridad de la información en un entorno digital, centrándose en aspectos específicos del cumplimiento normativo, automatización de procesos y gestión de riesgos.

Este TFG también tiene la intención de reflejar los resultados de una experiencia personal adquirida durante la implementación y mantenimiento del SGSI en una empresa real, culminando con la obtención de la certificación ISO 27001 por parte de AENOR. A partir de estos aprendizajes, el presente trabajo adapta las operaciones y desafíos reales a un escenario ficticio, lo que permite delimitar el alcance del análisis y centrarse en los aspectos clave de la gestión de la seguridad de la información.

Es importante resaltar que, aunque el trabajo incluye una base teórica, desarrollada en los capítulos 3 "Marco Teórico" y 4 "Metodología", es esencial destacar su enfoque eminentemente práctico.

A lo largo de este TFG, se han desarrollado de manera profunda y realista seis elementos fundamentales que han sido aplicados con rigor, reflejando un esfuerzo significativo en el análisis de riesgos, valoración de activos, personas y su vinculación con situaciones de riesgo. Las decisiones sobre la implementación de controles, la asignación de plazos, recursos y personas, no han sido meramente teóricas, sino fruto de un trabajo detallado y práctico basado en experiencias reales en la gestión de un SGSI.

Entre los aspectos más destacados, se encuentran la creación de documentos clave como un Plan de Continuidad de Negocio y una Política de Seguridad de la Información. Estos documentos no solo demuestran la importancia de la gestión adecuada de la información documentada en un SGSI, sino que subrayan el papel crucial que un profesional con Grado en Ingeniería Informática puede desempeñar como consultor tecnológico en empresas que aspiran a la excelencia operativa en un entorno tecnológico.

Los resultados obtenidos, expuestos en el capítulo 5 "Resultados y Discusión", y las tablas exhaustivas incluidas en dicho capítulo, son prueba tangible del enfoque práctico del trabajo. Estas tablas no solo reflejan la complejidad y alcance del análisis realizado, sino que también muestran el esfuerzo dedicado a valorar y gestionar los riesgos de una manera que se asemeja mucho a situaciones reales. Esta metodología ha sido la clave para que la empresa, en su representación ficticia, haya logrado la certificación ISO 27001 por una entidad acreditada por ENAC.

En definitiva, aunque este trabajo se basa en un marco teórico necesario, el verdadero valor del TFG reside en su enfoque aplicado, que no solo abarca una amplia gama de situaciones prácticas, sino que también muestra el impacto real que un SGSI bien implementado puede tener en la seguridad y continuidad de las operaciones de una empresa tecnológica.

1.3.1. Alcance del trabajo.

El alcance del proyecto ha sido deliberadamente limitado a las áreas más relevantes y de mayor impacto en la seguridad de la información para la empresa ficticia. Los elementos desarrollados incluyen:

1. **Evaluación de Riesgos y Plan de Acción:** Identificación de activos críticos, análisis de amenazas y vulnerabilidades, evaluación de riesgos, y desarrollo de un plan de acción para mitigar los riesgos identificados.
2. **Objetivos e Indicadores de Seguridad:** Establecimiento de objetivos de seguridad alineados con la estrategia organizativa y definición de indicadores clave para medir el desempeño del SGSI.
3. **Declaración de Aplicabilidad (SOA):** Selección y justificación de los controles de seguridad que serán implementados, basados en los resultados de la evaluación de riesgos y los requisitos específicos de la empresa.
4. **Automatización en Microsoft Azure:** Implementación de soluciones automatizadas en la plataforma de nube Microsoft Azure para gestionar los controles y otros elementos del SGSI, incluyendo la monitorización, respuesta a incidentes y la aplicación de políticas de seguridad.
5. **Plan de Continuidad de Negocio:** Desarrollo de un plan integral que asegure la continuidad operativa de la empresa en caso de interrupciones o desastres, alineado con las mejores prácticas de la ISO 27001.
6. **Política de Seguridad de la Información:** Creación de una política de seguridad que establezca las directrices y procedimientos para proteger la información crítica de la empresa, asegurando el cumplimiento de las normativas y la sensibilización del personal.

A través de estos seis elementos, el TFG no solo busca cumplir con los requisitos académicos de demostrar un conocimiento de la norma ISO 27001, sino también ofrecer una aplicación práctica que puede servir como modelo para organizaciones que operan en un entorno similar. La elección de estos componentes refleja la necesidad de una aproximación enfocada en las áreas más críticas de la seguridad de la información, especialmente en un contexto de trabajo remoto y con una infraestructura tecnológica basada en la nube.

En definitiva, la idea central de este trabajo es implementar de manera práctica y detallada los elementos clave de un SGSI, aportando un valor tangible tanto a la teoría de la gestión de la seguridad de la información como a su aplicación en un entorno empresarial realista.

1.3.2. Limitaciones del trabajo.

Si bien este TFG demuestra un conocimiento integral y aplicado de la norma ISO 27001, es importante señalar que no todos los requisitos y apartados de la norma han sido abordados. Las limitaciones de este trabajo se detallan a continuación:

1. **Exclusión de otros requisitos de la ISO 27001:**
    - Este TFG se ha centrado exclusivamente en los aspectos más críticos de la implementación del SGSI que tienen un mayor impacto técnico y estratégico. Otros requisitos de la ISO 27001, como la gestión de recursos, la evaluación del desempeño en su totalidad o y ciertas cláusulas de control interno no han sido abordados.
2. **Enfoque en la implementación práctica:**
    - El trabajo ha sido deliberadamente acotado para permitir un desarrollo práctico más profundo de los elementos seleccionados, lo cual se entiende más relevante y manejable dentro del contexto de un TFG. Esta decisión busca proporcionar un valor tangible y aplicable a escenarios reales, especialmente en el ámbito de la informática y la seguridad en la nube.
3. **Limitaciones de tiempo y recursos:**
    - Como cualquier proyecto académico, este TFG ha estado sujeto a limitaciones de tiempo y recursos. Estas restricciones han influido en la decisión de acotar el alcance del trabajo, enfocándose en los elementos que pueden ser implementados de manera práctica y efectiva dentro del marco temporal disponible.
4. **Generalización de ciertos aspectos:**
    - Algunos aspectos de la implementación se han generalizado o asumido para adecuarse al formato académico del TFG. Si bien las soluciones propuestas están alineadas con las mejores prácticas y la norma ISO 27001, algunas decisiones y configuraciones específicas podrían variar en un entorno de producción real dependiendo de las necesidades exactas de la organización.

1.3.3. Reconocimiento de requisitos no cubiertos.

Aunque este TFG no aborda todos los aspectos de la ISO 27001, se reconoce la importancia de los requisitos no incluidos en el alcance. Se tiene un conocimiento sólido de

las demás cláusulas y controles de la norma, y se entiende que su aplicación completa sería necesaria para lograr una certificación integral del SGSI en una empresa real.

Este enfoque acotado no implica una subestimación de los otros requisitos de la ISO 27001, sino una decisión consciente de centrarse en los elementos que pueden ser desarrollados de manera más significativa en el contexto de este proyecto académico.

2. OBJETIVOS.

2.1. Objetivo general.

El objetivo general de este Trabajo Fin de Grado es diseñar e implementar los elementos clave de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001 en la empresa ficticia **InnovaTech Consulting**, enfocándose en la protección de la información crítica en un entorno digital altamente distribuido y basado en la nube. Este objetivo se centra en asegurar que los aspectos más relevantes y críticos de la seguridad de la información sean abordados de manera efectiva, mediante el desarrollo de una evaluación de riesgos exhaustiva, la definición de controles aplicables y la implementación de soluciones automatizadas y estratégicas.

El trabajo busca demostrar cómo una organización puede fortalecer su postura de seguridad a través de la aplicación práctica de la norma ISO 27001, asegurando la confidencialidad, integridad y disponibilidad de la información en un contexto de trabajo remoto y utilizando infraestructura en la nube. A través de este objetivo, se pretende proporcionar un modelo de referencia que pueda ser aplicado a empresas con características similares, contribuyendo tanto al campo académico como al desarrollo de buenas prácticas en la industria.

2.2. Objetivos específicos.

La finalidad de definir unos objetivos específicos es la de proporcionar una estructura clara y práctica para la implementación de la ISO 27001 en **InnovaTech Consulting**, asegurando que todos los aspectos críticos de la seguridad de la información sean abordados de manera integral.

Para alcanzar el objetivo general de este Trabajo Fin de Grado, se han definido los siguientes objetivos específicos, que guían el desarrollo de los elementos clave del Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001 en InnovaTech Consulting:

1. **Realizar una Evaluación de Riesgos:**
    - Identificar y catalogar los activos de información críticos de **InnovaTech Consulting**.
    - Analizar las amenazas y vulnerabilidades asociadas a estos activos.
    - Evaluar los riesgos en términos de probabilidad e impacto, priorizando aquellos que requieren acciones inmediatas.
    - Desarrollar un plan de acción para mitigar los riesgos identificados, asegurando la protección de la información crítica.
2. **Establecer Objetivos e Indicadores de Seguridad:**
    - Definir objetivos de seguridad alineados con la estrategia organizativa y las necesidades específicas de **InnovaTech Consulting**.
    - Desarrollar indicadores clave de desempeño (KPIs) que permitan medir y monitorear el cumplimiento de los objetivos de seguridad establecidos.
    - Implementar un sistema de seguimiento para evaluar continuamente el desempeño del SGSI.
3. **Elaborar la Declaración de Aplicabilidad (SOA):**
    - Seleccionar y justificar los controles de seguridad aplicables en base a los resultados de la evaluación de riesgos.
    - Documentar la declaración de aplicabilidad, explicando la razón de cada control seleccionado y cómo se implementará para mitigar los riesgos identificados.
    - Alinear la SOA con los requisitos específicos de **InnovaTech Consulting** y los estándares de la norma ISO 27001.
4. **Automatizar parte de la gestión del SGSI en Microsoft Azure:**
    - Implementar soluciones automatizadas en la plataforma de nube Microsoft Azure para gestionar elementos del SGSI, incluyendo la monitorización, respuesta a incidentes y la aplicación de políticas de seguridad.
    - Configurar herramientas y servicios en Azure que soporten la automatización de procesos clave, mejorando la eficiencia y la capacidad de respuesta ante incidentes de seguridad.

5. **Desarrollar un Plan de Continuidad de Negocio:**
    - Diseñar un plan integral que asegure la continuidad operativa de **InnovaTech Consulting** en caso de interrupciones o desastres.
    - Incluir estrategias de recuperación ante desastres, planes de contingencia, y procedimientos de respuesta ante incidentes que puedan afectar la disponibilidad de los servicios críticos.
6. **Crear la Política de Seguridad de la Información:**
    - Desarrollar una política de seguridad que establezca las directrices y procedimientos para proteger la información crítica de **InnovaTech Consulting**.
    - Asegurar que la política cubra todos los aspectos relevantes de la seguridad de la información, incluyendo la gestión de accesos, la protección de datos, y la respuesta a incidentes.
    - Promover la sensibilización y el cumplimiento de la política entre todos los empleados y partes interesadas de la organización.

3. MARCO TEÓRICO.

El marco teórico de este Trabajo Fin de Grado proporciona el contexto conceptual y técnico necesario para comprender la importancia y el enfoque de la seguridad de la información, especialmente en el contexto de las empresas de Software como Servicio (SaaS). Este capítulo aborda los fundamentos de la seguridad de la información, explorando los conceptos clave, las amenazas y vulnerabilidades comunes en el entorno SaaS, y la relevancia de la norma ISO 27001 como un estándar internacional para la gestión de la seguridad de la información.

3.1. Seguridad de la Información.

La seguridad de la información es un aspecto crítico para las organizaciones actuales, especialmente para aquellas que operan en un entorno digital intensivo, como las empresas SaaS. La información, en sus diversas formas, es uno de los activos más valiosos para cualquier organización, y su protección es fundamental para garantizar la continuidad del negocio, la confianza de los clientes y el cumplimiento de las regulaciones legales.

La seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información contra una amplia gama de amenazas, asegurando que los riesgos asociados sean gestionados de manera efectiva. En el contexto de las empresas SaaS, esto implica no solo proteger los datos internos de la organización, sino también la información sensible de los clientes que confían en estos servicios para gestionar sus propios datos y operaciones.

3.1.1. Conceptos clave.

a) Confidencialidad, Integridad y Disponibilidad (CIA).

Uno de los pilares fundamentales de la seguridad de la información es el modelo CIA, que se compone de los siguientes elementos:

- **Confidencialidad:** Asegura que la información solo sea accesible a las personas autorizadas y evita la divulgación no autorizada de información. Esto es crucial en un entorno SaaS, donde los datos de múltiples clientes se almacenan en sistemas compartidos.
- **Integridad:** Garantiza que la información sea precisa y completa, y que no haya sido alterada de manera no autorizada. La integridad es vital para mantener la confianza en los datos almacenados y procesados por las aplicaciones SaaS.

- **Disponibilidad:** Asegura que la información esté accesible y utilizable cuando sea necesario. En los servicios SaaS, la disponibilidad es un factor crítico, ya que los clientes dependen de estos sistemas para sus operaciones diarias.

b) Amenazas y vulnerabilidades.

En el ámbito de la seguridad de la información, las amenazas son eventos o circunstancias que pueden causar daño a los activos de información, mientras que las vulnerabilidades son debilidades o fallas en un sistema que pueden ser explotadas por dichas amenazas. En el contexto de las empresas SaaS, algunas amenazas comunes incluyen:

- **Ciberataques:** Incluyen actividades maliciosas como hacking, phishing, y ataques de ransomware, que buscan comprometer la seguridad de la información.
- **Errores Humanos:** La falta de formación o errores no intencionados por parte del personal pueden exponer la información a riesgos significativos.
- **Fallos de Sistema:** Problemas técnicos como caídas de servidores, fallos en la infraestructura de red o bugs en el software pueden afectar la disponibilidad y la integridad de la información.

c) Gestión de Riesgos.

La gestión de riesgos es un proceso esencial dentro de la seguridad de la información que implica identificar, evaluar y priorizar los riesgos para implementar controles que minimicen su impacto. Este proceso es particularmente relevante en empresas SaaS debido a la naturaleza interconectada de sus servicios, donde los riesgos pueden propagarse rápidamente a través de diversas plataformas y sistemas.

d) Controles de Seguridad.

Los controles de seguridad son medidas, políticas y procedimientos implementados para mitigar los riesgos identificados. En el contexto de la ISO 27001, estos controles están organizados en el Anexo A de la norma y abarcan aspectos como el control de acceso, la gestión de incidentes de seguridad, la criptografía, y la seguridad física y ambiental, entre otros. La correcta implementación de estos controles es fundamental para la protección eficaz de la información.

3.1.2. Amenazas y vulnerabilidades en entornos SaaS.

Las empresas que operan bajo el modelo de Software como Servicio (SaaS) se encuentran en un entorno altamente dinámico y digitalizado, lo que las expone a una variedad de amenazas y vulnerabilidades que pueden comprometer la seguridad de la información.

Dado que estas empresas manejan grandes volúmenes de datos sensibles, tanto propios como de sus clientes, es crucial identificar y gestionar las amenazas y vulnerabilidades para asegurar la continuidad del negocio y proteger la integridad de la información.

Las principales amenazas en entornos SaaS son:

1. **Ciberataques dirigidos:**
    - **Ataques de Phishing:** Los ataques de phishing son un método común utilizado por los ciberdelincuentes para obtener acceso no autorizado a información sensible. En entornos SaaS, los atacantes suelen dirigirse a los usuarios con correos electrónicos falsos que parecen legítimos para robar credenciales de inicio de sesión.
    - **Malware y Ransomware:** Los ataques de malware, incluyendo ransomware, son una amenaza significativa para las empresas SaaS. Estos ataques pueden cifrar datos críticos, bloqueando el acceso a los sistemas hasta que se pague un rescate. En un entorno SaaS, donde los servicios deben estar disponibles de manera continua, un ataque de ransomware puede tener consecuencias devastadoras.
    - **Ataques de Denegación de Servicio (DDoS):** Los ataques DDoS buscan interrumpir el acceso a los servicios de una empresa SaaS inundando sus servidores con tráfico malicioso. Estos ataques pueden causar interrupciones significativas en el servicio, afectando la disponibilidad de las aplicaciones SaaS para los usuarios.
2. **Compromiso de la infraestructura en la nube:**
    - **Acceso no autorizado a la nube:** Las empresas SaaS dependen en gran medida de la infraestructura en la nube para almacenar y procesar datos. Si los controles de acceso a estos recursos no están adecuadamente configurados, los atacantes pueden obtener acceso a datos sensibles.
    - **Fallos en la configuración de la nube:** Configuraciones incorrectas o inadecuadas de la infraestructura en la nube pueden exponer los datos a riesgos innecesarios. Ejemplos de esto incluyen almacenamiento de datos en buckets públicos sin la seguridad adecuada o la falta de cifrado en tránsito o en reposo.

3. **Exposición de APIs y conexiones externas:**
    - **Vulnerabilidades en APIs:** Las aplicaciones SaaS a menudo dependen de APIs para la integración con otros servicios y aplicaciones. Si una API está mal configurada o contiene vulnerabilidades, puede ser explotada por atacantes para acceder a datos sensibles o comprometer la integridad del sistema.
    - **Conexiones inseguras:** La comunicación entre diferentes servicios a través de conexiones no cifradas o inseguras puede ser interceptada por atacantes, lo que lleva a la exposición de información sensible.
4. **Amenazas internas:**
    - **Errores humanos:** Los empleados o usuarios internos pueden, accidentalmente o intencionadamente, comprometer la seguridad de la información. Esto puede incluir desde la divulgación involuntaria de información hasta la eliminación accidental de datos.
    - **Insiders maliciosos:** Los empleados descontentos o con acceso privilegiado pueden abusar de su acceso para extraer o manipular información crítica, lo que representa una amenaza significativa para la seguridad interna.

Las vulnerabilidades comunes en entornos SaaS son:

1. **Deficiencias en la gestión de accesos:**
    - **Políticas de contraseñas débiles:** La falta de políticas robustas para la gestión de contraseñas puede facilitar ataques de fuerza bruta o el uso de contraseñas comprometidas, permitiendo el acceso no autorizado a sistemas críticos.
    - **Falta de autenticación multifactor (MFA):** No implementar la autenticación multifactor en los accesos a los sistemas SaaS aumenta significativamente el riesgo de que cuentas comprometidas sean explotadas.
2. **Inadecuada segregación de datos:**
    - **Compartición de recursos:** La arquitectura multitenant típica de los servicios SaaS, donde múltiples clientes comparten la misma infraestructura, puede presentar riesgos si no se aseguran adecuadamente los límites entre los datos de diferentes clientes.

- **Errores en la configuración de permisos:** Permisos mal configurados pueden permitir que usuarios no autorizados accedan a datos de otros clientes, lo que representa un riesgo significativo de violación de datos.

3. **Actualizaciones y parches insuficientes:**
   - **Vulnerabilidades no parcheadas:** La falta de actualización regular de software y la demora en aplicar parches de seguridad pueden dejar expuestos a los sistemas SaaS a vulnerabilidades conocidas que los atacantes pueden explotar.
   - **Dependencia de software de terceros:** Las empresas SaaS a menudo dependen de bibliotecas y componentes de software de terceros. Si estos no se actualizan o parchan adecuadamente, pueden introducir vulnerabilidades en el sistema.
4. **Falta de controles de monitorización y detección:**
   - **Monitorización inadecuada:** La ausencia de sistemas adecuados de monitorización y detección puede significar que los incidentes de seguridad pasen desapercibidos durante largos períodos, permitiendo que los atacantes operen sin ser detectados.
   - **Respuestas tardías a incidentes:** Sin un sistema de detección temprana, las respuestas a los incidentes de seguridad pueden ser lentas e ineficaces, lo que aumenta el impacto de cualquier brecha de seguridad.

3.2. La Norma ISO 27001.

La norma ISO/IEC 27001 es un estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información mediante un proceso continuo de evaluación de riesgos, implementación de controles, y revisión y mejora del sistema. Esta norma es ampliamente reconocida y adoptada a nivel mundial, y su cumplimiento puede proporcionar una ventaja competitiva significativa para las organizaciones, al demostrar su compromiso con la seguridad de la información.

La norma ISO 27001 es particularmente relevante para empresas que, como las de Software como Servicio (SaaS), manejan grandes volúmenes de datos sensibles y operan en un entorno digital altamente interconectado. Esta norma ofrece un marco estructurado y

estandarizado que ayuda a estas organizaciones a gestionar los riesgos asociados con la seguridad de la información de manera eficaz y a cumplir con las regulaciones y expectativas del mercado.

3.2.1. Estructura y principios fundamentales.

La ISO 27001 está organizada en torno a un conjunto de requisitos específicos que una organización debe cumplir para establecer un SGSI efectivo. Estos requisitos se presentan en una estructura sistemática que facilita su implementación, seguimiento y mejora continua. A continuación, se describen los componentes clave de la estructura y los principios fundamentales de la norma:

a) Estructura de la norma ISO 27001.

La estructura de la ISO 27001 se basa en la metodología conocida como PDCA (Plan-Do-Check-Act), que se utiliza para guiar la implementación y el mantenimiento del SGSI. Esta metodología permite a las organizaciones seguir un ciclo continuo de mejora, asegurando que la gestión de la seguridad de la información se mantenga relevante y efectiva frente a las amenazas y cambios en el entorno. La norma se organiza en las siguientes secciones principales:

- **Sección 4: Contexto de la organización.**
    - Establece la necesidad de comprender la organización y su contexto, identificar las partes interesadas y definir el alcance del SGSI. Esta sección es fundamental para garantizar que el SGSI esté alineado con las necesidades y expectativas de la organización.
- **Sección 5: Liderazgo.**
    - Requiere el compromiso de la alta dirección en el establecimiento y mantenimiento del SGSI. Incluye la definición de políticas de seguridad de la información, la asignación de roles y responsabilidades, y la promoción de la concienciación y la cultura de seguridad dentro de la organización.
- **Sección 6: Planificación.**
    - Describe la necesidad de planificar acciones para abordar los riesgos y oportunidades en la seguridad de la información, incluyendo la realización de evaluaciones de riesgos, la definición de objetivos de seguridad, y la planificación de cómo se alcanzarán estos objetivos.

- **Sección 7: Apoyo.**
    - Cubre los requisitos para proporcionar los recursos necesarios para el SGSI, incluyendo la competencia del personal, la concienciación, la comunicación, y el control de la información documentada.
- **Sección 8: Operación.**
    - Detalla los requisitos para la implementación y operación del SGSI, incluyendo la evaluación y tratamiento de riesgos de seguridad de la información, y la implementación de los controles necesarios.
- **Sección 9: Evaluación del desempeño.**
    - Enfocada en la monitorización, medición, análisis y evaluación del desempeño del SGSI. Incluye la realización de auditorías internas y la revisión por la dirección para asegurar que el SGSI sea efectivo y cumpla con los objetivos de la organización.
- **Sección 10: Mejora.**
    - Establece los requisitos para la mejora continua del SGSI, incluyendo la gestión de no conformidades, acciones correctivas y la mejora continua basada en los resultados de la monitorización y las auditorías.

b) Principios fundamentales de la ISO 27001.

Los principios fundamentales de la ISO 27001 se centran en la gestión sistemática de la seguridad de la información a través de un enfoque basado en riesgos. Algunos de los principios clave incluyen:

- **Enfoque basado en riesgos:** La ISO 27001 se centra en la identificación y evaluación de los riesgos que podrían afectar la seguridad de la información. Este enfoque permite a las organizaciones priorizar y aplicar los controles más adecuados para mitigar estos riesgos de manera efectiva.
- **Confidencialidad, integridad y disponibilidad (CIA):** La norma está diseñada para asegurar que la información sea accesible solo por quienes están autorizados (confidencialidad), sea precisa y completa (integridad), y esté disponible cuando se necesite (disponibilidad).

- **Mejora continua:** La ISO 27001 promueve la mejora continua del SGSI a través del ciclo PDCA (Plan-Do-Check-Act, planificar, implementar, verificar y mejorar). Esto asegura que el sistema evolucione para adaptarse a nuevas amenazas, cambios en el entorno organizativo y la introducción de nuevas tecnologías.
- **Cumplimiento legal y regulatorio:** La norma también enfatiza la necesidad de que las organizaciones cumplan con todas las leyes y regulaciones aplicables en materia de seguridad de la información, lo que es esencial en entornos como el SaaS, donde se manejan datos sensibles de clientes.
- **Documentación y evidencia:** La ISO 27001 requiere una documentación exhaustiva del SGSI, lo que incluye políticas, procedimientos, registros y evidencia de cumplimiento. Esto no solo facilita la implementación y el mantenimiento del sistema, sino que también es crucial durante las auditorías internas y externas.

3.2.2. Cláusulas clave.

La norma ISO 27001 establece un conjunto de cláusulas clave que son fundamentales para la creación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) eficaz. Entre estas, la evaluación de riesgos, la implementación de controles de seguridad y la gestión de incidentes son elementos críticos que permiten a una organización identificar, mitigar y responder a las amenazas a la seguridad de la información. A continuación, se describen estas cláusulas y su importancia en el contexto de la norma.

a) Evaluación de riesgos (Cláusula 6.1.2).

La evaluación de riesgos es uno de los procesos más importantes dentro de la ISO 27001 y está descrito en la Cláusula 6.1.2. Este proceso se centra en la identificación, análisis y valoración de los riesgos que podrían afectar la seguridad de la información de una organización. La evaluación de riesgos proporciona una base sólida para la toma de decisiones informadas sobre qué medidas de seguridad deben implementarse para proteger los activos de información. La secuencia es la siguiente:

- **Identificación de riesgos:** El primer paso en la evaluación de riesgos consiste en identificar las amenazas y vulnerabilidades que podrían comprometer los activos de información de la organización. Esto incluye la identificación de todas las fuentes de riesgo potencial, como ciberataques, errores humanos, fallos técnicos y desastres naturales.
- **Análisis de riesgos:** Una vez identificados los riesgos, es necesario analizarlos para comprender su probabilidad de ocurrencia y el impacto potencial en la organización.

Este análisis permite priorizar los riesgos en función de su gravedad y determinar cuáles requieren atención inmediata.

- **Valoración de riesgos:** La valoración de riesgos implica comparar el nivel de riesgo analizado con los criterios de riesgo establecidos por la organización. Esto ayuda a decidir si el riesgo es aceptable o si se necesitan acciones adicionales para mitigarlo.
- **Tratamiento de riesgos:** Basado en la valoración, se desarrollan y seleccionan estrategias para tratar los riesgos, que pueden incluir la evitación, transferencia, mitigación o aceptación del riesgo. Este proceso es esencial para garantizar que los recursos de seguridad se asignen de manera efectiva.

b) Controles de seguridad (Cláusula 6.1.3 y Anexo A).

La implementación de controles de seguridad es fundamental para mitigar los riesgos identificados durante la evaluación de riesgos. La Cláusula 6.1.3 y el Anexo A de la ISO 27001 proporcionan un marco detallado para la selección y aplicación de estos controles, que son esenciales para proteger la confidencialidad, integridad y disponibilidad de la información. Para ello se seguirá el proceso siguiente:

- **Selección de controles:** La Cláusula 6.1.3 requiere que las organizaciones seleccionen controles de seguridad específicos para tratar los riesgos identificados. Estos controles deben ser apropiados para el nivel de riesgo y deben estar alineados con los objetivos de seguridad de la organización.
- **Anexo A - Controles de seguridad:** El Anexo A de la ISO/IEC 27001:2022 incluye 93 controles distribuidos en estos cuatro grupos, lo que representa una simplificación y actualización respecto a la versión anterior y que cubren todas las áreas clave de la seguridad de la información, desde el control de accesos y la seguridad física hasta la gestión de incidentes y la seguridad en las comunicaciones. Las organizaciones deben revisar estos controles y decidir cuáles son aplicables a su entorno específico, documentando esta selección en la Declaración de Aplicabilidad.
- **Implementación de controles:** Una vez seleccionados, los controles deben implementarse de manera efectiva en los sistemas y procesos de la organización. Esto incluye la integración de controles en las políticas de seguridad, procedimientos operativos y en la infraestructura tecnológica.
- **Monitorización y revisión de controles:** La eficacia de los controles debe ser monitoreada regularmente para asegurarse de que siguen siendo adecuados para mitigar los riesgos, especialmente en un entorno cambiante. Esto implica realizar

auditorías internas y evaluaciones continuas para ajustar los controles según sea necesario.

c) Gestión de incidentes (Cláusula 16).

La gestión de incidentes es otra cláusula clave de la ISO 27001, descrita en la Cláusula 16. Esta cláusula aborda la necesidad de que las organizaciones establezcan procedimientos para identificar, responder y recuperarse de incidentes de seguridad de la información de manera efectiva. Una gestión adecuada de incidentes es crucial para minimizar el impacto de los incidentes en la organización y asegurar la continuidad del negocio.

- **Identificación de incidentes:** El proceso de gestión de incidentes comienza con la identificación y reporte de incidentes de seguridad. Esto incluye cualquier evento que tenga el potencial de comprometer la seguridad de la información, como accesos no autorizados, fallos en los sistemas de seguridad, o ataques cibernéticos.
- **Respuesta a incidentes:** Una vez identificado un incidente, la organización debe seguir procedimientos establecidos para responder de manera rápida y eficaz. Esto puede incluir el aislamiento de sistemas afectados, la recopilación de evidencias, y la contención del incidente para prevenir una mayor propagación.
- **Investigación y análisis:** Después de la respuesta inicial, se debe llevar a cabo una investigación para determinar la causa raíz del incidente, evaluar su impacto y entender cómo se produjo. Este análisis es fundamental para evitar la recurrencia del incidente.
- **Recuperación y restauración:** La gestión de incidentes también incluye la recuperación y restauración de los sistemas y datos afectados por el incidente, asegurando que se retorne a las operaciones normales de manera segura y controlada.
- **Mejora continua:** Finalmente, los incidentes deben ser documentados y analizados para identificar oportunidades de mejora en el SGSI. Esto puede llevar a la actualización de políticas, procedimientos y controles para fortalecer la seguridad de la información y prevenir futuros incidentes.

3.3. Relación de la ISO 27001 con otras Normas y Buenas Prácticas.

La norma ISO 27001 es ampliamente reconocida como un estándar internacional de referencia para la gestión de la seguridad de la información, pero no existe en un vacío. La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la ISO 27001 a menudo se complementa y se integra con otras normas, marcos y buenas prácticas que abordan diferentes aspectos de la seguridad y la gestión de la información. Este enfoque integrado ayuda a las organizaciones a cumplir con los requisitos normativos y mejorar su postura de seguridad general.

ISO 27002.

La norma ISO/IEC 27002 es una guía complementaria a la ISO 27001 que proporciona directrices detalladas para la implementación de los controles de seguridad de la información. Mientras que la ISO 27001 especifica los requisitos que una organización debe cumplir, la ISO 27002 ofrece recomendaciones sobre cómo implementar estos requisitos y controles. Esta norma es particularmente útil para organizaciones que buscan alinearse con las mejores prácticas en seguridad de la información, proporcionando ejemplos concretos de cómo cada control puede ser implementado en diferentes contextos organizacionales.

La ISO 27002 no es una norma certificable por sí misma, sino que actúa como un soporte para la implementación de la ISO 27001. Juntas, estas normas permiten a las organizaciones no solo establecer un SGSI, sino también implementar los controles de seguridad de manera efectiva y conforme a las mejores prácticas internacionales.

ISO 9001.

La ISO 9001 es la norma internacional para sistemas de gestión de la calidad (SGC). Aunque su enfoque principal es la calidad, existe una relación directa entre la gestión de la calidad y la seguridad de la información. Ambas normas comparten principios comunes, como el enfoque en la mejora continua, la gestión basada en procesos y la necesidad de liderazgo y compromiso de la alta dirección.

Las organizaciones que ya han implementado un SGC basado en ISO 9001 pueden encontrar sinergias al implementar un SGSI conforme a ISO 27001. Por ejemplo, los procesos de auditoría interna, revisión por la dirección y gestión de documentos pueden ser comunes o estar alineados entre ambos sistemas, lo que facilita la gestión integrada y reduce el esfuerzo administrativo.

GDPR (Reglamento General de Protección de Datos).

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea establece obligaciones legales para la protección de datos personales. Aunque no es una norma de gestión de la seguridad de la información en sí, el GDPR tiene implicaciones significativas para cualquier organización que maneje datos personales, lo que incluye muchas empresas de SaaS.

La ISO 27001 puede ser una herramienta eficaz para demostrar el cumplimiento con el GDPR. Al implementar un SGSI que proteja la confidencialidad, integridad y disponibilidad de los datos, las organizaciones pueden gestionar mejor los riesgos asociados con el tratamiento de datos personales y cumplir con las obligaciones del GDPR. Los controles de seguridad definidos en la ISO 27001, como la gestión de accesos, la encriptación y la gestión de incidentes, son directamente aplicables para asegurar el cumplimiento con el GDPR.

NIST Cybersecurity Framework.

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) es un conjunto de directrices voluntarias que ayudan a las organizaciones a gestionar y reducir los riesgos de ciberseguridad. El marco del NIST es muy utilizado, especialmente en Estados Unidos, y se centra en cinco funciones principales: identificar, proteger, detectar, responder y recuperar.

Aunque el NIST Cybersecurity Framework y la ISO 27001 son diferentes en su enfoque y origen, son compatibles y se pueden utilizar de manera complementaria. Mientras que el NIST proporciona un enfoque detallado para gestionar riesgos de ciberseguridad, la ISO 27001 ofrece un marco de gestión más amplio y certificable que incluye la seguridad de la información en general. Las organizaciones pueden utilizar el NIST para guiar las actividades técnicas de ciberseguridad y la ISO 27001 para integrar estas actividades dentro de un SGSI certificado.

Buenas Prácticas en Seguridad de la Información (CIS Controls).

Los CIS Controls son un conjunto de mejores prácticas de ciberseguridad desarrolladas por el Center for Internet Security (CIS). Estos controles están diseñados para ayudar a las organizaciones a defenderse de las amenazas más comunes y son ampliamente reconocidos como una guía práctica para mejorar la ciberseguridad.

Los CIS Controls son prácticos y detallados, proporcionando pasos concretos para mejorar la seguridad técnica. Al implementar un SGSI conforme a ISO 27001, las organizaciones pueden utilizar los CIS Controls como una referencia para seleccionar e

implementar controles específicos que mitiguen riesgos técnicos. Esto ayuda a asegurar que las medidas de seguridad estén alineadas con las amenazas actuales y las mejores prácticas reconocidas en el ámbito de la ciberseguridad.

ITIL (Information Technology Infrastructure Library)

ITIL es un marco de gestión de servicios de TI (ITSM) que proporciona un enfoque sistemático para la gestión de los servicios de tecnología de la información. ITIL cubre aspectos como la gestión de incidentes, la gestión de cambios y la gestión de problemas, todos los cuales son relevantes para la seguridad de la información.

Al implementar ISO 27001, las organizaciones pueden aprovechar ITIL para mejorar la gestión de la seguridad de la información dentro del contexto más amplio de la gestión de servicios de TI. ITIL ofrece procedimientos detallados para gestionar incidentes y problemas que se alinean con los requisitos de gestión de incidentes y continuidad de negocio de la ISO 27001.

4. METODOLOGÍA.

En este capítulo se detalla la metodología utilizada para la implementación de la norma ISO 27001 en la empresa ficticia dedicada al desarrollo de software como servicio (SaaS). La metodología adoptada sigue un enfoque sistemático y estructurado, alineado con las directrices establecidas por la ISO 27001, y se basa en la aplicación del ciclo comentado anteriormente PDCA (Planificar-Hacer-Verificar-Actuar) para garantizar la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI).

El proceso metodológico se divide en varias fases clave que abordan desde la definición del alcance del SGSI hasta la selección e implementación de controles de seguridad específicos. Cada fase del proceso está diseñada para identificar, evaluar y mitigar los riesgos de seguridad de la información a los que se enfrenta la empresa ficticia, garantizando que el SGSI sea robusto y eficaz para proteger la confidencialidad, integridad y disponibilidad de la información.

La metodología también contempla la preparación para la certificación ISO 27001 por tercero acreditado, incluyendo la realización de auditorías internas y la revisión por la dirección, con el objetivo de asegurar que el SGSI cumple con los requisitos normativos y está alineado con las mejores prácticas internacionales. Además, se describen las herramientas y recursos utilizados para apoyar la implementación del SGSI, así como los procedimientos específicos adoptados para la gestión de incidentes, la evaluación de riesgos y la mejora continua del sistema.

Se va a usar **InnovaTech Consulting** como nombre ficticio para la empresa. Es un nombre que sugiere innovación y tecnología, alineándose bien con las características de la empresa descrita.

4.1. Descripción de la Empresa.

InnovaTech Consulting es una empresa ficticia desarrollada para este Trabajo de Fin de Grado (TFG), pero basada en un caso real con ciertas variaciones adaptadas al contexto académico. La empresa se especializa en ofrecer servicios de consultoría en el cumplimiento normativo, la automatización de procesos internos de negocio, así como en el desarrollo de proyectos de ingeniería industrial y medioambiental.

La estructura de **InnovaTech Consulting** se fundamenta en una plataforma digital de desarrollo propio, **NormaPro**, que permite gestionar de manera eficiente todos los servicios que presta la empresa, garantizando la seguridad de la información y el cumplimiento de las normativas vigentes.

4.1.1. Misión y Visión de InnovaTech Consulting.

La misión de **InnovaTech Consulting** es proporcionar a las empresas herramientas y soluciones integrales para mejorar su eficiencia operativa y garantizar el cumplimiento normativo. A través de la automatización de procesos internos y el uso de tecnologías avanzadas como la plataforma **NormaPro**, ayudan a sus clientes a ser más competitivos en un entorno empresarial en constante evolución, asegurando al mismo tiempo la protección de la información sensible.

La empresa aspira a convertirse en un referente en el ámbito de la consultoría tecnológica y de cumplimiento normativo mediante la integración de soluciones innovadoras, sostenibles y seguras, contribuyendo al desarrollo de un entorno empresarial más eficiente y conforme a las normativas internacionales de seguridad.

4.1.2. Servicios y soluciones ofrecidas.

InnovaTech Consulting ofrece una serie de servicios clave centrados en optimizar las operaciones empresariales y garantizar el cumplimiento normativo, todo ello a través de su plataforma digital propia, **NormaPro**:

- **Consultoría de cumplimiento normativo**: La empresa ayuda a sus clientes a gestionar el cumplimiento normativo que les afecta, enfocándose en mitigar riesgos y alinear los procesos internos con los estándares regulatorios.
- **Automatización de procesos internos**: Mediante **NormaPro**, InnovaTech optimiza flujos de trabajo, reduciendo la carga operativa y minimizando errores, lo que aumenta la productividad.
- **Proyectos de ingeniería industrial y medioambiental**: La empresa diseña e implementa soluciones técnicas en proyectos de ingeniería, centradas en mejorar la sostenibilidad y cumplir con las regulaciones medioambientales.
- **Plataforma NormaPro**: **NormaPro** facilita la gestión integrada y segura de proyectos, automatizando tareas y garantizando la protección de la información sensible.

4.1.3. Recursos Humanos.

InnovaTech Consulting cuenta con un equipo especializado compuesto por 13 profesionales altamente capacitados, quienes desempeñan roles clave para asegurar el cumplimiento de las normativas y la eficiencia en los proyectos de consultoría y automatización de procesos empresariales. Este equipo multidisciplinario se organiza en

diferentes perfiles, cada uno de ellos responsable de gestionar y proteger información sensible de sus respectivas áreas.

Estructura de la empresa

La empresa está organizada en los siguientes perfiles:

- **Administrativo:** Responsable de la gestión de la contabilidad y finanzas, asegurando que los procesos financieros cumplan con las normativas aplicables.
- **Consultores de Cumplimiento Normativo (2 personas):** Encargados de gestionar la documentación de clientes en relación con la implementación de normas de seguridad de la información y de cumplimiento legal.
- **Desarrolladores de Software (2 personas):** Su responsabilidad principal es el desarrollo y mantenimiento del código fuente de **NormaPro**, la plataforma que soporta las operaciones de la empresa.
- **Técnicos de Proyectos de Ingeniería y Medio Ambiente (2 personas):** Gestionan proyectos técnicos de clientes en las áreas de ingeniería industrial y medioambiental, asegurando su desarrollo y cumplimiento en base a normativas específicas del sector.
- **Responsable de TI:** Encargado de gestionar y proteger toda la información de la empresa, exceptuando la información contable, asegurando la seguridad y la continuidad operativa de los sistemas.
- **Dirección General:** Supervisa la gestión estratégica de la empresa y tiene acceso a toda la información de la organización, con excepción del código fuente.
- **Dirección Financiera:** Asegura el control financiero de la empresa, gestionando los procesos contables y financieros.
- **Responsable del Sistema Integrado de Gestión (ISO 9001, ISO 27001, ISO 45001):** Gestiona la documentación y procesos relacionados con los sistemas de gestión de calidad, seguridad de la información y seguridad y salud en el trabajo.
- **Comercial:** Encargado de la gestión de los datos de clientes, principalmente en relación con la expansión de los servicios de la empresa.
- **Administrador de Sistemas y DBA:** Asegura el correcto funcionamiento y seguridad de los sistemas y bases de datos, protegiendo la integridad de la información que la empresa gestiona.

Facturación.

InnovaTech Consulting mantiene una facturación anual de un millón de euros, lo que refleja su posición sólida en el mercado. Esta cifra de facturación es resultado directo del alto nivel de especialización de su equipo, de su enfoque en el cumplimiento normativo y en la eficiencia empresarial, y del uso intensivo de su plataforma digital **NormaPro**, que permite a la empresa brindar soluciones integradas y de alto valor agregado a sus clientes.

4.1.4. Infraestructura tecnológica.

InnovaTech Consulting se destaca por operar completamente de manera remota, con un equipo distribuido que colabora a través de herramientas digitales y plataformas en la nube. Esta estructura les permite optimizar sus operaciones y reducir costos, a la vez que mantienen un alto nivel de seguridad y eficiencia. La empresa ha trasladado recientemente toda su infraestructura tecnológica a servidores en la nube proporcionados por un proveedor líder en servicios de cloud computing, garantizando así un nivel elevado de escalabilidad, disponibilidad y seguridad.

A continuación, se detallan los principales componentes de la infraestructura tecnológica de la empresa, que abarcan tanto los equipos de hardware como las aplicaciones y entornos digitales empleados por el equipo.

4.1.4.1. Equipos.

InnovaTech Consulting dispone de una variedad de equipos físicos utilizados por sus empleados para desempeñar las diferentes funciones dentro de la empresa. La mayoría de estos equipos están orientados a labores de consultoría, desarrollo de software, y gestión de proyectos. Aunque operan en su mayoría en entornos en la nube, la empresa mantiene algunas infraestructuras físicas mínimas, como un Centro de Procesamiento de Datos (CPD) en Rack.

Entre los equipos más importantes, se encuentran:

- **Thinkpad E15**: Utilizado por el personal administrativo y comercial para la gestión de ventas y proyectos. Cuenta con software estándar como Microsoft Office 365 y Windows Defender para la seguridad.
- **Portátiles Lenovo Yoga 500**: Equipos utilizados por el personal técnico y de dirección, con software para la gestión de proyectos, desarrollo de software y gestión corporativa. Estos equipos cuentan con herramientas como Visual Studio, MySQL Workbench, y Ubuntu en WSL, esenciales para los desarrolladores y gestores de sistemas.

- **Tablets Samsung SM-T713**: Utilizadas por los auditores para registrar datos en el campo, que luego son volcados a los sistemas principales de la empresa a través del software **Audire Pro**.
- **Inicie IT Desk (Intel Core i7-8700k)**: Utilizados por el personal de TI y el director general para la gestión de todas las llaves de acceso a los servicios informáticos y el desarrollo de software. Este equipo tiene instalado software avanzado como Visual Studio Code, MySQL Workbench, y sistemas de virtualización como VirtualBox y Ubuntu WSL.

Estos equipos están distribuidos entre los diferentes perfiles profesionales de la empresa, como se detalla en la **Tabla 1** de este TFG.

4.1.4.2. Aplicaciones y software.

InnovaTech Consulting se apoya en una serie de herramientas y aplicaciones digitales para garantizar la eficiencia operativa y la seguridad en todos sus procesos. La empresa utiliza licencias digitales y software de código abierto que cubren necesidades clave, desde la gestión de proyectos hasta el desarrollo de software.

Entre las principales aplicaciones utilizadas destacan:

- **Microsoft Office 365**: Herramienta central para la edición de documentos, hojas de cálculo y correos electrónicos. Utilizada por todos los perfiles de la empresa.
- **Windows 10 y Windows 11**: Sistemas operativos instalados en los equipos de trabajo.
- **Microsoft Visual Studio Code** y **GitHub Desktop**: Herramientas clave para el desarrollo de software, control de versiones y gestión del código fuente.
- **MySQL Workbench**: Utilizado por los desarrolladores para gestionar las bases de datos y diseñar soluciones de software integradas.
- **Azure DevOps**: Plataforma de Microsoft para la gestión de proyectos, utilizada por la empresa para coordinar los proyectos de desarrollo y automatización.

Estas aplicaciones aseguran un flujo de trabajo eficiente, especialmente con la infraestructura de nube utilizada por la empresa. El total de aplicaciones quedan especificadas en la Tabla 1 de este TFG.

4.1.4.3. Infraestructura en la nube.

La reciente migración de toda la infraestructura tecnológica de **InnovaTech Consulting** a servidores en la nube ha sido un paso crucial para asegurar la disponibilidad,

escalabilidad y seguridad de las operaciones. El proveedor de servicios en la nube ofrece características avanzadas, como la encriptación de datos, autenticación multifactor y monitorización en tiempo real de amenazas.

La infraestructura alojada en la nube permite a la empresa ajustarse rápidamente a las fluctuaciones en la demanda de servicios, ofreciendo así una mayor flexibilidad operativa. El uso de clusters en **Scaleway** y **Azure** permite que los desarrolladores y los gestores de sistemas tengan un entorno seguro y eficiente para la gestión del código fuente y los entornos de desarrollo.

Gracias a esta infraestructura, **InnovaTech Consulting** puede garantizar la continuidad de su negocio, protegiendo la información crítica y escalando sus operaciones sin interrupciones.

La tabla 1 de este TFG muestra las principales infraestructuras en la nube utilizadas por InnovaTech Consulting para el desarrollo, producción y almacenamiento de código fuente. A continuación, se comentan los elementos clave:

- **Cluster Scaleway**: Este entorno virtual está dedicado al desarrollo de los últimos códigos fuente de los proyectos en curso. Funciona como un entorno aislado donde se realizan pruebas y ajustes antes de la implementación en producción, garantizando que los desarrollos se realicen de forma controlada.
- **Cluster Azure**: Azure es otra plataforma utilizada para los servidores en desarrollo. Este entorno proporciona escalabilidad y flexibilidad para los proyectos en fase de creación, con las ventajas adicionales que ofrece un proveedor líder en la nube, como la integración con otras herramientas y servicios en el ecosistema de Microsoft.
- **Servidor hosting IONOS**: Utilizado para el sitio web corporativo de la empresa en un entorno de producción, IONOS garantiza la disponibilidad y estabilidad necesarias para la presencia web de InnovaTech Consulting. Este servidor actúa como la cara visible de la empresa hacia sus clientes y otros stakeholders.
- **GitHub**: GitHub se emplea como el principal repositorio de código fuente. Es una herramienta fundamental para el control de versiones y la colaboración entre los desarrolladores. En este entorno, se almacena y gestiona el código de todos los proyectos en desarrollo, permitiendo la trazabilidad y el control de cambios.

4.1.5. Clientes y Mercados.

InnovaTech Consulting atiende a una amplia variedad de clientes, que van desde pequeñas y medianas empresas hasta grandes corporaciones multinacionales. Sus servicios están presentes en diversos sectores, incluyendo manufactura, servicios financieros, salud, y tecnología. Los clientes confían en la empresa para mejorar sus procesos internos, asegurar el cumplimiento normativo, y proteger la información crítica que manejan.

4.1.6. Desafíos de Seguridad de la Información

Dado el enfoque digital de las operaciones de **InnovaTech Consulting** y la naturaleza sensible de los datos que maneja, la seguridad de la información es una prioridad estratégica. La empresa gestiona volúmenes significativos de información confidencial de sus clientes, que incluyen datos sobre procesos internos, informes de cumplimiento, y evaluaciones de riesgos. Es fundamental proteger esta información contra accesos no autorizados, pérdidas y alteraciones para mantener la confianza de los clientes y cumplir con las normativas vigentes.

La dependencia de la infraestructura en la nube y el trabajo remoto también presenta desafíos adicionales en términos de ciberseguridad. Entre estos desafíos se incluyen la protección contra ciberataques, la gestión segura de accesos remotos, y la implementación de controles de seguridad eficaces en un entorno distribuido. Para mitigar estos riesgos y asegurar una continuidad operativa robusta, Innovatech Consulting ha optado por mantener, de manera complementaria por el momento, una infraestructura mínima con un servidor físico en un rack en su sede física ubicada en su domicilio social.

4.1.7. Entorno de trabajo remoto.

InnovaTech Consulting opera en un entorno de trabajo completamente remoto, lo que significa que, aunque mantiene una sede física, todos sus empleados y colaboradores desempeñan sus funciones desde ubicaciones geográficamente dispersas. Este modelo de trabajo ha sido adoptado por la empresa tanto por sus ventajas en términos de flexibilidad y eficiencia operativa, como por su capacidad para atraer talento a nivel global sin las limitaciones de una ubicación física específica.

El entorno de trabajo remoto en **InnovaTech Consulting** está respaldado por una infraestructura tecnológica robusta que permite una colaboración efectiva y segura entre todos los miembros del equipo. A continuación, se describen las principales características de este entorno:

1. **Infraestructura en la nube:**

- Toda la infraestructura tecnológica de la empresa está alojada en servidores contratados a un proveedor líder de servicios en la nube (Microsoft AZURE). Esto incluye no solo el alojamiento de la plataforma digital de la empresa, sino también las herramientas de colaboración y comunicación utilizadas por los empleados. La nube ofrece a **InnovaTech Consulting** la flexibilidad de escalar sus operaciones según las necesidades del negocio, garantizando al mismo tiempo la alta disponibilidad y seguridad de sus servicios.

2. **Herramientas de comunicación y colaboración:**
    - **InnovaTech Consulting** utiliza una variedad de herramientas digitales para facilitar la comunicación y la colaboración entre sus empleados. Estas herramientas incluyen aplicaciones de mensajería instantánea, videoconferencias, y plataformas de gestión de proyectos, que permiten a los equipos trabajar de manera coordinada, independientemente de su ubicación física. La empresa también utiliza espacios de trabajo compartidos en la nube para gestionar documentos, proyectos y recursos de manera centralizada y accesible.
3. **Seguridad en el acceso remoto:**
    - La seguridad es una prioridad en el entorno de trabajo remoto de **InnovaTech Consulting**. La empresa ha implementado políticas estrictas de seguridad, que incluyen la autenticación multifactor (MFA) para acceder a los sistemas corporativos, el cifrado de datos en tránsito y en reposo, y la gestión de dispositivos seguros. Además, se utilizan redes privadas virtuales (VPN) para asegurar que las conexiones remotas a los recursos de la empresa estén protegidas contra accesos no autorizados.
4. **Gestión del rendimiento y la productividad:**
    - **InnovaTech Consulting** emplea herramientas avanzadas de monitorización y gestión del rendimiento para asegurarse de que los empleados mantengan altos niveles de productividad y cumplan con sus objetivos. Estas herramientas permiten a los gestores supervisar el progreso de los proyectos, gestionar las cargas de trabajo y ofrecer retroalimentación en tiempo real. El trabajo remoto también se apoya en una cultura organizativa que promueve la autodisciplina, la responsabilidad y la comunicación efectiva.
5. **Cultura organizacional y bienestar de los empleados:**

- A pesar de la dispersión geográfica, **InnovaTech Consulting** se esfuerza por mantener una cultura organizacional fuerte y unida. Se realizan reuniones periódicas de equipo, eventos virtuales, y actividades de formación para fomentar el espíritu de equipo y el desarrollo profesional. Además, la empresa valora el bienestar de sus empleados, ofreciendo horarios flexibles y promoviendo un equilibrio saludable entre la vida laboral y personal.

Aunque el entorno de trabajo remoto ofrece numerosas ventajas, también presenta desafíos específicos, especialmente en lo que respecta a la seguridad de la información. Entre estos desafíos se incluyen:

- **Gestión de accesos remotos:** Garantizar que solo los empleados autorizados tengan acceso a los sistemas y datos críticos de la empresa, y que este acceso sea seguro y monitoreado.
- **Protección de datos en dispositivos personales:** Asegurar que los datos corporativos no se vean comprometidos en dispositivos personales que los empleados utilizan para trabajar remotamente.
- **Mantenimiento de la cohesión del equipo:** Asegurar una comunicación efectiva y un sentido de pertenencia entre los empleados, a pesar de la falta de interacción cara a cara.

InnovaTech Consulting ha abordado estos desafíos mediante la implementación de controles de seguridad rigurosos y el fomento de una cultura organizativa fuerte que apoya a los empleados en un entorno de trabajo distribuido.

4.1.7. Infraestructura en la nube.

A pesar de mantener provisionalmente una infraestructura mínima con un servidor físico de manera temporal (CPD), se puede afirmar que **InnovaTech Consulting** basa su operación en una infraestructura completamente alojada en la nube, lo que le permite gestionar de manera eficiente sus servicios digitales y soportar su entorno de trabajo remoto. Esta decisión estratégica ha sido clave para la empresa, dado su enfoque en la flexibilidad, escalabilidad y seguridad, características esenciales para una organización que opera en un entorno digital global.

La infraestructura en la nube de **InnovaTech Consulting** está contratada a un proveedor líder en servicios de nube como es AZURE de Microsoft, reconocido por su fiabilidad y capacidad para manejar entornos empresariales críticos. Esta infraestructura

ofrece una serie de características clave que son fundamentales para las operaciones de la empresa:

1. **Escalabilidad y flexibilidad:**
    - La nube permite a **InnovaTech Consulting** escalar sus recursos tecnológicos de acuerdo con las necesidades del negocio. Esto significa que la empresa puede aumentar o reducir su capacidad de almacenamiento, procesamiento y ancho de banda en función de la demanda, sin la necesidad de inversiones en hardware físico. Esta flexibilidad es especialmente útil durante los picos de actividad o cuando se lanzan nuevos proyectos que requieren mayor capacidad computacional.
2. **Alta disponibilidad y resiliencia:**
    - La infraestructura en la nube garantiza que los servicios de **InnovaTech Consulting** estén disponibles para sus empleados y clientes en todo momento. El proveedor de servicios en la nube ofrece redundancia geográfica, lo que significa que los datos y aplicaciones de la empresa están replicados en múltiples centros de datos alrededor del mundo. Esto asegura que, en caso de una falla en un centro de datos, los servicios puedan continuar sin interrupciones desde otra ubicación.
3. **Seguridad avanzada:**
    - La seguridad es un pilar fundamental de la infraestructura en la nube de **InnovaTech Consulting**. El proveedor de la nube implementa medidas de seguridad de última generación, como la encriptación de datos tanto en tránsito como en reposo, autenticación multifactor (MFA) para el acceso a los sistemas, y monitorización en continuo de amenazas y vulnerabilidades. Además, la nube ofrece capacidades avanzadas de control de acceso y segmentación de red, lo que permite a la empresa aislar y proteger los datos sensibles.
4. **Cumplimiento normativo:**
    - La infraestructura en la nube cumple con las normativas internacionales de seguridad y privacidad, lo que facilita a **InnovaTech Consulting** el cumplimiento de sus propios compromisos legales y regulatorios. Esto incluye el cumplimiento con normas como el GDPR para la protección de datos personales y otras regulaciones específicas del sector en el que operan los clientes de la empresa.

5. **Gestión y automatización:**
    - La nube permite a **InnovaTech Consulting** automatizar gran parte de la gestión de su infraestructura, desde la implementación de nuevos recursos hasta la aplicación de actualizaciones y parches de seguridad. Esto no solo reduce la carga operativa sobre el equipo de TI, sino que también minimiza el riesgo de errores humanos, aumentando la eficiencia y la seguridad de las operaciones.

El uso de una infraestructura en la nube proporciona a **InnovaTech Consulting** varios beneficios estratégicos:

- **Reducción de Costos Operativos:** Al no necesitar inversiones en hardware ni en su mantenimiento, la empresa puede destinar más recursos a la innovación y el desarrollo de nuevos servicios.
- **Agilidad en la Innovación:** La capacidad de desplegar nuevos servicios y aplicaciones de manera rápida permite a **InnovaTech Consulting** mantenerse competitivo en un mercado en constante evolución.
- **Protección de Datos:** Con medidas de seguridad avanzadas y cumplimiento normativo, la empresa asegura la confidencialidad, integridad y disponibilidad de los datos, tanto propios como de sus clientes.
- **Accesibilidad Global:** La nube permite que los empleados y clientes de **InnovaTech Consulting** accedan a los servicios y recursos desde cualquier lugar del mundo, en cualquier momento, facilitando la colaboración y el soporte continuo.

Aunque la infraestructura en la nube ofrece numerosos beneficios, también presenta desafíos que **InnovaTech Consulting** debe gestionar cuidadosamente:

- **Gestión de la Seguridad en un entorno Multitenant:** Al compartir recursos con otras organizaciones en un entorno multitenant, la empresa debe asegurarse de que los datos estén completamente aislados y protegidos.
- **Dependencia del proveedor de servicios:** La empresa debe confiar en el proveedor de la nube para garantizar la disponibilidad y seguridad de sus servicios, lo que requiere una evaluación continua de la relación y las prácticas del proveedor.

- **Latencia y rendimiento:** En algunas ocasiones, la latencia o el rendimiento de la red pueden verse afectados por la distancia física a los centros de datos, lo que puede impactar la experiencia del usuario.

InnovaTech Consulting aborda estos desafíos mediante la implementación de políticas de seguridad rigurosas, la elección de un proveedor de nube de confianza y la monitorización constante del rendimiento de la infraestructura, asegurando así que los beneficios de la nube se maximicen mientras se mitigan los riesgos.

4.2. Definición del alcance del SGSI.

La definición del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) en **InnovaTech Consulting** es un proceso esencial para garantizar que los esfuerzos de implementación de la norma ISO 27001 se enfoquen en las áreas críticas de la organización, que son fundamentales para proteger la información sensible y asegurar la continuidad del negocio. Este proceso de definición del alcance abarca tanto la identificación de los límites del SGSI como la determinación de los activos, procesos y áreas críticas que serán incluidos en el sistema de gestión.

El alcance del SGSI en **InnovaTech Consulting** ha sido deliberadamente delimitado para centrarse en los componentes más relevantes y de impacto significativo para la seguridad de la información, especialmente considerando el entorno de trabajo remoto y la infraestructura basada en la nube. Esto permite una implementación efectiva y orientada a resultados, que aborda las necesidades específicas de la organización sin dispersar recursos en áreas de menor relevancia.

4.2.1. Descripción de los límites y aplicabilidad del SGSI en la empresa.

El SGSI de **InnovaTech Consulting** ha sido diseñado para abarcar todas las operaciones que tienen un impacto directo o indirecto en la seguridad de la información. Dado que la empresa opera en un entorno distribuido y digital, con una infraestructura basada en la nube, es esencial establecer límites claros y un marco de aplicabilidad que cubra tanto las actividades internas como las interacciones con clientes y terceros.

1. **Ámbito geográfico:**
    - **Globalidad del entorno operacional:** El entorno operativo de **InnovaTech Consulting** es global debido a su modelo de trabajo remoto. El SGSI abarca todas las ubicaciones desde las cuales operan los empleados y colaboradores, sin importar su ubicación geográfica. Esto incluye tanto las residencias particulares de los empleados como cualquier otro espacio desde donde se

accede a los sistemas de la empresa. Además, se incluyen las ubicaciones de los centros de datos de los proveedores de nube donde se alojan los sistemas de la empresa.

- **Impacto de la movilidad:** La movilidad es una característica inherente al modelo de trabajo remoto, lo que significa que los empleados pueden acceder a los sistemas de la empresa desde diversos dispositivos y ubicaciones. El SGSI debe abordar las implicaciones de esta movilidad, asegurando que se mantengan los mismos estándares de seguridad, independientemente de dónde se acceda a la información.

2. **Ámbito funcional:**
    - **Cobertura Integral de Procesos:** El SGSI cubre todos los procesos relacionados con la gestión de la seguridad de la información, que incluyen la evaluación de riesgos, la implementación de controles de seguridad, la gestión de incidentes, y la continuidad del negocio. También incluye procesos de soporte como la administración de la infraestructura en la nube, la gestión de recursos humanos en relación con la seguridad, y la gestión de las relaciones con proveedores y terceros.
    - **Incorporación de funciones transversales:** Dado que la seguridad de la información es un aspecto transversal en la operación de **InnovaTech Consulting**, el SGSI también abarca funciones como la formación y concienciación en seguridad para todos los empleados, asegurando que el personal entienda y cumpla con las políticas de seguridad establecidas.
3. **Ámbito de aplicabilidad:**
    - **Aplicabilidad a toda la organización:** El SGSI es aplicable a todos los niveles de la organización, incluyendo empleados, contratistas, y cualquier tercero que tenga acceso a los sistemas o datos de **InnovaTech Consulting**. Esto asegura una cobertura completa y coherente en la aplicación de controles de seguridad.
    - **Cobertura de dispositivos y sistemas:** La aplicabilidad del SGSI se extiende a todos los dispositivos, tanto corporativos como personales, que son utilizados para acceder a los sistemas de la empresa. Esto incluye computadoras portátiles, dispositivos móviles, y cualquier otro equipo que se conecte a la red de la empresa o a sus aplicaciones en la nube.
4. **Interacción con proveedores y terceros:**

- **Proveedores de servicios en la nube:** El SGSI abarca la interacción con proveedores de servicios en la nube, quienes desempeñan un papel crucial en la gestión y seguridad de los sistemas y datos de la empresa. Se incluyen en el alcance los acuerdos de nivel de servicio (SLA) y las políticas de seguridad que estos proveedores deben cumplir.
- **Subcontratistas y socios comerciales:** Además de los proveedores de nube, el SGSI incluye a todos los subcontratistas y socios comerciales que manejan información sensible o que tienen acceso a los sistemas de **InnovaTech Consulting**. Esto asegura que se apliquen los mismos estándares de seguridad y protección de datos a lo largo de toda la cadena de suministro.

4.2.2. Identificación de activos, procesos y áreas críticas incluidas en el alcance.

La identificación de los activos, procesos y áreas críticas es un paso esencial en la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en **InnovaTech Consulting**. Este proceso permite asegurar que todos los elementos fundamentales para la operación y la seguridad de la información estén adecuadamente protegidos y gestionados bajo el marco de la norma ISO 27001. La identificación se basa en un análisis detallado de las operaciones de la empresa, considerando el entorno tecnológico, la naturaleza de los datos manejados, y las interacciones entre diferentes procesos y sistemas:

1. Activos Críticos.

Los activos críticos son aquellos que, debido a su naturaleza y valor, requieren un nivel de protección elevado para garantizar la confidencialidad, integridad y disponibilidad de la información. En **InnovaTech Consulting**, se han identificado los siguientes activos como críticos dentro del SGSI:

- **Datos de Clientes:**
  - **Descripción:** Los datos confidenciales proporcionados por los clientes, que incluyen información sobre proyectos, datos financieros, evaluaciones de riesgos y otros documentos sensibles, son considerados como uno de los activos más valiosos de **InnovaTech Consulting**. Estos datos se encuentran almacenados y procesados en la plataforma digital de la empresa y están sujetos a estrictas normativas de protección de datos.
  - **Justificación de la criticidad:** La pérdida, alteración o acceso no autorizado a estos datos podría tener consecuencias graves, incluyendo pérdida de

confianza por parte de los clientes, daño a la reputación de la empresa y posibles sanciones legales. Por tanto, es vital asegurar que estos datos estén adecuadamente protegidos mediante controles de acceso, encriptación y auditorías regulares.

- **Documentación interna:**
    - **Descripción:** Incluye políticas de seguridad, procedimientos operativos, planes de continuidad del negocio, registros de auditorías, y otros documentos estratégicos que guían las operaciones de **InnovaTech Consulting**. Esta documentación es fundamental para el cumplimiento normativo y para la gestión interna de la seguridad de la información.
    - **Justificación de la Criticidad:** La integridad y disponibilidad de esta documentación son esenciales para mantener la operación segura de la empresa. Cualquier alteración o pérdida de estos documentos podría comprometer la capacidad de **InnovaTech Consulting** para gestionar incidentes de seguridad, cumplir con las normativas y operar de manera efectiva.
- **Plataforma Digital:**
    - **Descripción:** La plataforma digital desarrollada por **InnovaTech Consulting** es el núcleo de su operación. Incluye aplicaciones y servicios que son utilizados tanto internamente como por los clientes para gestionar proyectos, analizar datos y automatizar procesos.
    - **Justificación de la criticidad:** La disponibilidad y seguridad de la plataforma digital son esenciales para la continuidad del negocio. Cualquier fallo en esta plataforma podría afectar la prestación de servicios a los clientes y poner en riesgo la seguridad de la información procesada a través de ella.
- **Sistemas en la Nube:**
    - **Descripción:** Los sistemas alojados en la nube, especialmente en Microsoft Azure, soportan la infraestructura tecnológica de **InnovaTech Consulting**. Estos sistemas incluyen servidores, bases de datos, aplicaciones y servicios que son críticos para las operaciones diarias.
    - **Justificación de la criticidad:** Dado que la empresa opera en un entorno de trabajo remoto, la infraestructura en la nube es vital para la conectividad y la

gestión de datos. La protección de estos sistemas contra ciberataques, interrupciones del servicio y accesos no autorizados es crucial para mantener la operación segura y eficiente.

2. Procesos críticos.

Los procesos críticos son aquellos que tienen un impacto directo en la seguridad de la información y en la operación de **InnovaTech Consulting**. Estos procesos son esenciales para la gestión efectiva del SGSI y para asegurar que se cumplan los requisitos de la norma ISO 27001:

- **Evaluación de Riesgos y Gestión de la Seguridad de la Información:**
  - **Descripción:** Este proceso incluye la identificación y análisis de amenazas, vulnerabilidades y riesgos que pueden afectar a los activos críticos de la empresa. También abarca la implementación de controles de seguridad que mitigan estos riesgos y aseguran que los activos estén protegidos.
  - **Importancia:** La evaluación de riesgos es el fundamento sobre el cual se construye todo el SGSI. Permite a la empresa priorizar los recursos y esfuerzos en las áreas que presentan mayores riesgos, garantizando una protección efectiva de la información crítica.
- **Gestión de Accesos:**
  - **Descripción:** Este proceso se centra en la administración de los derechos de acceso a los sistemas y datos de la empresa. Incluye la gestión de identidades de usuarios, la autenticación multifactor, y la asignación y revisión periódica de permisos de acceso.
  - **Importancia:** La gestión adecuada de los accesos es fundamental para prevenir accesos no autorizados y proteger la confidencialidad e integridad de la información. Un control deficiente de los accesos puede dar lugar a brechas de seguridad significativas.
- **Automatización en Azure:**
  - **Descripción:** Este proceso involucra la implementación y gestión de soluciones automatizadas en la plataforma de Microsoft Azure para facilitar la monitorización continua, la respuesta a incidentes y la aplicación de políticas de seguridad.

- **Importancia:** La automatización en Azure permite a **InnovaTech Consulting** gestionar la seguridad de manera proactiva y eficiente, asegurando una respuesta rápida ante cualquier incidente y minimizando el riesgo de errores humanos.

3. Áreas Críticas.

Las áreas críticas identificadas son aquellas que requieren una atención particular dentro del SGSI debido a su impacto potencial en la seguridad de la información y en la continuidad del negocio:

- **Infraestructura en la Nube:**
  - **Descripción:** La infraestructura tecnológica alojada en Microsoft Azure es una de las áreas más críticas para **InnovaTech Consulting**. Esta infraestructura incluye todos los servidores, aplicaciones y bases de datos que soportan la operación de la empresa.
  - **Importancia:** La dependencia de la nube para todas las operaciones significa que cualquier vulnerabilidad o fallo en esta área podría tener un impacto devastador en la disponibilidad y seguridad de la información. La gestión adecuada de esta infraestructura es esencial para el éxito del SGSI.
- **Plan de Continuidad de Negocio:**
  - **Descripción:** El plan de continuidad de negocio es una estrategia integral que garantiza que **InnovaTech Consulting** pueda mantener sus operaciones críticas en caso de interrupciones o desastres. Incluye procedimientos de recuperación ante desastres, planes de contingencia, y la preparación de los empleados para manejar situaciones de emergencia.
  - **Importancia:** La continuidad del negocio es crucial para asegurar que la empresa pueda operar sin interrupciones significativas, incluso en situaciones adversas. Un plan sólido y bien gestionado es clave para mantener la confianza de los clientes y la estabilidad operativa.

4.3. Fases de Implementación de la ISO 27001.

La implementación de la norma ISO 27001 en **InnovaTech Consulting** se ha llevado a cabo mediante un enfoque estructurado y detallado, que asegura la cobertura completa de los aspectos críticos de la seguridad de la información dentro de la organización. Este proceso

se ha dividido en varias fases, cada una de las cuales se enfoca en un componente clave del Sistema de Gestión de la Seguridad de la Información (SGSI). Estas fases han sido diseñadas para garantizar que la empresa cumpla con los requisitos de la ISO 27001 y proteja eficazmente su información crítica en un entorno digital distribuido y basado en la nube.

Como ya se comentó en los apartados 1.3.1. y 1.3.2. “Alcance y Limitaciones del Trabajo”, el alcance del presente Trabajo Fin de Grado ha sido cuidadosamente delimitado para enfocarse en aquellos elementos del Sistema de Gestión de la Seguridad de la Información (SGSI) que son considerados críticos desde un punto de vista técnico y estratégico en el contexto de **InnovaTech Consulting**. Este enfoque ha guiado las decisiones metodológicas tomadas durante la implementación, garantizando que los recursos se concentren en áreas donde el impacto y el valor añadido son mayores.

Así las cosas, en este TFG se ha priorizado el desarrollo práctico de los siguientes componentes de la norma ISO 27001:

- Evaluación de Riesgos y Plan de Acción.
- Objetivos e Indicadores de Seguridad.
- Declaración de Aplicabilidad (SOA).
- Automatización en Microsoft Azure.
- Plan de Continuidad de Negocio.
- Política de Seguridad de la Información.

Aunque la norma ISO 27001 abarca un amplio espectro de controles y requisitos, este trabajo no aborda todos sus componentes. Se han excluido deliberadamente ciertos requisitos y fases de implementación que, aunque importantes, no se consideran dentro del alcance práctico de este proyecto. Estas exclusiones incluyen, pero no se limitan a:

- Gestión completa de recursos humanos en relación con la seguridad.
- Revisión y auditoría completa del SGSI más allá de lo implementado.
- Control interno y gobernanza en su totalidad.

La decisión de acotar el alcance del trabajo responde a la necesidad de abordar con mayor profundidad los aspectos más relevantes y de impacto directo en la operación de la empresa, asegurando la calidad y aplicabilidad de los resultados obtenidos. Las limitaciones de tiempo y recursos inherentes a un proyecto de fin de grado también influyeron en esta decisión.

Este enfoque metodológico, aunque acotado, proporciona una base sólida y replicable para la implementación de un SGSI en un entorno similar, garantizando que los elementos clave sean gestionados con el rigor y la atención que requiere la norma ISO 27001.

Por tanto, las fases de implementación abarcan desde la identificación y gestión de riesgos hasta la automatización de procesos en la nube, pasando por el desarrollo de políticas de seguridad y la planificación de la continuidad del negocio. Cada fase ha sido cuidadosamente planificada y ejecutada para asegurar que el SGSI no solo cumpla con las normas, sino que también sea práctico, eficiente y adaptable a las necesidades específicas de **InnovaTech Consulting**.

En los siguientes apartados, se detallará cada una de estas fases, destacando los procedimientos, herramientas y resultados obtenidos durante la implementación.

4.3.1. Evaluación de Riesgos (Cláusula 6.1.2).

La evaluación de riesgos es un componente esencial en la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001. Para **InnovaTech Consulting**, se ha seleccionado la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) como la herramienta principal para llevar a cabo esta evaluación.

MAGERIT es una metodología desarrollada por el Consejo Superior de Administración Electrónica de España, ampliamente utilizada en organizaciones que requieren un análisis riguroso y detallado de los riesgos relacionados con la seguridad de la información. Esta metodología es especialmente adecuada para entornos en los que la gestión de riesgos debe ser sistemática, documentada y alineada con las mejores prácticas internacionales.

El uso de MAGERIT en **InnovaTech Consulting** permite no solo identificar y analizar los riesgos que podrían comprometer la seguridad de la información, sino también priorizar las medidas de mitigación en función de su impacto y probabilidad. Esta metodología proporciona un marco estructurado que abarca desde la identificación de activos y la valoración de riesgos hasta la definición de un plan de acción para mitigar los riesgos identificados.

En el contexto de este TFG, la aplicación de MAGERIT se centra en los siguientes objetivos:

- **Identificar y catalogar los activos de información críticos** de **InnovaTech Consulting**.

- **Analizar las amenazas y vulnerabilidades** que afectan a estos activos, evaluando los riesgos asociados en términos de probabilidad e impacto.
- **Priorizar los riesgos** según su nivel de criticidad, asegurando que los recursos se asignen de manera efectiva para proteger la información más sensible.
- **Desarrollar un plan de acción** específico que establezca las medidas de mitigación necesarias para reducir los riesgos a niveles aceptables.

En los siguientes apartados, se detallará cómo se ha llevado a cabo la evaluación de riesgos utilizando MAGERIT, destacando los pasos seguidos, las herramientas empleadas y los resultados obtenidos en el contexto de **InnovaTech Consulting**.

4.3.1.1. Identificación y valoración de Activos.

Siguiendo el marco de la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo con la metodología establecida el primer paso es el de la identificación y valoración de los activos. Esta operación constituye una parte crítica para garantizar que todos los elementos que sustentan la operación de la empresa estén adecuadamente protegidos y se ha realizado, a su vez, siguiendo las siguientes fases:

4.3.1.1.1. Proceso de identificación de Activos.

La primera etapa en la evaluación de riesgos consiste en la identificación exhaustiva de todos los activos de información de **InnovaTech Consulting**. Los activos se clasificaron en varias categorías clave, que reflejan las áreas críticas de la organización:

1. **Equipos:** Incluyen dispositivos físicos como ordenadores, tabletas, smartphones, y otros equipos que manejan o almacenan información sensible.
2. **Aplicaciones:** Software utilizado para la gestión de información crítica, desarrollo de proyectos, y otras actividades esenciales.
3. **Servidores:** Infraestructura de servidores, tanto físicos como virtuales, que soportan la operación de las aplicaciones y el almacenamiento de datos.
4. **Telefonía Fija:** Dispositivos de comunicación que forman parte de la infraestructura de soporte.
5. **Personas:** Perfiles de usuarios, empleados, y roles clave dentro de la organización, que interactúan con los sistemas y manejan información sensible.

6. **Servicios:** Servicios internos y externos que proporcionan soporte a la operación diaria de la empresa, incluyendo la gestión comercial, administración, y atención al cliente.
7. **Instalaciones:** Infraestructura física, como oficinas y centros de datos, que alojan activos de información o proporcionan soporte a la operación.

4.3.1.1.2. Valoración de Activos.

Para cada activo identificado, se realizó una valoración basada en tres criterios fundamentales: **Disponibilidad, Confidencialidad, e Integridad**.

a) **DISPONIBILIDAD:** Evalúa la importancia de que el activo esté disponible para su uso en el momento requerido.

A continuación, se expone la **tabla 1** de criterios de evaluación para justificar el nivel de "Disponibilidad" de los activos en función de su impacto en la empresa y su criticidad operativa. Esta tabla te servirá como referencia para justificar por qué un activo se clasifica con una determinada puntuación de disponibilidad en una escala del 1 al 5.

Tabla 8: Criterios de evaluación para justificar el nivel de "Disponibilidad" de los activos.

Nivel de Disponibilidad	Criterio de Evaluación	Descripción del Impacto
1 - Bajo	El activo no es crítico para la operación diaria, su falta de disponibilidad no afecta significativamente a la continuidad del negocio.	El activo puede estar fuera de servicio durante largos periodos (días o semanas) sin afectar gravemente las operaciones o productividad de la empresa.
2 - Medio (-)	El activo es importante pero su inactividad puede ser tolerada por periodos limitados (horas o hasta un día) sin grandes impactos.	La falta de disponibilidad puede generar ciertas ineficiencias, pero existen mecanismos o recursos alternativos que permiten la continuidad operativa.
3 - Medio (+)	El activo es importante para la operación diaria, pero la empresa puede tolerar su inactividad durante un corto periodo (horas).	La falta de disponibilidad causa inconvenientes y pérdida de productividad, pero no detiene las operaciones críticas si se soluciona rápidamente.
4 - Alto	El activo es crucial para el funcionamiento de varios procesos de negocio, su inactividad causa interrupciones significativas.	La falta de disponibilidad del activo por periodos cortos (horas) afecta seriamente la productividad, generando pérdidas de eficiencia y posibles retrasos.
5 - Crítico	El activo es vital para las operaciones de la empresa, su inactividad implica la paralización completa o casi completa del negocio.	La falta de disponibilidad incluso por periodos cortos (minutos) genera graves problemas operativos y financieros, afectando a procesos críticos.

Con más detalle, se puede afirmar lo siguiente:

- **Nivel 1 (Bajo):** Este nivel se aplica a activos que no afectan directamente la operación crítica de la empresa. Por ejemplo, periféricos no esenciales como impresoras

secundarias o equipos usados esporádicamente. La organización puede continuar su operación sin el activo por un tiempo considerable sin efectos adversos importantes.

- **Nivel 2 (Medio -):** Activos que son útiles para el día a día, pero cuya falta no interrumpe significativamente las funciones principales. Por ejemplo, dispositivos que se usan para tareas administrativas de bajo impacto o software no crítico que puede ser reemplazado temporalmente.
- **Nivel 3 (Medio +):** Activos que son necesarios para las operaciones diarias pero que pueden estar inactivos durante algunas horas sin una gran afectación. Un ejemplo serían ordenadores de empleados que no están directamente relacionados con funciones críticas, pero que son necesarios para la productividad general.
- **Nivel 4 (Alto):** Se refiere a activos que afectan a varios procesos de negocio o a departamentos clave. Su inactividad por más de unas horas generaría pérdidas en productividad y posiblemente retrasos en los proyectos o servicios ofrecidos. Por ejemplo, un servidor de aplicaciones de uso común.
- **Nivel 5 (Crítico):** Este nivel aplica a activos cuya disponibilidad es absolutamente esencial para la operación del negocio. Su inactividad implica una parada total o casi total de las operaciones. Un ejemplo claro serían los servidores que gestionan la infraestructura digital de la empresa, como bases de datos o sistemas de producción en tiempo real.

Como ejemplo de Aplicación, si se está evaluando un **servidor que aloja una base de datos** crítica para la operación de la empresa, este activo podría tener una **disponibilidad de 5 (Crítico)** porque su inactividad incluso durante unos minutos podría paralizar la operación. Así mismo, un **ordenador de un empleado administrativo** podría tener una **disponibilidad de 2 (Medio -)** si su falta de uso no afecta directamente la continuidad de procesos clave y puede ser sustituido temporalmente.

b) **CONFIDENCIALIDAD:** Mide la necesidad de proteger el acceso a la información contenida en el activo contra accesos no autorizados.

A continuación, se presenta la **Tabla 2** de criterios de evaluación para la **Confidencialidad** de los activos, que permitirá justificar por qué un activo se clasifica en un determinado nivel de confidencialidad en una escala del 1 al 5.

Tabla 9: Criterios de evaluación para la Confidencialidad de los activos.

Nivel de Confidencialidad	Criterio de Evaluación	Descripción del Impacto
1 - Bajo	El acceso no autorizado al activo tiene un impacto insignificante o nulo.	La información contenida en el activo no es sensible ni confidencial, y su divulgación no genera ningún riesgo o daño para la organización.
2 - Medio (-)	El acceso no autorizado al activo puede causar molestias menores, pero no tiene un impacto significativo.	La información es de baja sensibilidad, y aunque su divulgación no es ideal, no compromete gravemente los intereses de la organización.
3 - Medio (+)	El acceso no autorizado al activo puede causar inconvenientes y posibles impactos en áreas no críticas de la organización.	La información es algo sensible, y su divulgación podría generar cierto nivel de impacto, aunque no comprometería los activos críticos.
4 - Alto	El acceso no autorizado al activo comprometería información sensible y tendría un impacto significativo en la organización.	La información es confidencial y su divulgación causaría daños importantes, afectando la competitividad, reputación o el cumplimiento legal.
5 - Crítico	El acceso no autorizado al activo tendría consecuencias graves o catastróficas para la organización.	La información es extremadamente sensible (p.ej. datos personales, financieros, propiedad intelectual) y su divulgación tendría consecuencias legales o financieras graves.

Se describen a continuación de forma más explícita los impactos:

- **Nivel 1 (Bajo):** La información contenida en el activo es pública o de baja sensibilidad. Su acceso no autorizado no genera ninguna amenaza significativa para la organización. Un ejemplo podría ser documentos informativos o material de marketing público.
- **Nivel 2 (Medio -):** La información contenida es de baja sensibilidad, como datos operativos internos que, si bien preferiblemente no deben divulgarse, no causarían un daño considerable si son accedidos por terceros. Por ejemplo, información sobre procedimientos administrativos no críticos.
- **Nivel 3 (Medio +):** La información es algo sensible y podría afectar negativamente a la organización si es divulgada. Un ejemplo sería información interna relacionada con presupuestos o reportes financieros preliminares que, si se acceden, podrían causar inconvenientes a la empresa.
- **Nivel 4 (Alto):** El activo contiene información sensible, como datos de clientes o proyectos confidenciales. Su divulgación a personas no autorizadas podría tener un impacto significativo en la empresa, afectando la reputación, la confianza de los clientes o resultando en pérdidas financieras.
- **Nivel 5 (Crítico):** El activo contiene información extremadamente sensible, como datos personales protegidos por la ley (p.ej., RGPD), propiedad intelectual crítica o información financiera vital. El acceso no autorizado a estos datos resultaría en graves problemas legales, sanciones regulatorias o daños financieros importantes.

A modo de ejemplo, un **servidor que almacena datos personales de clientes** tendría una **confidencialidad de 5 (Crítico)**, ya que su acceso no autorizado podría causar graves problemas legales, sanciones por incumplimiento normativo y pérdida de confianza por parte de los clientes. Por otro lado, un **documento público de marketing** podría tener una **confidencialidad de 1 (Bajo)**, ya que su divulgación no tendría impacto alguno, pues está destinado para el acceso público. Igualmente, un **reporte financiero preliminar** podría tener una **confidencialidad de 3 (Medio +)**, ya que su divulgación causaría algunos problemas operativos o financieros menores.

c) **INTEGRIDAD:** Considera la necesidad de proteger la exactitud y completitud de la información contenida en el activo.

La **Tabla 3** permitirá justificar el nivel de integridad asignado a un activo en una escala del 1 al 5.

Tabla 10: Nivel de integridad asignado a un activo.

Nivel de Integridad	Criterio de Evaluación	Descripción del Impacto
1 - Bajo	La exactitud o completitud de la información contenida en el activo tiene poca o ninguna relevancia para la organización.	La corrupción o modificación de la información contenida en el activo no afectaría significativamente el funcionamiento o decisiones.
2 - Medio (-)	La exactitud o completitud de la información es deseable pero no crítica.	La información puede contener errores menores o modificaciones sin que afecte significativamente la operación, aunque es preferible evitarlo.
3 - Medio (+)	La exactitud y completitud de la información es importante, aunque un pequeño error o modificación podría ser corregido fácilmente.	Los errores en la información pueden causar inconvenientes, pero pueden ser identificados y corregidos sin gran impacto en el funcionamiento.
4 - Alto	La exactitud y completitud de la información es crucial para la operación, cualquier error puede tener un impacto significativo.	La corrupción o modificación no detectada podría tener efectos graves, como decisiones operativas incorrectas o afectación de la calidad del servicio.
5 - Crítico	La exactitud y completitud de la información es vital; cualquier error o modificación tendría consecuencias graves.	La corrupción o modificación no detectada podría llevar a pérdidas financieras, daños legales o graves impactos operativos.

De manera más detallada se puede abundar en la descripción de los impactos de la siguiente forma:

- **Nivel 1 (Bajo):** La integridad de la información no tiene relevancia para la organización. Los errores o modificaciones en el activo no tienen impacto significativo. Por ejemplo, una lista de contactos que puede ser fácilmente corregida o sustituida sin mayor esfuerzo o implicación para la empresa.

- **Nivel 2 (Medio -):** La exactitud y completitud son importantes, pero un error en la información no resultaría en impactos significativos. Ejemplo: Documentos administrativos internos que, si contienen errores, no impactan el core del negocio.
- **Nivel 3 (Medio +):** La exactitud y completitud de la información son necesarias para el correcto funcionamiento de las operaciones, pero errores menores pueden corregirse con algo de esfuerzo sin graves consecuencias. Ejemplo: Reportes operacionales o informes de actividad que son revisados y corregidos regularmente.
- **Nivel 4 (Alto):** La exactitud de la información es crítica para la toma de decisiones y la operativa de la empresa. Cualquier error o modificación no detectada podría generar decisiones incorrectas o ineficiencia. Ejemplo: Documentos financieros, reportes contables o datos de clientes, donde los errores impactan directamente la operación o la gestión financiera.
- **Nivel 5 (Crítico):** La exactitud y completitud de la información son absolutamente vitales, y cualquier error o corrupción podría tener consecuencias graves o catastróficas para la organización. Ejemplo: Datos médicos, sistemas financieros que gestionan grandes transacciones o documentación legal. Un error o modificación en este tipo de información podría generar sanciones legales, pérdidas económicas o incluso riesgo para la vida humana (en el caso de información médica).

Así, un sistema de facturación podría tener una **integridad de 5 (Crítico)**, ya que cualquier error en las cifras o en la información de pago podría generar serios problemas legales, financieros y de confianza con los clientes. Sin embargo, un **calendario de eventos públicos** podría tener una **integridad de 1 (Bajo)**, ya que los errores en fechas o eventos pueden ser fácilmente corregidos sin mayor impacto. Otro ejemplo es el de un **informe operativo diario** podría tener una **integridad de 3 (Medio +)**, ya que los errores menores pueden ser corregidos, pero no afectarán gravemente las decisiones a largo plazo, aunque pueden causar inconvenientes.

Así pues, en la práctica, la valoración de cada activo se obtuvo calculando la media aritmética de las puntuaciones asignadas a estos tres criterios. Esta media se utilizó para determinar la criticidad del activo, lo que permite priorizar los esfuerzos de protección.

4.3.1.1.3. Tratamiento de Activos críticos.

Según los criterios establecidos, se consideran críticos aquellos activos que presentan una valoración media superior a 3. Estos activos fueron destacados y marcados en rojo en el análisis para indicar que requieren un tratamiento especial. Estos activos son aquellos que, debido a su alta criticidad, demandan una atención prioritaria en la implementación de controles de seguridad y en la planificación de medidas de mitigación de riesgos.

4.3.1.2. Identificación de Amenazas y Vulnerabilidades.

La identificación de amenazas y vulnerabilidades permite a **InnovaTech Consulting** comprender mejor los riesgos a los que están expuestos sus activos de información. Este proceso, ha permitido identificar y catalogar las posibles amenazas y vulnerabilidades que podrían afectar negativamente la confidencialidad, integridad, y disponibilidad de los activos críticos de la empresa.

4.3.1.2.1. Metodología de identificación.

El análisis se ha basado en una clasificación sistemática de los activos, agrupándolos en las siguientes categorías:

1. **Servidores.**
2. **Equipos.**
3. **Aplicaciones** (como herramientas de desarrollo de código, gestores de bases de datos, control de versiones y gestores de ficheros).
4. **Servicios** (en particular, los relacionados con la prestación de servicios con el software NormaPro de desarrollo propio de **InnovaTech Consulting**).

Para cada categoría, se identificaron amenazas y vulnerabilidades, clasificadas en cuatro grandes grupos:

- Desastres naturales.
- De origen industrial.
- Errores y fallos no intencionados.
- Ataques intencionados.

Como se verá más adelante, en la **Tabla 2** correspondiente se destacan en rojo aquellas amenazas y vulnerabilidades que se consideran más probables y que, por lo tanto, requieren una mayor atención en la gestión del riesgo.

Desastres naturales.

Las amenazas naturales, como incendios y daños por agua, son riesgos que pueden afectar significativamente tanto a los servidores como a los equipos y las instalaciones de **InnovaTech Consulting**. Estas amenazas son difíciles de predecir, pero tienen un impacto potencialmente devastador. La **Tabla 2** indica que todos los activos mencionados están expuestos a estos riesgos, especialmente los servidores y los servicios críticos:

Amenazas de origen industrial.

Las amenazas de origen industrial incluyen eventos como contaminación electromagnética, fallos en el suministro eléctrico, y averías de origen físico o lógico. Estos riesgos son particularmente relevantes para los servidores y equipos, ya que pueden afectar gravemente la operatividad y la integridad de los datos almacenados. En la tabla 2, se destaca que todos los activos están expuestos a estos riesgos, con especial énfasis en las condiciones inadecuadas de temperatura y humedad que pueden afectar a los equipos y servidores.

Errores y fallos no intencionados.

Los errores y fallos no intencionados abarcan una amplia gama de vulnerabilidades, desde errores de usuario y administrador hasta fallos en la configuración de software y hardware. Este tipo de amenazas son comunes en cualquier entorno de TI y pueden provocar fugas de información, destrucción accidental de datos, y caídas del sistema. Igualmente, la tabla 2 muestra que todos los activos están expuestos a estos riesgos, especialmente los sistemas de gestión de bases de datos y las aplicaciones críticas para el desarrollo de software.

Ataques intencionados.

Los ataques intencionados representan una de las amenazas más graves para la seguridad de la información en **InnovaTech Consulting**. Estos incluyen manipulaciones de registros y configuraciones, suplantación de identidad, difusión de software dañino, y accesos no autorizados. Las aplicaciones críticas y los servidores son particularmente vulnerables a estos tipos de ataques, que podrían comprometer gravemente la confidencialidad y la integridad de la información gestionada por la empresa.

Resultados de la identificación.

El análisis realizado ha permitido destacar las amenazas y vulnerabilidades más probables para cada tipo de activo, marcadas en rojo en la tabla. Estos riesgos requieren una atención prioritaria en la fase de gestión de riesgos, donde se desarrollarán e implementarán las medidas de mitigación necesarias para proteger los activos críticos de la empresa.

La identificación de estas amenazas y vulnerabilidades es un paso esencial para la planificación de las medidas de seguridad que aseguren la resiliencia de los sistemas y servicios de **InnovaTech Consulting** frente a los riesgos identificados.

Las medidas de mitigación priorizadas deben enfocarse en proteger contra las amenazas identificadas como más probables y de mayor impacto, incluyendo la protección

física de instalaciones, la seguridad informática, y la capacitación del personal. Implementar estas medidas de manera proactiva ayudará a reducir significativamente los riesgos y a asegurar la resiliencia de **InnovaTech Consulting** frente a las amenazas identificadas.

4.3.1.3. Cálculo del Riesgo Real.

El cálculo del riesgo real es una etapa crítica en la gestión de riesgos dentro del Sistema de Gestión de la Seguridad de la Información (SGSI) de **InnovaTech Consulting**. Este proceso permite cuantificar los riesgos asociados a cada activo y priorizar las acciones de mitigación basadas en su nivel de criticidad. A continuación, se detalla la metodología seguida y los resultados obtenidos en esta fase.

El enfoque metodológico para el cálculo del riesgo real sigue un proceso riguroso y estructurado, basado en las mejores prácticas de la metodología MAGERIT:

1. **Identificación de Activos críticos:**
    - El primer paso consiste en identificar aquellos activos que han sido clasificados con un valor **ALTO** o **CRÍTICO** en la fase de valoración. Estos activos son los más relevantes para la operación y seguridad de la empresa, y por tanto, requieren una atención prioritaria.
2. **Asociación de Amenazas probables:**
    - A cada activo crítico se le asocian las amenazas previamente identificadas y consideradas como **probables**. Estas amenazas incluyen tanto eventos de origen natural e industrial como errores humanos y ataques intencionados. La probabilidad de ocurrencia de cada amenaza se evalúa en función de su historial y contexto específico en **InnovaTech Consulting**.
3. **Asignación de Probabilidad de ocurrencia:**
    - Para cada amenaza identificada, se asigna una **probabilidad de ocurrencia** en una escala de 1 a 5 según los criterios que muestra la **Tabla 4** siguiente:

Tabla 11: Tabla de Probabilidad de Ocurrencia de la Amenaza.

Nivel de Probabilidad	Criterios de Evaluación	Descripción del Nivel de Probabilidad
1 - Muy baja	Pocas o ninguna amenaza documentada en el pasado.	La amenaza identificada es extremadamente improbable y no hay historial de ocurrencias similares en la organización. Históricamente, no ha ocurrido esta amenaza en InnovaTech Consulting o en organizaciones similares, y es altamente improbable que ocurra en el futuro.
2 - Baja	Amenazas raras pero posibles.	La amenaza es poco frecuente, aunque puede ocurrir en casos excepcionales. La organización ha experimentado pocos eventos similares. Ha habido casos limitados de ocurrencias en el pasado, pero no es común que suceda. Se asocia con eventos aislados.
3 - Media	Amenazas que pueden ocurrir ocasionalmente.	La amenaza ha ocurrido en la organización o en contextos similares con cierta frecuencia, pero no es recurrente. Ha ocurrido ocasionalmente en la organización o en su industria. La probabilidad de que ocurra en el futuro es moderada.
4 - Alta	Amenazas con historial frecuente o condiciones que aumentan la probabilidad.	La amenaza es recurrente o las condiciones actuales aumentan la exposición del activo a dicha amenaza. Es probable que ocurra debido a las condiciones actuales o históricas. La organización tiene antecedentes de eventos similares.
5 - Muy alta	Amenaza prácticamente asegurada.	La amenaza ha ocurrido regularmente o es muy probable que ocurra en el futuro cercano dado el contexto del activo. Es casi seguro que ocurra. Las condiciones internas o externas indican un riesgo inminente y recurrente.

Esta valoración se basa en factores como la frecuencia de eventos similares en el pasado, la exposición del activo a la amenaza, y la efectividad de los controles actuales.

4. **Asignación de Impacto:**
    - A continuación, se evalúa el **impacto potencial** de la amenaza sobre el activo, utilizando la **Tabla 5** también en una escala de 1 a 5:

Tabla 12: Tabla de Impacto Potencial de la Amenaza sobre el Activo.

Nivel de Impacto	Criterios de Evaluación	Descripción del Nivel de Impacto
1 - Impacto bajo (-)	Consecuencias mínimas para la operación.	La amenaza tiene un impacto prácticamente insignificante sobre la operación, con consecuencias leves que pueden pasar desapercibidas. La amenaza tendría un impacto mínimo sobre el activo y sobre la operación de la empresa. Por ejemplo, pequeñas modificaciones en documentos internos sin mayor repercusión.
2 - Impacto bajo (+)	Consecuencias menores y manejables.	La amenaza podría causar leves interrupciones o inconvenientes, pero la operación puede continuar sin grandes dificultades. La amenaza podría causar inconvenientes menores, pero su impacto es manejable. Ejemplo: Pequeñas interrupciones en sistemas secundarios.
3 - Impacto medio (-)	Consecuencias moderadas, que requieren atención.	La amenaza provoca una interrupción en algunos procesos, afectando la operación o los servicios temporalmente. La amenaza podría generar una interrupción temporal o daños parciales que afectan a la operativa o a la calidad del servicio, pero se puede gestionar de forma relativamente rápida.
4 - Impacto medio (+)	Consecuencias significativas que requieren intervención.	La amenaza afecta gravemente la operación o algunos servicios, requiriendo acciones correctivas inmediatas para evitar daños mayores. El impacto de la amenaza es serio y requiere una intervención rápida para evitar mayores consecuencias. Ejemplo: Fallo temporal en servicios críticos para la empresa.
5 - Impacto alto	Consecuencias críticas y duraderas.	La amenaza tendría consecuencias catastróficas para la confidencialidad, integridad o disponibilidad de la información, con impactos financieros, reputacionales o legales graves. El impacto es catastrófico, afectando gravemente a la operación, la reputación o las finanzas de la empresa. Ejemplo: Pérdida total de datos críticos o paralización de operaciones claves.

Esta valoración considera las posibles consecuencias para la confidencialidad, integridad, y disponibilidad de la información, así como el impacto financiero, reputacional y operacional.

5. **Cálculo del Riesgo Real:**

   - El riesgo real se calcula utilizando la siguiente fórmula:

$$\text{Riesgo Real} = \frac{\text{Probabilidad de Ocurrencia} + \text{Impacto}}{2}$$

- Este cálculo proporciona un valor que representa la gravedad del riesgo asociado a la combinación de activo y amenaza. Los resultados se clasifican de la siguiente manera según se expone en la **Tabla 6** siguiente que integra todos los textos de cada nivel, proporcionando una descripción completa que permitirá justificar claramente la clasificación del riesgo real.

Tabla 13: Tabla de Clasificación del Riesgo Real.

Valor de Riesgo Real	Nivel de Riesgo	Descripción del Nivel de Riesgo
1	Riesgo Bajo (-)	**El riesgo es considerado bajo y no se requiere intervención inmediata. Los controles actuales son suficientes para mitigar las amenazas sin un impacto significativo.** Este nivel indica un riesgo muy bajo, que no representa una amenaza para la operación de los activos. El sistema de seguridad actual es efectivo, y no se espera un impacto considerable. No se requiere acción inmediata, pero se puede realizar una revisión periódica.
2	Riesgo Bajo (+)	**El riesgo es todavía bajo, pero debe ser monitorizado. Aunque no requiere una acción inmediata, puede que se necesite ajustar algunos controles para mayor seguridad.** Este nivel implica que el riesgo sigue siendo bajo, pero debe vigilarse de cerca. Es posible que algunos controles existentes necesiten ser ajustados o reforzados, dependiendo de cómo evolucione el entorno de amenazas.
3	Riesgo Medio (-)	**El riesgo es moderado y podría causar problemas en ciertos activos. Se recomienda una revisión de los controles actuales para prevenir un impacto mayor.** Aquí se observa un riesgo moderado, que podría comprometer los activos si no se aborda correctamente. Se recomienda evaluar las medidas preventivas y, si es necesario, mejorar los controles de seguridad existentes para evitar posibles impactos.
4	Riesgo Medio (+)	**El riesgo es alto-moderado y requiere tratamiento. Los controles actuales no son totalmente efectivos y pueden necesitar mejoras para evitar posibles daños.** Este nivel representa un riesgo significativo que necesita ser tratado con prioridad. Aunque no es crítico, existe la posibilidad de que las amenazas se materialicen si no se implementan medidas adicionales. Una revisión completa de los controles es necesaria.
5	Riesgo Alto	**El riesgo es significativo y debe ser mitigado lo antes posible. Se debe implementar un plan de acción inmediato para reducir tanto la probabilidad como el impacto.** Este es el nivel más alto de riesgo, que probablemente causará impactos graves si no se aborda de inmediato. Las medidas correctivas deben implementarse de manera urgente para evitar daños significativos en la seguridad de la información o la operación de la empresa.

6. **Identificación de Riesgos No Aceptables:**
    - Los riesgos que resultan en una puntuación igual o superior a 3 se consideran **No Aceptables**. Estos riesgos requieren una atención prioritaria y la implementación de medidas de mitigación para reducirlos a un nivel aceptable.

4.3.1.4 Análisis del Riesgo.

En el contexto de la implementación de la norma ISO 27001, el análisis del riesgo es una fase crítica que permite identificar, evaluar y mitigar los riesgos asociados a los activos de la organización. En este caso, se ha seguido un enfoque sistemático utilizando la metodología MAGERIT, adaptada para evaluar los riesgos de seguridad de la información en los distintos activos de la empresa ficticia InnovaTech Consulting.

La metodología utilizada incluye los siguientes pasos clave:

1. **Identificación de Activos**: Se identificaron los activos clave de la organización, clasificados en cuatro categorías principales: Equipos, Aplicaciones, Servidores y Servicios. Cada activo fue descrito detalladamente, incluyendo su ubicación y el personal responsable.
2. **Identificación de Amenazas**: Para cada activo, se identificaron las amenazas potenciales, agrupadas en tres categorías: Desastres Naturales, Errores y Fallos No Intencionados, y Ataques Intencionados. Las amenazas incluyeron desde incendios y fallos eléctricos hasta accesos no autorizados y manipulación de registros.
3. **Evaluación del Riesgo**: Se asignó una probabilidad de ocurrencia y un impacto potencial a cada amenaza, ambos valores fueron calificados en una escala de 1 a 5. El cálculo del riesgo se realizó promediando estos dos valores.
4. **Determinación del Riesgo Aceptable**: Se estableció un umbral de riesgo aceptable, considerando como tratables los riesgos cuyo valor fuera mayor o igual a 3.
5. **Asignación de Controles**: Para los riesgos identificados, se asignaron controles específicos recomendados en el Anexo A de la norma ISO 27001, con el objetivo de mitigar los riesgos y reducirlos a niveles aceptables.
6. **El nivel de madurez,** según la metodología MAGERIT, se refiere a la efectividad y consistencia con la que se implementan los controles de seguridad en una organización. A medida que el nivel de madurez aumenta, los procesos son más robustos, predecibles y capaces de adaptarse a cambios en el entorno. La evaluación

de la madurez ayuda a determinar en qué punto se encuentra una organización en su capacidad para gestionar riesgos de manera eficiente y proactiva.

Este nivel de madurez refleja la capacidad de la empresa para mantener un Sistema de Gestión de Seguridad de la Información (SGSI) sólido. En el contexto del análisis de riesgo descrito, este nivel de madurez es esencial para la evaluación de cómo se gestionan los riesgos una vez implementados los controles de seguridad y cómo se reduce el riesgo residual.

Los niveles de madurez se calculan según la **Tabla 7** siguiente:

Tabla 14: Cálculo de los niveles de madurez alcanzado con los controles.

Eficacia	Nivel de Madurez	Significado
0%	L0	**Inexistente**, la medida de seguridad no existe
10%	L1	**Inicial**, la medida la medida de seguridad se aplica cuando se considera adecuado, pero No queda establecido
50%	L2	**Reproducible**
90%	L3	**Proceso Definido**. La medida de seguridad se aplica y queda definida documentalmente.
95%	L4	Medida de seguridad **Gestionada y Medible**
100%	L5	Medida de Seguridad **Optimizada** . A la mmedida de seguridad implementada y gestionada se le aplica proceso de mejora y optimización.

7. **Cálculo del Riesgo Residual**: Tras la implementación de los controles, se recalculó el riesgo, evaluando su reducción y determinando el riesgo residual para cada activo.

4.3.2. Plan de Acción basado en la Evaluación de Riesgos.

El Plan de Acción del periodo 2024 se ha desarrollado siguiendo una metodología estructurada, alineada con las directrices establecidas por la norma ISO/IEC 27001 y las mejores prácticas de gestión de riesgos. Los pasos clave en la metodología empleada son los siguientes:

1. **Identificación de dominios y Controles Relevantes**: Se partió de la Declaración de Aplicabilidad (SOA) de Innovatech Consulting, que define los dominios y controles aplicables a la organización. Aquellos controles que no son aplicables a Innovatech Consulting fueron excluidos del Plan de Riesgos, garantizando que el análisis se centra únicamente en las áreas críticas para la seguridad de la información.

2. **Evaluación del nivel de Madurez Inicial**: Se evaluó el nivel de madurez inicial de cada control mediante la revisión de la implementación actual de políticas, procedimientos y medidas de seguridad en cada dominio. Los niveles de madurez se determinaron siguiendo una escala estandarizada que va de L1 (mínima madurez) a L5 (madurez óptima) según la **Tabla 7**.
3. **Determinación del nivel de Madurez Objetivo**: Para cada control, se estableció un nivel de madurez esperado acorde con los requisitos estratégicos y operativos de Innovatech Consulting, considerando las expectativas de seguridad y cumplimiento normativo.
4. **Definición de acciones correctivas y mejoras**: Se identificaron las acciones necesarias para cerrar la brecha entre el nivel de madurez inicial y el objetivo. Estas acciones se clasificaron en dos categorías:
    - **Acciones Organizativas (A.O.)**: Incluyen actividades como la revisión de políticas, la formación del personal, y la mejora de procesos.
    - **Acciones Técnicas (A.T.)**: Incluyen implementaciones de herramientas tecnológicas, actualizaciones de software, y medidas de seguridad física.
5. **Monitorización del Grado de avance**: Se estableció un sistema de seguimiento para monitorear el grado de avance de cada acción, con plazos específicos y responsables asignados para asegurar la implementación efectiva.
6. **Plazos y responsables de validación**: Todos los resultados en cuanto a fechas, plazos, recursos y decisiones se documentaron en el Plan de Riesgos 2024 y fueron validados por los responsables asignados por Innovatech Consulting.

4.3.3. Análisis del riesgo de partes interesadas.

El análisis de riesgo de partes interesadas se realiza de manera independiente para garantizar que las preocupaciones, expectativas y vulnerabilidades de cada grupo relevante para la organización sean abordadas de manera específica y adecuada. Cada parte interesada posee intereses únicos y distintos niveles de influencia sobre la organización, lo que requiere una evaluación detallada que permita mitigar riesgos específicos asociados a cada grupo. Este enfoque permite personalizar las acciones de mitigación de riesgos, asegurando que todos los aspectos de la seguridad de la información estén cubiertos de acuerdo con las características particulares de cada grupo de interés, optimizando así la gestión del riesgo de la organización en su conjunto.

La metodología empleada para el análisis de riesgo de partes interesadas en INICIE se basa en una matriz de evaluación de riesgo que, igualmente, considera dos factores principales: la probabilidad de ocurrencia del riesgo y el impacto que este podría tener sobre la organización. Cada parte interesada es evaluada en términos de:

- **Probabilidad (P):** Estimada en una escala de 1 a 5 de acuerdo a los criterios establecidos en la **Tabla 4**.
- **Impacto (I):** Valorado en una escala de 1 a 5, de acuerdo a los criterios establecidos en la **Tabla 5**.

El valor de riesgo se obtiene hallando la media aritmética de los valores obtenidos para la probabilidad y el impacto, resultando en un rango de valores que permiten clasificar el riesgo en distintas categorías según lo expuesto en la **Tabla 6**. En función del valor de riesgo calculado, se determinan las acciones de mitigación necesarias y su grado de urgencia.

Para la implementación de las acciones de mitigación, se han identificado dos tipos de acciones:

- **Acciones Organizativas (A.O.):** Relacionadas con la documentación, formación y establecimiento de normativas.
- **Acciones Técnicas (A.T.):** Referentes a la implementación de controles técnicos específicos, como la creación de identificadores de acceso y la caducidad de contraseñas.

4.3.4. Establecimiento de objetivos e indicadores de Seguridad.

En el contexto de un Sistema de Gestión de Seguridad de la Información (SGSI), la Norma ISO 27001 establece la necesidad de definir, implementar y mantener objetivos claros y medibles para garantizar la seguridad de la información dentro de una organización. La principal razón para establecer estos objetivos es asegurar que todos los riesgos relacionados con la seguridad de la información sean gestionados adecuadamente, mitigando posibles amenazas y vulnerabilidades. Además, estos objetivos proporcionan una base para la medición del rendimiento del SGSI, permitiendo evaluar su eficacia y eficiencia.

Los objetivos de seguridad de la información deben alinearse con la política de seguridad de la organización y los requisitos legales y reglamentarios aplicables. Además, deben ser específicos, medibles, alcanzables, relevantes y con un tiempo determinado (SMART), lo que facilita su seguimiento y evaluación continua. La monitorización de estos

objetivos a través de indicadores es fundamental para asegurar que se están cumpliendo y, en caso contrario, poder tomar medidas correctivas a tiempo.

4.3.4.1. Metodología utilizada para establecer Objetivos e Indicadores.

Para el establecimiento de los objetivos e indicadores de seguridad de la información, se ha seguido una metodología que incluye las siguientes etapas:

1. **Identificación de Riesgos y Oportunidades**: A partir de la evaluación de riesgos, se identifican los aspectos críticos que necesitan ser gestionados a través de objetivos específicos. Esto incluye identificar tanto los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información, como las oportunidades para mejorar el SGSI.
2. **Definición de Objetivos**: Basados en la identificación de riesgos y oportunidades, se definen los objetivos de seguridad. Estos objetivos son específicos y están alineados con la política de seguridad de la información. Además, se aseguran de que sean medibles para poder evaluar su cumplimiento.
3. **Selección de Indicadores**: Para cada objetivo, se seleccionan indicadores que permitan medir de manera continua su progreso y cumplimiento. Estos indicadores son claves para monitorear la efectividad de las medidas de seguridad implementadas y están diseñados para ser fáciles de interpretar y aplicar en la práctica diaria.
4. **Periodicidad de seguimiento**: Se establece la frecuencia con la cual se realizará el seguimiento de cada indicador. Dependiendo de la naturaleza del objetivo y la criticidad del indicador, la periodicidad puede ser mensual, trimestral, o anual.
5. **Asignación de responsabilidades**: Se designa un responsable para cada objetivo e indicador, quien será el encargado de llevar a cabo el seguimiento, evaluación y reporte de resultados.
6. **Documentación y comunicación**: Todos los objetivos e indicadores se documentan formalmente y se comunican a las partes interesadas pertinentes dentro de la organización. Esto asegura que todos los involucrados estén al tanto de los estándares de seguridad que deben cumplirse.

4.3.4.2. Descripción de los Indicadores.

La metodología para definir los indicadores se basó en una estructura estandarizada donde cada indicador incluye:

- **Identificación del Indicador (KPI)**: Cada indicador tiene un código único que facilita su identificación y referencia en los informes.
- **Responsable de Seguimiento**: Se asigna un responsable específico para el seguimiento y reporte del indicador.
- **Periodicidad de Seguimiento**: Se establece un calendario de medición para garantizar la consistencia en el seguimiento del indicador.
- **Método de Cálculo**: Se detalla la fórmula o el procedimiento utilizado para calcular el valor del indicador, asegurando transparencia y consistencia en la medición.
- **Comentarios**: Se incluyen notas relevantes que proporcionan contexto adicional, tales como observaciones sobre el desempeño del indicador en periodos anteriores o consideraciones específicas que pueden influir en su comportamiento futuro.

Ejemplos de los Indicadores definidos:

- **Indicador K1**: "% de riesgos de seguridad de la información para los cuales se han implantado controles". Este indicador mide la efectividad de las acciones correctivas implementadas en función del número total de riesgos identificados.
- **Indicador K2**: "% de cambios aprobados con error conocido por incidencias". Este indicador permite monitorear la calidad de los cambios implementados en el entorno de producción, asegurando que los errores sean mínimos y controlados.

Estos son solo ejemplos que reflejan cómo se estructuran y monitorean los indicadores para garantizar un sistema de gestión de la seguridad de la información robusto y eficaz.

4.3.4.3. Benéficos esperados al establecer indicadores.

Los indicadores no solo facilitan el cumplimiento de los requisitos normativos y la gestión del SGSI, sino que también son fundamentales para la toma de decisiones estratégicas, la mejora continua, y la construcción de una cultura organizacional centrada en la seguridad de la información. Por lo tanto, establecer indicadores de seguridad de la información en un sistema de gestión basado en la norma ISO 27001 ofrece varios beneficios clave y que son esenciales para garantizar la protección y gestión adecuada de la información en una organización. Estos beneficios incluyen:

1. Monitorización en continuo del rendimiento: Los indicadores permiten un seguimiento constante del rendimiento del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando que las medidas de seguridad implementadas están funcionando de manera efectiva. Por otro lado, a través de la medición continua, es posible identificar

rápidamente cualquier desviación de los objetivos establecidos, permitiendo la adopción de medidas correctivas antes de que se conviertan en problemas mayores.

2. Toma de decisiones basadas en datos: Los indicadores proporcionan datos concretos que respaldan la toma de decisiones informadas. Esto es crucial para la alta dirección, que necesita información precisa para gestionar riesgos y recursos de manera efectiva. Con indicadores claros, la organización puede priorizar sus recursos en las áreas de mayor riesgo o donde se identifican brechas significativas en la seguridad.

3. Cumplimiento normativo: Establecer y monitorizar indicadores es un requisito de la norma ISO 27001 y ayuda a la organización a mantenerse en conformidad con las mejores prácticas internacionales y a superar auditorías externas. Además, los indicadores proporcionan una base documental sólida para demostrar el cumplimiento de los requisitos normativos y de los clientes.

4. Mejora continua: A través del análisis de los resultados de los indicadores la organización puede identificar áreas donde se pueden realizar mejoras en los procesos y controles de seguridad. Por lo tanto, los indicadores facilitan la evaluación y ajuste continuo del SGSI, promoviendo una cultura de mejora continua en la gestión de la seguridad de la información.

5. Comunicación y transparencia: Establecer indicadores ayuda a comunicar claramente los objetivos de seguridad a todos los niveles de la organización, alineando a los empleados y equipos con la estrategia de seguridad. Los indicadores son herramientas efectivas para reportar el estado de la seguridad de la información a las partes interesadas, incluyendo la alta dirección, clientes y reguladores.

6. Reducción de Riesgos: Los indicadores permiten una identificación proactiva de riesgos emergentes, permitiendo a la organización tomar acciones preventivas antes de que ocurran incidentes de seguridad. Además, al medir la eficacia de la respuesta a incidentes a través de indicadores específicos, la organización puede mejorar continuamente su capacidad de respuesta y recuperación.

7. Aumento de la confianza: La existencia de indicadores de seguridad bien gestionados aumenta la confianza de las partes interesadas (clientes, socios, inversores) en la capacidad de la organización para proteger su información. Por otro lado, el manejo eficiente de la seguridad de la información fortalece la reputación de la empresa en el mercado sobre todo si está respaldado por indicadores claros.

4.3.5. Declaración de Aplicabilidad (SOA).

El presente capítulo tiene como objetivo describir la metodología utilizada para la elaboración de la Declaración de Aplicabilidad (SOA) en el contexto del Sistema de Gestión de Seguridad de la Información (SGSI) de Innovatech Consulting, la empresa ficticia sobre la cual se basa este trabajo. La SOA es un documento clave que asegura que los controles de seguridad seleccionados estén alineados con los riesgos específicos identificados en la organización, así como con los requisitos normativos aplicables. A lo largo de este capítulo, se detallarán los procesos seguidos para determinar la aplicabilidad de cada control, la justificación de su inclusión o exclusión, y las herramientas empleadas en su desarrollo.

4.3.5.1. Definición de la SOA.

La Declaración de Aplicabilidad (SOA) es un documento central dentro del Sistema de Gestión de Seguridad de la Información (SGSI) de Innovatech Consulting, que especifica los controles de seguridad seleccionados para mitigar los riesgos identificados en la empresa. Este documento se basa en los controles propuestos en el Anexo A de la norma ISO 27001, pero también puede incluir controles adicionales relevantes para los contextos específicos de Innovatech Consulting, como la protección de la propiedad intelectual y la gestión segura de la información de sus clientes.

El propósito principal de la SOA en Innovatech Consulting es proporcionar una justificación clara y fundamentada para la inclusión, modificación o exclusión de cada control de seguridad, según su relevancia y aplicabilidad en el contexto de la empresa. La SOA no solo garantiza la efectividad del SGSI, sino que también facilita la evaluación y auditoría del sistema, demostrando el compromiso de Innovatech Consulting con la seguridad de la información y el cumplimiento de los requisitos normativos y contractuales.

Por ejemplo, en el caso de Innovatech Consulting, que maneja datos sensibles de sus clientes y desarrolla soluciones tecnológicas, la SOA juega un papel crucial al asegurar que los controles implementados protejan adecuadamente tanto los activos de la empresa como la información crítica de sus clientes. La SOA, por lo tanto, se convierte en una referencia indispensable para la implementación y el mantenimiento de controles efectivos en Innovatech Consulting, asegurando que la empresa esté preparada para enfrentar los desafíos de seguridad en un entorno dinámico y altamente regulado.

4.3.5.2. Metodología para la elaboración de la SOA.

En este apartado se describe el enfoque metodológico seguido por Innovatech Consulting para la elaboración de la Declaración de Aplicabilidad (SOA), un documento clave

que garantiza la alineación entre los riesgos identificados y los controles de seguridad seleccionados. La metodología adoptada se basa en un análisis riguroso y sistemático, que incluye la identificación, evaluación y justificación de cada control, asegurando que la SOA refleje fielmente las necesidades y particularidades de Innovatech Consulting. A continuación, se detallan los pasos clave de este proceso, desde la identificación inicial de los controles hasta la justificación de su aplicabilidad, pasando por la evaluación rigurosa de su relevancia para la organización.

4.3.5.2.1. Proceso de identificación de controles.

El proceso de identificación de controles en Innovatech Consulting se llevó a cabo con el objetivo de asegurar que todas las posibles amenazas a la seguridad de la información fueran adecuadamente mitigadas a través de controles específicos y efectivos. Este proceso se estructuró en los siguientes pasos:

1. **Revisión del Anexo A de la ISO 27001**: Se comenzó con un análisis exhaustivo del Anexo A de la norma ISO 27001, el cual proporciona un conjunto de 93 controles divididos en 4 dominios. Cada uno de estos controles fue evaluado para determinar su relevancia en el contexto de las operaciones y la estructura de Innovatech Consulting.
2. **Consideración de marcos y estándares complementarios**: Además de la ISO 27001, se consideraron otros marcos y estándares complementarios, como la ISO 27017 (para seguridad en la nube) y la ISO 27018 (protección de datos personales en la nube). Estos estándares adicionales fueron revisados para identificar controles que pudieran ser relevantes para **Innovatech Consulting**, especialmente dado su enfoque en servicios de consultoría tecnológica y su manejo de datos sensibles.
3. **Mapeo de controles a riesgos identificados**: A partir del análisis de riesgos realizado previamente, se llevó a cabo un mapeo detallado donde cada riesgo identificado fue vinculado con uno o varios controles del Anexo A o de los marcos complementarios. Esto garantizó que todos los riesgos significativos fueran abordados por controles específicos.
4. **Consultas con expertos y stakeholders**: Para asegurar que la identificación de controles fuera exhaustiva y aplicable, se realizaron consultas con expertos en seguridad de la información y con partes interesadas clave dentro de la empresa. Esto permitió incorporar perspectivas adicionales y asegurar que no se pasara por alto ningún control relevante.

5. **Documentación y revisión de la lista de controles**: Una vez identificados los controles, se documentó detalladamente la justificación de su selección en un primer borrador de la SOA. Esta lista fue revisada por el comité de seguridad de la información para asegurar su alineación con los objetivos estratégicos y operativos de Innovatech Consulting.

4.3.5.2.2. Evaluación de la Aplicabilidad de los controles.

El proceso de evaluación de la aplicabilidad de los controles en Innovatech Consulting se centró en asegurar que cada control identificado fuera pertinente y necesario para mitigar los riesgos específicos que enfrenta la organización. Este proceso se estructuró en los siguientes pasos:

a. **Revisión del análisis de Riesgos:** Se comenzó por revisar el análisis de riesgos previamente realizado, el cual identificó las amenazas y vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de la información gestionada por Innovatech Consulting. Este análisis fue crucial para entender el contexto en el que los controles debían aplicarse.

b. **Clasificación de Riesgos por Impacto y Probabilidad:** Los riesgos identificados fueron clasificados según su impacto potencial y la probabilidad de ocurrencia. Esta clasificación permitió priorizar los riesgos que requerían una atención más inmediata y determinar qué controles eran críticos para mitigar los riesgos más significativos.

c. **Evaluación de la Relevancia de cada control:** Cada control listado en el Anexo A de la ISO 27001 y en los marcos complementarios fue evaluado para determinar su relevancia frente a los riesgos clasificados. Se analizaron factores como la capacidad del control para mitigar uno o varios riesgos y su adecuación al contexto operativo y tecnológico de Innovatech Consulting.

d. **Consideración de la capacidad y recursos de la organización:** La evaluación de la aplicabilidad también tomó en cuenta la capacidad de Innovatech Consulting para implementar y mantener cada control, considerando recursos disponibles, competencias técnicas y limitaciones operativas. Aquellos controles que no eran factibles de implementar con los recursos actuales fueron revisados para determinar si podían ser sustituidos por alternativas más viables.

e. **Consulta y validación con el comité de seguridad de la información:** Los resultados de la evaluación fueron discutidos con el comité de seguridad de la

información para validar las decisiones sobre la aplicabilidad de cada control. Este paso garantizó que las decisiones fueran alineadas con la estrategia de seguridad de la información y los objetivos organizacionales.

f. **Documentación en la SOA:** Finalmente, se documentaron las decisiones de aplicabilidad en la Declaración de Aplicabilidad (SOA), incluyendo justificaciones claras para cada control aplicable y las razones por las cuales ciertos controles no se consideraron necesarios. Esto proporcionó una base sólida y transparente para la gestión continua de la seguridad de la información en Innovatech Consulting.

4.3.5.2.3. Justificación de la inclusión o exclusión de controles.

El proceso de justificación de la inclusión o exclusión de los controles en la Declaración de Aplicabilidad (SOA) de Innovatech Consulting se basó en un análisis riguroso de los riesgos identificados y en la alineación de estos controles con los requisitos específicos de la organización. A continuación, se detallan los principales aspectos que han sido considerados en este proceso:

1. **Relación directa con los Riesgos identificados**: Cada control propuesto en el Anexo A de la ISO 27001 ha sido evaluado en función de su capacidad para mitigar riesgos específicos previamente identificados en el análisis de riesgos. Aquellos controles que demostraron ser efectivos para reducir la probabilidad o el impacto de un riesgo fueron incluidos en la SOA. Por ejemplo, si un riesgo relacionado con la pérdida de confidencialidad de la información sensible se consideraba alto, se justificaba la inclusión de controles de cifrado y acceso restringido.

2. **Requisitos legales y contractuales**: La inclusión de ciertos controles se ha visto justificada por la necesidad de cumplir con requisitos legales, reglamentarios o contractuales específicos. Estos controles son esenciales para asegurar que Innovatech Consulting operara dentro del marco legal aplicable, minimizando el riesgo de sanciones o incumplimientos. En casos donde no existían tales requisitos, y el riesgo asociado era bajo, se consideró la exclusión del control.

3. **Relevancia para el contexto operativo de la organización**: Se ha tenido en cuenta la relevancia de cada control en el contexto operativo y tecnológico de Innovatech Consulting. Controles que no se aplicaban directamente al entorno operativo o al modelo de negocio de la empresa han sido excluidos con la correspondiente justificación, aunque estuviesen reconocidos por la norma. Por ejemplo, si un control relacionado con la protección de dispositivos móviles no era relevante debido a

políticas de uso limitado de dichos dispositivos, se ha optado por no incluirlo en la SOA.

4. **Capacidad de implementación y mantenimiento**: La capacidad de la organización para implementar y mantener los controles también fue un factor clave en la justificación. Algunos controles que requerían recursos o competencias técnicas que la organización no poseía, fueron evaluados críticamente. En estos casos, se decidió excluir aquellos controles que no eran factibles de implementar de manera efectiva, optando, en ese caso, por controles alternativos más alineados con las capacidades internas de **Innovatech Consulting**.

5. **Consenso y validación con el comité de seguridad**: Todas las decisiones sobre la inclusión o exclusión de controles fueron validadas por el comité de seguridad de la información de **Innovatech Consulting**. Este grupo revisó las justificaciones proporcionadas, asegurándose de que estaban alineadas con los objetivos de seguridad de la organización y con las expectativas de las partes interesadas.

6. **Documentación de las Decisiones**: Cada decisión de inclusión o exclusión fue debidamente documentada en la SOA con una justificación clara y concisa. Esto incluyó referencias a los riesgos específicos abordados o a las razones por las cuales un control no era aplicable. Esta documentación no solo sirve para las auditorías tanto de revisión interna como externa para la certificación de la norma, sino que también proporciona una base para futuras evaluaciones de riesgos y actualizaciones de la SOA.

4.3.6. Automatización del SGSI en Microsoft Azure.

Microsoft Azure es una plataforma de computación en la nube que ofrece una amplia gama de servicios para la gestión, almacenamiento y procesamiento de datos, así como para la implementación y mantenimiento de aplicaciones. Una de las características más relevantes de Azure en el contexto de la seguridad de la información es su capacidad para automatizar controles de seguridad a través de herramientas como Microsoft Defender for Cloud.

Estas herramientas permiten la integración de evaluaciones automáticas, monitorización continua y generación de informes de cumplimiento, alineando las operaciones de la empresa con estándares internacionales como la ISO 27001. En particular, Microsoft Defender for Cloud realiza evaluaciones automatizadas que proporcionan evidencia relevante sobre el estado de los controles de seguridad, facilitando la gestión integral del Sistema de Gestión de Seguridad de la Información (SGSI).

Para Innovatech Consulting, una empresa que opera principalmente en un entorno de trabajo remoto y que depende en gran medida de la infraestructura en la nube, la automatización de los controles de seguridad es crucial. La naturaleza distribuida de su equipo y la dependencia de servicios en la nube exigen un enfoque de seguridad que sea tanto proactivo como reactivo. La automatización en Microsoft Azure no solo permite a Innovatech Consulting mantener un alto nivel de seguridad, sino que también asegura una respuesta rápida y eficiente a posibles incidentes de seguridad. Además, la automatización minimiza la carga operativa del equipo de IT, permitiendo que se concentren en áreas estratégicas y de mayor valor añadido, al tiempo que garantiza que los controles de seguridad estén siempre actualizados y alineados con las mejores prácticas de la industria.

Esta combinación de características hace que la automatización en Microsoft Azure sea un componente esencial en la estrategia de seguridad de Innovatech Consulting, asegurando que la empresa pueda operar con confianza en un entorno digital cada vez más complejo.

4.3.6.1. Beneficios de la automatización en el SGSI.

La automatización de los controles de seguridad en Microsoft Azure proporciona múltiples beneficios que son esenciales para la seguridad operativa de una organización como Innovatech Consulting. En primer lugar, la automatización reduce significativamente el riesgo de error humano en la implementación y monitorización de controles de seguridad, asegurando una aplicación consistente y precisa de las políticas de seguridad. Además, permite una respuesta más rápida y eficiente a posibles incidentes de seguridad, gracias a la capacidad de Microsoft Defender for Cloud para detectar amenazas en tiempo real y aplicar medidas correctivas de manera automática o semi-automática.

Otro beneficio clave es la capacidad de realizar evaluaciones continuas de cumplimiento normativo sin la necesidad de intervención manual, lo que asegura que la organización se mantenga siempre alineada con los estándares internacionales, como la ISO 27001. La automatización también facilita la generación de informes detallados sobre el estado de la seguridad, proporcionando a los responsables de IT y a la alta dirección una visión clara y actualizada de la postura de seguridad de la empresa. Estos informes permiten una mejor toma de decisiones y una planificación más efectiva de las estrategias de seguridad.

4.3.6.2. Monitorización y evaluación de controles automatizados.

Microsoft Defender for Cloud es una herramienta avanzada de monitorización que permite a Innovatech Consulting realizar un seguimiento continuo y detallado de los controles de seguridad implementados en su infraestructura en la nube. La metodología de

monitorización se basa en la recopilación y análisis en tiempo real de datos de seguridad provenientes de los recursos de Azure. Estos datos incluyen eventos de seguridad, configuraciones de acceso y otros indicadores clave que pueden afectar la seguridad de la organización.

La herramienta está diseñada para alinearse con los requisitos de la norma ISO 27001, asegurando que todos los controles relevantes sean supervisados de manera efectiva. Microsoft Defender for Cloud realiza evaluaciones automatizadas de cumplimiento, que verifican que los controles se apliquen correctamente y que cumplan con los estándares internacionales. La herramienta también genera alertas cuando se detecta una desviación en la configuración de seguridad, permitiendo una respuesta rápida para mitigar posibles riesgos.

Además, esta monitorización se integra con la función de auditoría interna, proporcionando a los responsables de seguridad la capacidad de revisar y ajustar los controles según sea necesario, garantizando que el Sistema de Gestión de Seguridad de la Información (SGSI) se mantenga robusto y en constante mejora.

4.3.6.3. Evaluación y mejora continua de la automatización.

La automatización de controles de seguridad en Innovatech Consulting ha mostrado un alto grado de efectividad, sin embargo, algunos controles críticos han presentado fallos que requieren atención especial. Un ejemplo relevante es el área de "Access Control" (Control de Acceso), donde se encontraron deficiencias en la gestión de derechos de acceso privilegiado (A.9.2.3) y en la gestión de la información de autenticación secreta de los usuarios (A.9.2.4). Estos fallos indican que, a pesar de la automatización, es necesario realizar revisiones periódicas y ajustes en la configuración de acceso para garantizar que los controles se mantengan eficaces y alineados con las políticas de seguridad establecidas.

Para abordar las deficiencias identificadas en los controles, se proponen estrategias de mejora como las siguientes:

1. **Revisión y fortalecimiento de Políticas de acceso:** Actualizar y fortalecer las políticas de acceso privilegiado y autenticación, asegurando que se apliquen configuraciones más restrictivas y que todos los cambios en los derechos de acceso sean auditados y registrados automáticamente.
2. **Capacitación adicional:** Proveer formación adicional a los administradores de sistemas y otros usuarios con acceso privilegiado, para garantizar que comprendan plenamente las políticas de acceso y la importancia de adherirse a ellas.

3. **Implementación de herramientas adicionales:** Considerar la integración de herramientas adicionales de gestión de identidad y acceso (IAM) dentro de Microsoft Azure, que permitan una monitorización más granular y la aplicación automática de políticas de acceso basadas en roles.
4. **Auditorías de seguimiento:** Realizar auditorías de seguimiento específicas en las áreas donde se han identificado fallos, para verificar que las mejoras implementadas sean efectivas y que los controles se mantengan en conformidad con la norma ISO 27001.

La implementación y monitorización de controles automatizados en Microsoft Azure deben alinearse con el ciclo de mejora continua (PDCA: Plan, Do, Check, Act). Este enfoque asegura que los procesos no solo se mantengan eficaces, sino que también evolucionen para adaptarse a nuevas amenazas y requisitos de seguridad:

- **Plan (Planificar):** Identificar áreas de mejora basadas en los resultados de la monitorización y las auditorías, y desarrollar planes de acción específicos para abordar las deficiencias.
- **Do (Hacer):** Implementar las mejoras propuestas, como la actualización de políticas de acceso, la formación de usuarios, y la integración de nuevas herramientas.
- **Check (Verificar):** Realizar una evaluación exhaustiva de los controles mejorados a través de auditorías internas y el uso continuo de Microsoft Defender for Cloud para monitorear el cumplimiento.
- **Act (Actuar):** Ajustar los controles y procesos según sea necesario, basándose en los resultados de las evaluaciones y auditorías, y documentar los cambios para asegurar la continuidad del proceso de mejora.

4.3.7. Plan de Continuidad de Negocio.

El Plan de Continuidad de Negocio (BCP, por sus siglas en inglés) es un componente esencial para garantizar la resiliencia operativa de Innovatech Consulting ante eventos disruptivos. Este capítulo tiene como objetivo destacar la importancia de contar con un BCP robusto, que permita a la empresa mantener sus operaciones críticas y proteger sus activos, incluso en situaciones de crisis.

En el contexto de Innovatech Consulting, donde la innovación y la tecnología son pilares fundamentales, la capacidad de respuesta ante incidentes que puedan interrumpir las actividades del negocio es vital para asegurar la continuidad del servicio a clientes, la

protección de datos y la estabilidad organizativa. En este caso no solo se pretende cubrir la recuperación de los sistemas de información, sino abarcar todos los aspectos críticos del negocio, asegurando que la empresa pueda seguir operando bajo circunstancias adversas, minimizando el impacto en sus procesos, reputación y viabilidad financiera.

El BCP se integra de manera directa en el Sistema de Gestión de Seguridad de la Información (SGSI) de Innovatech Consulting, tal como lo establece la norma ISO 27001:2022. Esta norma internacional subraya la necesidad de un enfoque sistemático para la gestión de la seguridad de la información, y el BCP es una extensión natural de estos principios, centrado en la continuidad operativa.

Según la ISO 27001:2022, el BCP debe alinearse con los objetivos de seguridad de la información de la empresa, identificando y mitigando los riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información. De esta manera, el BCP no solo protege los procesos de negocio, sino que también refuerza la seguridad de la información, creando una estrategia integral que permite a Innovatech Consulting afrontar y superar las adversidades con eficacia.

4.3.7.1. Metodología para la elaboración del BCP.

4.3.7.1.1. Identificación de Procesos Críticos.

La identificación de los procesos críticos es un proceso que se basa en la comprensión profunda de las operaciones de la empresa y su interdependencia con los activos de información. Se comienza por mapear todos los procesos de negocio, evaluando cuáles son esenciales para la continuidad operativa y cuáles podrían detenerse temporalmente sin un impacto significativo en la organización. En este caso, las herramientas y técnicas utilizadas han sido:

- **Análisis de Impacto en el Negocio (BIA):** Este análisis ayuda a identificar las funciones y procesos críticos al evaluar el impacto que su interrupción tendría en la organización.
- **Evaluación de riesgos:** Se aplican matrices de evaluación de riesgos para determinar la probabilidad y el impacto de eventos adversos en cada proceso crítico.
- **Entrevistas con líderes de proceso:** Para obtener una visión detallada de los procesos críticos y sus dependencias.

4.3.7.1.2. Evaluación de Riesgos y Amenazas.

La evaluación de riesgos y amenazas es el siguiente paso para garantizar la continuidad de los procesos críticos identificados. Innovatech Consulting lleva a cabo un análisis exhaustivo de los riesgos que podrían interrumpir estos procesos, incluyendo desastres naturales, fallos tecnológicos, ciberataques, y otros eventos adversos. Las metodologías de evaluación utilizadas han sido:

- **Análisis DAFO:** Este análisis se utiliza para identificar fortalezas, oportunidades, debilidades y amenazas relacionadas con la continuidad del negocio.
- **Análisis de escenarios:** Se modelan posibles escenarios de interrupción para evaluar el impacto y desarrollar respuestas efectivas.
- **Matrices de probabilidad e impacto:** Estas matrices ayudan a priorizar las amenazas en función de su probabilidad de ocurrencia y el impacto en la organización.

4.3.7.1.3. Desarrollo de estrategias de continuidad.

Una vez identificados los riesgos y amenazas, Innovatech Consulting desarrolla estrategias específicas para mitigar estos riesgos y garantizar la continuidad de las operaciones. Estas estrategias se diseñan para minimizar el tiempo de inactividad y asegurar que los procesos críticos puedan reanudarse lo más rápido posible tras una interrupción.

Tipos de estrategias posibles:

- **Recuperación ante desastres:** Incluye la restauración de datos y sistemas críticos desde copias de seguridad y la reubicación de operaciones a sitios alternativos.
- **Redundancia de sistemas:** Implementación de sistemas de TI redundantes para asegurar la disponibilidad continua de datos y aplicaciones clave.
- **Planes de contingencia:** Planes específicos para responder a eventos de interrupción, incluyendo la reasignación de recursos y la reubicación de operaciones.

4.3.7.1.4. Elaboración del Plan de Respuesta.

El Plan de Respuesta ante incidentes define los pasos específicos que Innovatech Consulting debe seguir cuando se active el BCP y abarca hasta la restauración completa de las operaciones. Los componentes clave del plan de respuesta son:

- **La activación del BCP:** Se establecen criterios claros para determinar cuándo se debe activar el BCP, incluyendo los procedimientos de notificación y escalación.

- **Las comunicaciones de emergencia:** El plan incluye estrategias para la comunicación interna y externa, garantizando que todos los interesados estén informados y que se mantenga la confianza de los clientes y socios.
- **La asignación de responsabilidades:** Se han de asignar responsabilidades específicas de los equipos de respuesta ante incidentes, incluyendo líderes de proceso, personal de TI, así como la alta dirección.

4.3.7.1.5. Documentación y aprobación del BCP.

La documentación del BCP es fundamental para asegurar que todos los aspectos del plan estén claramente definidos y puedan ser entendidos y ejecutados eficazmente. Esta documentación incluye detalles sobre los roles y responsabilidades, los procedimientos para la gestión de incidentes y los recursos necesarios para la implementación del plan.

Para ello, lo primero que se ha de hacer es documentar cada componente del BCP, asegurando que esté claro y accesible para todos los implicados. Posteriormente, el BCP es revisado por la alta dirección de Innovatech Consulting para garantizar que cumple con los objetivos de la organización y que está alineado con la estrategia general del SGSI. Una vez aprobado, el BCP se distribuye a los equipos responsables y se almacena en un lugar seguro, con copias de respaldo disponibles para su acceso en caso de emergencia.

4.3.7.2. Implementación del BCP.

4.3.7.2.1. Formación y Capacitación.

La implementación efectiva del Plan de Continuidad de Negocio (BCP) en Innovatech Consulting requiere que todo el personal esté debidamente informado y capacitado sobre sus responsabilidades y acciones en caso de un incidente. El plan de formación y capacitación se centra en garantizar que todos los empleados comprendan los procedimientos del BCP y puedan ejecutar sus roles de manera efectiva durante una emergencia.

Los elementos más relevantes a diseñar en un adecuado Plan de formación y capacitación han de ser:

- **Simulacros:** Se realizan simulacros periódicos que permiten a los empleados practicar sus roles en un entorno controlado. Estos simulacros simulan escenarios de interrupción y permiten evaluar la capacidad de respuesta del personal.
- **Talleres y charlas:** Se organizan talleres educativos y charlas donde se discuten los componentes clave del BCP, las responsabilidades individuales y los procedimientos específicos a seguir durante un incidente.

- **Revisiones periódicas:** Se llevan a cabo revisiones regulares del BCP con el personal, asegurando que estén al tanto de cualquier actualización o cambio en el plan. Estas revisiones también sirven para reforzar el conocimiento familiarizarse con el mismo.

4.3.7.2.2. Pruebas y ejercicios.

Para garantizar que el Plan de Continuidad de Negocio (BCP) de Innovatech Consulting sea efectivo y operativo en caso de una interrupción real se realizan pruebas y ejercicios regulares de distinto tipo:

- **Pruebas de simulación:** Normalmente se recrean escenarios de interrupción específicos para evaluar la capacidad de respuesta del BCP. Estas pruebas permiten identificar fallos o áreas de mejora en los procedimientos establecidos.
- **Ejercicios funcionales:** Los ejercicios funcionales se centran en la práctica de tareas específicas dentro del BCP, como la activación de comunicaciones de emergencia o la restauración de sistemas críticos.

Las pruebas del BCP se llevan a cabo al menos una vez al año, con ejercicios adicionales programados según la necesidad o tras cualquier cambio significativo en los procesos de negocio o infraestructura de TI. Para medir la efectividad de las pruebas se utilizan criterios de evaluación claros, como el tiempo de respuesta, la efectividad en la comunicación y la capacidad para restaurar operaciones críticas. Los resultados de estas evaluaciones se utilizan para mejorar continuamente el BCP.

4.3.7.3. Monitorización y revisión del BCP.

4.3.7.3.1. Monitorización continua.

Para garantizar la efectividad y relevancia del Plan de Continuidad de Negocio (BCP) de Innovatech Consulting, se implementan mecanismos de monitorización continua. Estos mecanismos permiten detectar cambios en los riesgos, el entorno operativo, o las condiciones externas que puedan impactar la capacidad de la empresa para responder a incidentes.

Para ello, se emplean herramientas de monitorización en tiempo real para vigilar posibles amenazas, cambios en la infraestructura de TI, y variaciones en el entorno de negocio que puedan afectar al BCP.

Por otro lado, se establecen procesos de alerta que notifican de inmediato a los responsables cuando se detecta un cambio significativo en el entorno operativo o en el perfil de riesgo.

Igualmente, realiza un plan de evaluaciones periódicas de los riesgos actuales y potenciales, utilizando análisis de tendencias y datos históricos para anticipar futuras amenazas y ajustar el BCP en consecuencia.

4.3.7.3.2. Revisión y actualización periódica.

El BCP de Innovatech Consulting se revisa y actualiza de manera regular para asegurar que permanezca alineado con los objetivos de la organización y responda adecuadamente a los cambios en el entorno interno y externo. Este proceso garantiza que el plan sea siempre efectivo y esté listo para su activación en caso de ser necesario. Esta se revisión se realiza al menos una vez al año y, además, se programan revisiones adicionales en respuesta a eventos desencadenantes como cambios en la estructura organizativa, actualizaciones en la infraestructura tecnológica, o la aparición de nuevas amenazas.

Estas revisiones del BCP se basan en criterios como cambios en los procesos críticos, modificaciones en el entorno de TI, la aparición de nuevos riesgos, y lecciones aprendidas de incidentes anteriores o ejercicios de simulación. Después de cada revisión, cualquier actualización propuesta del BCP se presenta a la alta dirección para su aprobación, asegurando que las modificaciones se implementen de manera efectiva y se comuniquen adecuadamente a todo el personal involucrado.

4.3.7.4. Integración con el Sistema de Gestión de Seguridad de la Información (SGSI).

4.3.7.4.1. Relación entre BCP y SGSI.

El Plan de Continuidad de Negocio (BCP) en Innovatech Consulting no opera de manera aislada, sino que está estrechamente integrado con el Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa. Esta integración es esencial para asegurar que las medidas de continuidad del negocio se alineen con los requisitos de seguridad de la información y que ambos sistemas refuercen mutuamente la resiliencia de la organización.

Tanto el BCP como el SGSI comparten el objetivo común de proteger los activos críticos de Innovatech Consulting, garantizar la disponibilidad de los servicios, y preservar la confidencialidad e integridad de la información durante y después de cualquier interrupción.

Por otro lado, el BCP utiliza evaluaciones de riesgo y análisis de impacto desarrollados en el SGSI para identificar procesos críticos y determinar las estrategias de continuidad más adecuadas. Asimismo, los controles de seguridad establecidos en el SGSI son fundamentales para la efectividad del BCP, asegurando que las operaciones puedan continuar de manera segura durante una crisis.

Así mismo, en caso de un incidente de seguridad de la información o una interrupción significativa, el BCP y el SGSI se activan de manera coordinada, garantizando una respuesta integral que abarca tanto la recuperación operativa como la mitigación de impactos sobre la seguridad de la información.

4.3.7.4.2. Sinergias y beneficios.

La integración del BCP con el SGSI en Innovatech Consulting genera sinergias que fortalecen la capacidad de la organización para gestionar riesgos de manera efectiva y mejorar su resiliencia frente a interrupciones ya que, gracias a esta integración se facilita una visión global de los riesgos, permitiendo que Innovatech Consulting aborde simultáneamente los desafíos relacionados con la continuidad del negocio y la seguridad de la información.

Por otro lado, al combinar las capacidades del BCP y el SGSI, la empresa mejora su capacidad para resistir, responder y recuperarse de incidentes, minimizando el impacto en las operaciones y protegiendo los activos críticos.

Otra ventaja es que la integración reduce la duplicación de esfuerzos, ya que muchas de las medidas de seguridad necesarias para el SGSI también contribuyen a los objetivos del BCP. Esto optimiza el uso de recursos y asegura que las inversiones en seguridad y continuidad aporten el máximo valor a la organización.

Finalmente, la integración entre el BCP y el SGSI asegura que Innovatech Consulting cumpla con los requisitos normativos y las mejores prácticas establecidas por estándares como la ISO 27001:2022, proporcionando un marco robusto para la gestión de la seguridad de la información y la continuidad del negocio.

4.3.8. Metodología para el desarrollo de la Política de Seguridad de la Información.

Este capítulo tiene como objetivo detallar la metodología seguida por Innovatech Consulting para desarrollar su Política de Seguridad de la Información, una pieza clave en el Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022 ya que es fundamental para garantizar la protección de los activos de información de la empresa y asegurar el cumplimiento normativo.

Innovatech Consulting, en su proceso de adaptación y certificación bajo la norma ISO 27001:2022, reconoce la necesidad de establecer una política de seguridad de la información robusta que sea coherente con sus objetivos de negocio y con las mejores prácticas internacionales en gestión de la seguridad. Esta política no solo busca proteger los activos de

información, sino también generar confianza entre clientes, empleados y otras partes interesadas.

4.3.8.1. Proceso de desarrollo de la Política.

a) Análisis de requisitos y normativas: El primer paso en la creación de la Política de Seguridad de la Información fue la identificación y análisis de los requisitos legales, regulatorios y normativos que afectan a Innovatech Consulting. Este análisis incluyó la revisión de leyes locales, reglamentos específicos del sector y los requisitos de la norma ISO 27001:2022. Se llevaron a cabo entrevistas con los responsables de las distintas áreas de la empresa para garantizar que todos los aspectos relevantes fueran considerados.

b) Identificación de Activos y Riesgos: Para garantizar que la política abordara adecuadamente las necesidades de seguridad de la empresa, se realizó un inventario exhaustivo de los activos de información críticos. Paralelamente, se llevó a cabo un análisis de riesgos para identificar las amenazas y vulnerabilidades que podrían afectar a estos activos. Los resultados de este análisis permitieron definir las medidas de seguridad necesarias y priorizar los aspectos que debían ser cubiertos por la política.

c) Definición de principios de Seguridad: Con base en el análisis de riesgos y los requisitos normativos, se definieron los principios rectores de confidencialidad, integridad y disponibilidad. Estos principios forman el núcleo de la Política de Seguridad de la Información y guían todas las decisiones y acciones relacionadas con la protección de la información en Innovatech Consulting.

d) Asignación de roles y responsabilidades: La implementación efectiva de la política depende de una clara asignación de roles y responsabilidades. Se establecieron los roles clave, incluyendo los responsables de la gestión del SGSI, la dirección y los empleados, definiendo sus responsabilidades específicas en la aplicación y mantenimiento de la política. Esta asignación se basó en la estructura organizativa y en las competencias de cada área.

e) Revisión y aprobación de la Política: Una vez elaborada la política, se sometió a un proceso de revisión interna para asegurar que cumpliera con los objetivos de seguridad de la empresa y los requisitos de la norma ISO 27001:2022. Este proceso incluyó la revisión por parte de la alta dirección, quienes aportaron su feedback antes de dar su aprobación final. La política fue formalmente aprobada y adoptada por Innovatech Consulting, garantizando así su alineación con la estrategia corporativa de la empresa y su aplicabilidad en todo el SGSI.

4.3.8.2. Implementación de la Política de Seguridad.

Para asegurar que todos los empleados de Innovatech Consulting comprendieran y aplicaran la Política de Seguridad de la Información, se desarrolló un plan de comunicación y capacitación. Este plan incluyó la difusión de la política a través de múltiples canales, como reuniones, correos electrónicos y la plataforma de uso interno montada en NormaPro, así como la realización de sesiones de formación específicas para los diferentes niveles de la empresa.

La Política de Seguridad de la Información ha sido integrada en el SGSI de Innovatech Consulting, asegurando que todos los procesos, procedimientos y controles de seguridad se alinearan con los principios y directrices establecidos en la política. Esto se logró mediante la actualización de documentos y procedimientos existentes y la incorporación de nuevos controles cuando fue necesario.

También se establecieron mecanismos de monitorización para asegurar que la Política de Seguridad de la Información se aplicara consistentemente en toda la organización. Estos mecanismos incluyeron auditorías internas, revisiones periódicas de cumplimiento y el uso de herramientas de monitorización para detectar y corregir posibles incumplimientos de manera proactiva.

4.3.8.3. Revisión y mejora continua de la Política de seguridad.

La política está sujeta a revisiones periódicas para asegurar que siga siendo relevante y efectiva ante los cambios en el entorno de seguridad y las operaciones de la empresa. Estas revisiones se programan al menos una vez al año, o cuando se producen situaciones sobrevenidas como incidentes de seguridad, cambios significativos en la organización o en el entorno externo que puedan afectar la seguridad de la información.

Por otro lado, Innovatech Consulting se compromete a la mejora continua de su Política de Seguridad de la Información. Las lecciones aprendidas de incidentes de seguridad, auditorías internas y cambios en la normativa se incorporan de manera sistemática en la política, garantizando que esta evolucione junto con las necesidades de la empresa y las mejores prácticas del sector.

4.4. Herramientas y recursos utilizados.

En este capítulo, se describen las herramientas y recursos que se han utilizado a lo largo de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en Innovatech Consulting, conforme a la norma ISO 27001:2022. Estas herramientas han sido fundamentales tanto en la elaboración de este Trabajo de Fin de Grado (TFG) como en la

implementación efectiva de las políticas y procedimientos de seguridad en la empresa. Cada sección siguiente detalla las herramientas y recursos específicos empleados en diferentes fases y áreas clave del SGSI.

A) Para la Evaluación de Riesgos (Cláusula 6.1.2):

- **Herramientas utilizadas**: Para realizar la evaluación de riesgos se utilizaron hojas de cálculo en Microsoft Excel para el análisis cuantitativo y cualitativo de los riesgos.
- **Recursos adicionales**: Documentación de estándares ISO 27005 para la gestión de riesgos de seguridad de la información, así como guías de mejores prácticas en la industria.

B) Para el Plan de Acción basado en la Evaluación de Riesgos:

- **Herramientas utilizadas**: Se utilizó Microsoft Project para la planificación, seguimiento y gestión de las acciones de mitigación. Esta herramienta permitió la asignación de tareas, plazos y responsables, facilitando el seguimiento del progreso de las acciones.
- **Recursos adicionales**: Guías metodológicas de gestión de proyectos y normativas internas de Innovatech Consulting para la implementación de medidas correctivas y preventivas.

C) Para el análisis del Riesgo y Plan de Acción de las partes interesadas:

- **Herramientas utilizadas**: Se emplearon matrices de evaluación de partes interesadas en Microsoft Excel, así como para determinar el nivel de poder e interés de cada parte interesada. También se utilizó software como Azure Devs para facilitar la gestión y comunicación con las partes interesadas.
- **Recursos adicionales**: Documentación sobre mejores prácticas en gestión de partes interesadas y normativas de cumplimiento regulatorio.

D) Para el establecimiento de Objetivos e Indicadores de Seguridad:

- **Herramientas utilizadas**: Se emplearon hojas de cálculo en Microsoft Excel para la definición y seguimiento de los indicadores clave de rendimiento (KPI). Además, se empleó NormaPro para la monitorización de los indicadores de seguridad.
- **Recursos adicionales**: Guías de implementación de KPIs en seguridad de la información y referencias a estándares como ISO 27004 para medir la efectividad del SGSI.

E) Declaración de Aplicabilidad (SOA):

- **Herramientas utilizadas**: Para la elaboración de la SOA, se empleó un software de gestión documental como **SharePoint** y **NormaPro**, que permitió mantener la trazabilidad y versionado del documento. Se utilizó también Microsoft Excel para el mapeo de los controles del Anexo A de la ISO 27001:2022.
- **Recursos adicionales**: Directrices de la ISO 27001 y guías sobre la elaboración de la SOA.

F) Automatización del SGSI en Microsoft Azure:

- **Herramientas utilizadas**: **Microsoft Defender for Cloud** fue la herramienta principal utilizada para automatizar la implementación y monitorización de controles de seguridad. Esta herramienta permite una gestión centralizada y continua de la seguridad en el entorno en la nube.
- **Recursos Adicionales**: Documentación de Microsoft Azure sobre mejores prácticas de seguridad y guías de implementación de controles en la nube.

G) Plan de Continuidad de negocio:

- **Herramientas utilizadas**: **Microsoft Azure Site Recovery** se consultó para la planificación y ejecución de estrategias de recuperación ante desastres.
- **Recursos adicionales**: Normativas de la ISO 22301 sobre gestión de continuidad del negocio y guías de recuperación ante desastres específicas para entornos en la nube.

H) Política de Seguridad de la Información:

- **Herramientas Utilizadas**: **Microsoft Word** para la redacción y revisión colaborativa de la política, SharePoint y NormaPro para la gestión documental y control de versiones.
- **Recursos Adicionales**: Plantillas de políticas de seguridad de la información y guías de alineación con la ISO 27001:2022.

5. RESULTADOS Y DISCUSIÓN.

5.1. RESULTADOS DE LA EVALUACIÓN DE RIESGOS (CLÁUSULA 6.1.2).

5.1.1. Resultados del análisis de Activos.

El análisis llevado a cabo puede observarse con detalle en la **Tabla 8** siguiente en la que se identificaron y valoraron los activos en cada una de las categorías mencionadas y se tratarán elementos de riesgos con valores de activos por encima de >3 para lo que se marcan las casillas correspondientes en rojo. Dicha valoración final proviene de hallar la media aritmética de las valoraciones de la **Disponibilidad, Confidencialidad e Integridad** de acuerdo a los criterios establecidos en las Tablas 1, 2 y 3.

a) **EQUIPOS:** En la tabla "Riesgos Asociados a los Equipos" se presenta una evaluación detallada de los riesgos de los equipos en función de las tres dimensiones clave: disponibilidad, confidencialidad e integridad. Estos valores determinan el "Valor Activo", que se calcula como la media de estas tres valoraciones. A continuación, se destacan algunos puntos relevantes:

Equipos con Valoraciones Elevadas:

- **Thinkpad E15 (IHM)**: Este equipo tiene una valoración alta (4) debido a su alta disponibilidad y confidencialidad (4). Al ser un equipo que maneja software crítico como Microsoft Office 365 y programas contables, se considera fundamental para las operaciones diarias. Sin embargo, la integridad del equipo está valorada en 3, debido a que los programas contables no funcionan en la nube, lo que añade un factor de riesgo.
- **INICIE IT DESK01 (AT)**: Este equipo tiene un papel crucial ya que contiene las llaves de acceso a todos los servicios informáticos de la empresa. Aunque su confidencialidad está bien protegida (valor 4), la disponibilidad e integridad (valor 2 y 1, respectivamente) muestran que se han tomado medidas importantes, como el uso de VPN en Azure y copias de seguridad en GitHub, para mitigar los riesgos. Aun así, el valor global del activo es 2, lo que indica que sigue siendo un área a mejorar en términos de disponibilidad e integridad.

Monitores y Equipos de Bajo Riesgo:

- Los monitores (3 a 7) presentan un bajo nivel de riesgo, con valores de disponibilidad, confidencialidad e integridad todos en 2 o 1. Esto es lógico, ya que estos dispositivos

no manejan información crítica o confidencial y su impacto en la seguridad de la información es limitado.

Portátiles con Información Relevante:

- El **Thinkpad E15 (JA)** y el **Portatil Lenovo Thinkpad E15 (JMG)** destacan por manejar información relevante a ventas, clientes, y desarrollo corporativo. Aunque su disponibilidad es baja (1), el respaldo de toda la documentación en OneDrive garantiza que la información se puede recuperar rápidamente en caso de desastre. Esto reduce significativamente el riesgo, haciendo que ambos equipos tengan una valoración global de 3.

Observaciones y Supervisión del Riesgo:

- Es importante notar que todos los equipos cuentan con un supervisor asignado para gestionar los riesgos asociados. Las observaciones indican que se han tomado medidas concretas para reducir los riesgos, como el uso de respaldos y herramientas de recuperación de datos. Esto refleja un enfoque proactivo en la gestión de riesgos, donde se implementan controles adicionales para garantizar la disponibilidad y recuperación de la información.

b) **APLICACIONES:** En general, la tabla resalta que las aplicaciones asociadas a la gestión de bases de datos y la producción son las que requieren más atención en cuanto a la confidencialidad, mientras que otras herramientas más comunes presentan riesgos más bajos debido a su menor relevancia en términos de información crítica. Esto demuestra la necesidad de priorizar los controles en los activos más sensibles de la organización. A continuación, se presentan algunos comentarios prácticos relacionados con los datos obtenidos en la tabla:

1. **Aplicaciones de Office 365 Business y Windows 10**:
    - Ambas aplicaciones presentan un valor bajo en términos de disponibilidad, confidencialidad e integridad, lo que refleja su naturaleza más operativa y la existencia de controles robustos ya implementados. Estas aplicaciones son ampliamente utilizadas, y la información sensible que manejan es mínima, lo que justifica el bajo valor del riesgo asociado a estas herramientas.
2. **Aplicaciones con acceso a bases de datos y control de versiones (GITHUB, MySQL Workbench)**:

- En el caso de GitHub y MySQL Workbench, la confidencialidad recibe una valoración alta (5). Esto es lógico, ya que ambas aplicaciones están directamente relacionadas con la gestión y desarrollo de código fuente, así como la administración de bases de datos, lo que las convierte en activos de información crítica. Aquí, se debe garantizar un control más estricto para prevenir fugas de información o acceso no autorizado.
- En ambos casos, el valor activo es de "2", lo que indica que, aunque se reconoce el riesgo, los controles existentes reducen considerablemente el impacto y la probabilidad de incidentes críticos.

3. **Aplicaciones de gestión de ficheros y producción (WIN SCP, FileZilla)**:
   - Estas aplicaciones están vinculadas con la transferencia y el acceso a servidores de producción, lo que genera una mayor valoración de confidencialidad (5). Los controles de acceso en estas aplicaciones son cruciales, dado que un acceso no autorizado podría comprometer información en producción, afectando la operación global de la empresa. Aquí, el riesgo es moderado, reflejado en un valor activo de "2".
4. **Antivirus y Navegadores (Chrome, Firefox, Windows Defender)**:
   - Estas aplicaciones se evalúan como activos de bajo riesgo en cuanto a disponibilidad, confidencialidad e integridad, dado que son herramientas estándar dentro de cualquier entorno empresarial. Sin embargo, se debe asegurar que las actualizaciones automáticas y las configuraciones de seguridad estén siempre habilitadas para prevenir vulnerabilidades en estas aplicaciones.
5. **Azure DevOps**:
   - Esta herramienta, utilizada para la gestión de proyectos, tiene un valor activo de "1", lo cual indica un bajo riesgo percibido. A pesar de su importancia para el desarrollo y la coordinación de proyectos, los mecanismos de seguridad y control establecidos son adecuados para mantener los riesgos en un nivel mínimo.

c) **SERVIDORES:** La parte de la **Tabla 8** referida a los servidores muestra claramente que los más críticos para el desarrollo (Scaleway y Azure) requieren un mayor enfoque en la seguridad para garantizar tanto la disponibilidad como la confidencialidad. Los servidores menos críticos, como el hosting de IONOS y GitHub, aunque importantes,

no necesitan el mismo nivel de intervención. A continuación, se realizan algunos comentarios clave basados en esta información:

Cluster Scaleway y Cluster Azure:

- Estos servidores tienen la máxima calificación en términos de **disponibilidad** y **confidencialidad** (5), lo cual es lógico, ya que almacenan los últimos códigos en desarrollo y servidores en proceso. La alta disponibilidad asegura que las operaciones de desarrollo no se vean interrumpidas y que los datos críticos estén siempre protegidos.
- Sin embargo, la **integridad** se ha evaluado con un valor bajo (1). Esto podría deberse a la naturaleza del entorno de desarrollo, donde se espera que los datos cambien con frecuencia, por lo que la precisión o completitud no es tan crítica como en entornos de producción.
- Ambos servidores presentan un **valor activo alto (4)**, lo que indica la necesidad de controles estrictos para mantener la disponibilidad y confidencialidad.

Servidor hosting IONOS:

- Este servidor, que hospeda la web corporativa, tiene un riesgo bajo en todos los aspectos (1 en disponibilidad, confidencialidad e integridad). Esto indica que, aunque se trata de un servidor de producción, los datos gestionados no son críticos o sensibles, lo que reduce considerablemente el nivel de riesgo.
- El **valor activo** es bajo (1), lo que significa que no es necesario asignar demasiados recursos a la gestión de riesgos para este servidor en particular.

GitHub:

- GitHub, como repositorio de código fuente, obtiene una valoración máxima en **confidencialidad (5)**, lo cual es apropiado, ya que los proyectos en desarrollo y las propiedades intelectuales deben estar protegidos contra accesos no autorizados.
- La **disponibilidad** se ha calificado con un valor moderado (3), lo que indica que, aunque es importante, no es absolutamente crítico que esté disponible en todo momento.
- La **integridad** nuevamente se evalúa con un valor bajo (1), posiblemente debido a la naturaleza flexible del código en desarrollo, que puede cambiar con frecuencia sin un impacto directo en la operación.

- El **valor activo** de GitHub es de 3, lo que sugiere que, si bien es importante, no requiere el mismo nivel de atención que los servidores de desarrollo de Scaleway o Azure.

d) **PERSONAS:** En la parte de la Tabla 8 en la que se analizan los **Riesgos Asociados a las Personas**, se muestra una clasificación del riesgo vinculado a los perfiles de los distintos roles dentro de la organización y permite priorizar las medidas de seguridad y los controles en función del valor activo y la criticidad de los datos gestionados por cada persona. A continuación, se exponen algunos comentarios basados en los datos referidos:

Perfil Administrativo:

- Maneja información contable, considerada con una **confidencialidad e integridad** baja (2 y 1, respectivamente). Esto se debe a que, si bien la información contable es importante, no es tan sensible ni crítica como otros tipos de información.
- La **disponibilidad** del perfil se valora en 3, lo que indica que es moderadamente importante que el personal administrativo esté disponible para mantener las operaciones de la empresa.
- **Valor activo**: 2, lo que sugiere que el riesgo asociado a este perfil es relativamente bajo.

Técnicos NormaPro y Desarrolladores de software:

- Ambos perfiles manejan información de clientes o código fuente, con un enfoque en mantener la **confidencialidad** en nivel moderado (2). La **disponibilidad** también es de nivel medio (3), lo que indica que estas personas son necesarias para mantener los sistemas y la documentación de clientes.
- **Valor activo**: 2 y 3, respectivamente, lo que muestra que los técnicos tienen una importancia significativa, pero no tan crítica como otros roles, como el Administrador de Sistemas y DBA.

Responsable de TI y Dirección General:

- Estos roles manejan toda la información (excepto la contable y el código fuente) con una **confidencialidad e integridad** más altas (3). La alta importancia de la información que gestionan, unida a su nivel de responsabilidad, hace que su **disponibilidad** también sea crítica (3).

- **Valor activo**: 3, lo que refleja la importancia de estas personas en la gestión operativa y estratégica de la empresa.

Administrador de Sistemas y DBA:

- Este rol tiene un valor **crítico** en la organización, ya que maneja sistemas, bases de datos y datos sensibles como la contabilidad, facturación, RRHH y clientes. Tiene la mayor **disponibilidad** (5), lo que indica que es esencial que esté siempre disponible para evitar paradas operativas.
- **Confidencialidad e integridad** son de niveles medios (4 y 3), lo que refleja la necesidad de proteger y mantener la exactitud de la información gestionada.
- **Valor activo**: 4, lo que destaca la alta criticidad del rol en la continuidad y seguridad de los sistemas de la empresa.

Comercial y Subcontratas:

- Ambos perfiles manejan datos menos críticos como los **datos de clientes** o información variada. Se observan **niveles medios-bajos** de confidencialidad e integridad (2), mientras que la **disponibilidad** se mantiene en niveles intermedios (3).
- **Valor activo**: 2 y 3, reflejando que, aunque importantes, no son roles críticos en comparación con los responsables de sistemas o la dirección general.

e) **SERVICIOS**: La tabla muestra que los servicios con más alto riesgo son aquellos relacionados con la Prestación de Servicios NormaPro y la Gestión de la Web, donde se maneja información crítica y/o pública y se requiere una alta disponibilidad.

Gestión Web INICIE:

- La **disponibilidad** es alta (4), lo que refleja la importancia de mantener el servicio web accesible en todo momento ya que la información publicada es de carácter público.
- La **confidencialidad,** en este caso, es relativamente baja (2), ya que la información no es sensible, pero la **integridad** tiene una puntuación alta (4), lo que significa que la exactitud de la información publicada es crucial.
- **Valor activo**: 3, lo que indica un riesgo moderado, dado que la información es pública, pero la integridad es prioritaria para mantener la confianza en la organización.

Gestión de Servicios de Ingeniería y Consultoría:

- Con un valor bajo en **disponibilidad, confidencialidad** e **integridad** (2, 2 y 2), este servicio no presenta un riesgo crítico, aunque es importante mantener la información de los proyectos de ingeniería protegida y disponible.
- **Valor activo**: 2, reflejando que el riesgo es relativamente bajo, ya que la información no es extremadamente sensible o crítica para la operación diaria de la empresa.

Gestión Comercial:

- La **disponibilidad** es moderada (3), y tanto la **confidencialidad** como la **integridad** tienen un valor medio (2), lo que indica que la información de los clientes, aunque importante, no es crítica ni de alto riesgo.
- **Valor activo**: 2, lo que indica que, si bien es importante proteger los datos de los clientes, el riesgo no es alto.

Prestación de Servicios NormaPro:

- Este servicio es el que presenta un riesgo más elevado. Tanto la **disponibilidad** (4) como la **confidencialidad** (4) son altos, lo que refleja la necesidad de que el servicio esté siempre disponible y que la documentación de los clientes esté debidamente protegida.
- La **integridad** es también alta (3), lo que significa que es vital que la información se mantenga precisa y sin alteraciones.
- **Valor activo**: 4, lo que lo convierte en un servicio crítico dentro de la organización. Cualquier fallo en este servicio podría tener un impacto significativo en la operación y en la confianza de los clientes.

Gestión Administrativa y Económica:

- La **disponibilidad** es moderada (3), ya que la contabilidad y la facturación deben estar accesibles con frecuencia. La **confidencialidad** y la **integridad** son valores medios (2), lo significa que, aunque estos datos deben protegerse, el riesgo no es extremadamente alto.
- **Valor activo**: 3, lo que refleja un riesgo moderado para la operación de la empresa.

Atención a Clientes:

- Se observa una **alta disponibilidad** (4), lo que significa que es crucial que esté siempre accesible para los clientes. Tanto la **confidencialidad** como la **integridad** son bajas (1), lo que indica que la información no es especialmente sensible o crítica.
- **Valor activo**: 2, reflejando un riesgo bajo.

Gestión de Personal:

- Con una **disponibilidad** baja (2) y una **confidencialidad** alta (4), es evidente que la protección de los datos de nóminas es crítica, pero no es necesario que estén siempre accesibles. La **integridad** también es moderada (2).
- **Valor activo**: 3, lo que refleja un riesgo moderado, dada la importancia de proteger la información personal y financiera de los empleados.

f) **SERVICIOS**: Aunque la oficina contiene información importante, el bajo valor asignado a la disponibilidad, confidencialidad e integridad muestra que la dependencia de la oficina física es mínima para las operaciones de InnovaTech Consulting, reflejando una clara estrategia de externalización de servicios críticos a plataformas digitales:

- **Información**: Se menciona que la oficina alberga "toda la información de la organización", lo que normalmente implicaría un riesgo elevado. Sin embargo, se ha evaluado tanto la **disponibilidad**, la **confidencialidad**, y la **integridad** con un valor de 1, lo que denota que la oficina no juega un papel esencial en la disponibilidad o manejo de la información más crítica.
- **Localización**: La oficina se encuentra en una dirección física concreta (Calle Suspiro Verde, N°35), pero no se refleja una necesidad alta de protección o disponibilidad ya que las operaciones críticas de la organización están alojadas en la nube o en ubicaciones remotas que no dependen de esta oficina física.
- **Valor activo**: Con un valor activo de **1**, se concluye que las instalaciones no representan un riesgo significativo para las operaciones de la empresa. Esto es debido a que gran parte de la infraestructura tecnológica y de seguridad se ha externalizado a servicios en la nube, por lo que la pérdida de acceso a las oficinas no tendría un impacto considerable en la continuidad operativa.
- **Responsable del riesgo**: La responsabilidad del riesgo ha sido asignada a **AT**, lo que indica que el control de esta área está bajo supervisión, pero no requiere una monitorización intensiva, dada la baja criticidad de este activo.

Tabla 8: Análisis de activos.

CONSIDERACIONES:
1.- Todos los activos se valoran de [1-5], los elementos de DISPONIBILIDAD-CONIFIDENCIALIDAD-INTEGRIDAD.

2.- Se tratarán elementos de riesgos con valores de activos por encima de >3, se marcará la casilla en rojo.

Nivel de Disponibilidad	Criterio de Evaluación	Descripción del Impacto
1 - Bajo	El activo no es crítico para la operación diaria, su falta de disponibilidad no afecta significativamente a la continuidad del negocio.	El activo puede estar fuera de servicio durante largos periodos (días o semanas) sin afectar gravemente las operaciones o productividad de la empresa.
2 - Medio (-)	El activo es importante pero su inactividad puede ser tolerada por periodos limitados (horas o hasta un día) sin grandes impactos.	La falta de disponibilidad puede generar ciertas ineficiencias, pero existen mecanismos o recursos alternativos que permiten la continuidad operativa.
3 - Medio (+)	El activo es importante para la operación diaria, pero la empresa puede tolerar su inactividad durante un corto periodo (horas).	La falta de disponibilidad causa inconvenientes y pérdida de productividad, pero no detiene las operaciones críticas si se soluciona rápidamente.
4 - Alto	El activo es crucial para el funcionamiento de varios procesos de negocio, su inactividad causa interrupciones significativas.	La falta de disponibilidad del activo por periodos cortos (horas) afecta seriamente la productividad, generando pérdidas de eficiencia y posibles retrasos.
5 - Crítico	El activo es vital para las operaciones de la empresa, su inactividad implica la paralización completa o casi completa del negocio.	La falta de disponibilidad incluso por periodos cortos (minutos) genera graves problemas operativos y financieros, afectando a procesos críticos.

Nivel de Confidencialidad	Criterio de Evaluación	Descripción del Impacto
1 - Bajo	El acceso no autorizado al activo tiene un impacto insignificante o nulo.	La información contenida en el activo no es sensible ni confidencial, y su divulgación no genera ningún riesgo o daño para la organización.
2 - Medio (-)	El acceso no autorizado al activo puede causar molestias menores, pero no tiene un impacto significativo.	La información es de baja sensibilidad, y aunque su divulgación no es ideal, no compromete gravemente los intereses de la organización.
3 - Medio (+)	El acceso no autorizado al activo puede causar inconvenientes y posibles impactos en áreas no críticas de la organización.	La información es algo sensible, y su divulgación podría generar cierto nivel de impacto, aunque no comprometería los activos críticos.
4 - Alto	El acceso no autorizado al activo comprometería información sensible y tendría un impacto significativo en la organización.	La información es confidencial y su divulgación causaría daños importantes, afectando la competitividad, reputación o el cumplimiento legal.
5 - Crítico	El acceso no autorizado al activo tendría consecuencias graves o catastróficas para la organización.	La información es extremadamente sensible (p.ej. datos personales, financieros, propiedad intelectual) y su divulgación tendría consecuencias legales o financieras graves.

Nivel de Integridad	Criterio de Evaluación	Descripción del Impacto
1 - Bajo	La exactitud o completitud de la información contenida en el activo tiene poca o ninguna relevancia para la organización.	La corrupción o modificación de la información contenida en el activo no afectaría significativamente el funcionamiento o decisiones.
2 - Medio (-)	La exactitud o completitud de la información es deseable pero no crítica.	La información puede contener errores menores o modificaciones sin que afecte significativamente la operación, aunque es preferible evitarlo.
3 - Medio (+)	La exactitud y completitud de la información es importante, aunque un pequeño error o modificación podría ser corregido fácilmente.	Los errores en la información pueden causar inconvenientes, pero pueden ser identificados y corregidos sin gran impacto en el funcionamiento.
4 - Alto	La exactitud y completitud de la información es crucial para la operación, cualquier error puede tener un impacto significativo.	La corrupción o modificación no detectada podría tener efectos graves, como decisiones operativas incorrectas o afectación de la calidad del servicio.
5 - Crítico	La exactitud y completitud de la información es vital; cualquier error o modificación tendría consecuencias graves.	La corrupción o modificación no detectada podría llevar a pérdidas financieras, daños legales o graves impactos operativos.

Innovatech Consulting

Fecha última revisión: 4/03/2024 (inicio 2024)

Riesgos Asociados a los Equipos

EQUIPO	INFORMACIÓN	RESPONSABLE	Nº SERIE	RAM (Gb)	SOFTWARE	DISPONIB	CONFID	INTEGR	VALOR ACTIVO	SUPERVISOR RIESGO
Thinkpad E15	Sin información	IHM		4	Microsoft Office 365 Home, Factusol LogoConta Microsoft Windows Defender	4	4	3	4	AT
TABLET 1 SAMSUNG SM-T713	Registros de auditoría que se vuelcan al finalizar	AT	R52H70KP0EP	4	Audire Pro	2	2	1	2	AT
TABLET 2 SAMSUNG SM-T713	Registros de auditoría que se vuelcan al finalizar	AT	R52H50Z388K	6	Audire Pro	2	2	1	2	AT
PORTATIL 2 LENOVO YOGA 500 14.9 K-80R5	Sin información	DP	R9N0B5924001	8	Microsoft Office 365 Home Microsoft Windows Defender	3	2	1	2	AT
INICIE IT DESK01. Intel Core ™ i7-8700k CPU	Todas las llaves de acceso a todos los servicios informáticos vinculados con la empresa.	AT	AD86AF78-FB4C-48F7-8C7F-E7FEF0473F32	16	Visual Estudio Code, Github Desktop, MySQL Workbench, WINSCP, Ubuntu 20,04 LTS, FileZilla, Google Chrome	2	4	1	2	AT
Monitor 3 ASUS 22 PUL VH228D	Sin información	AT	B8LMTF133939			2	2	1	2	AT
Monitor 4 LG FLATRON (19) L192WS-SNQAEUQQP	Sin información	AT	802UXTC11361			2	2	1	2	AT
MONITOR 5 LG FLATRON L1754SMS	Sin información	AT	BEJL1754SMS			2	2	1	2	AT
MONITOR 6 FLATRON L1754SMS	Sin información	NM	708NDNU3U399			2	2	1	2	AT
MONITOR 7 LG FLATRON E2211SX	Sin información	JA	111NDWE0D329			2	2	1	2	AT
Thinkpad E15	Información relevante a ventas, clientes y proyectos	JA		8	Microsoft Office 365 Home Microsoft Windows Defender	1	4	3	3	AT
Samsung S20 FE 4g 128Gb	Sin información	JA	F2LTVDCCMHG04		Android 11	2	2	1	2	AT
PORTATIL 5 LENOVO YOGA 500	Sin información	DP	R90HENE6		Microsoft Office 365 Home Microsoft Windows Defender	3	3	1	2	AT
Portatil Lenovo Thinkpad E15	Información relevante a la compañía, desarrollo corporativo	JMG			Windows 11, Microsoft Office 365, Cantasia Studio 9.	1	4	3	3	AT
INICIE IT DESK02. Intel Core ™ i7-8700k CPU	Sin información	JMGH	C68999ED-17BE-47F9--A3F9-C0F95F3D50A8	16	Microsoft Office 365 Home Virtual Box, Visual Estudio Code, Visual Estudio, Github Desktop, MySQL Workbench, WINSCP, Ubuntu 18.08 WSL, Filecilla, Google Chrome, Mozilla FireFox, Microsoft Windows Defender	1	1	1	1	AT

Riesgos Asociados a las Aplicaciones

APLICACIONES	INFORMACIÓN	EMPRESA	LICENCIA	Uds.	UTILIDADES	DISPONIB	CONFID	INTEGR	VALOR ACTIVO	REPONSABLE RIESGO
OFFICE 365 Bussiness	Sin información	MICROSOFT	LICENCIA DIGITAL SUSCRIP- ANUAL	10	Editor de texto, hoja de cáclculo, correo electrónico	1	1	1	1	Comité SIG
WINDOWS 10	Sin información	MICROSOFT	LICENCIA DIGITAL	10	Sistema Operativo	1	1	1	1	Comité SIG
MICROSOFT VISUAL STUDIO CODE	Sin información	MICROSOFT	LICENCIA GPL	4	Herrmienta de Desarrollo de código para desarrollos internos	1	1	1	1	Comité SIG
GITHUB DESKTOP	Repositorio de código fuente de los proyectos de software	GITHUB	LICENCIA GPL	4	Control de versiones	1	5	1	2	Comité SIG
MY SQL WORKBENCH	Acceso a las bases de datos	ORACLE	LICNECIA GPL	4	Herrmienta de Desarrollo de código para desarrollos internos/ Gestor BBDD	1	5	1	2	Comité SIG
WIN SCP	Acceso a los servidores de producción	WIN SCP	LICENCIA GPL	4	Gestor de Ficheros	1	5	1	2	Comité SIG
FILEZILLA	Acceso a los servidores de producción	MOZILLA	LICENCIA GPL	4	Gestor de Ficheros	1	5	1	2	Comité SIG
CHROME	Sin información	GOOGLE	LIBRE	10	Navegador	1	1	1	1	Comité SIG
FIREFOX	Sin información	MOZILLA	LIBRE	10	Navegador	1	1	1	1	Comité SIG
MICROSOFT WINDOWS DEFENDER	Sin información	MICROSOFT	LICENCIA DIGITAL	10	Antivirus	1	1	3	2	Comité SIG
Azure Devops	Sin información	Microsoft	LICENCIA DIGITAL	10	Gestor de proyectos	1	1	1	1	Comité SIG

Riesgos Asociados a los Servidores

DIRECCIÓN IP	INFORMACIÓN		ENTORNO		DESCRIPCIÓN	DISPONIB	CONFID	INTEGR	VALOR ACTIVO	REPONSABLE RIESGO
Cluster Scaleway	Contiene los últimos fuentes en desarrollo		Desarrollo (virtual scaleway)			5	5	1	4	AT
Cluster Azure	Servidores en Desarrollo		Azure			5	5	1	4	AT
Servidor hosting IONOS	Servidor WebCorporativa (Hosting mantenido)		Servidor Web		Ionos 1&1	1	1	1	1	AT
GITHUB	Código fuente de las aplicaciones		Servidor de Git		Github	3	5	1	3	AT

Riesgos Asociados a la Telefonía Fija

EQUIPO	INFORMACIÓN	RESPONSABLE	Nº SERIE	RAM (Gb)	MARCA	DISPONIB	CONFID	INTEGR	VALOR ACTIVO	REPONSABLE RIESGO
TELEFONO MOVISTAR UNIFY	Sin información	IH	953190510		UNIFY	1	1	1	1	AT

Riesgos Asociados a las Personas

PERFIL	INFORMACIÓN	RESPONSABLE				DISPONIB	CONFID	INTEGR	VALOR ACTIVO	REPONSABLE RIESGO
Administrativo	Contabilidad	Dirección				3	2	1	2	JMGR
Técnicos NormaPro	Documentación de clientes	Dirección				3	2	1	2	AT
Desarrollador de software	Codigo fuente	Administrador de Sistemas y DBA				3	2	1	2	AT
Técnicos de Proyectos Ingeniería y MA	Proyectos de clientes	Dirección				3	2	1	2	AT
Responsable de TI	Toda la información excepto información contable	Dirección				3	3	3	3	AT
Dirección General	Toda la información excepto código fuente	Dirección				3	3	3	3	JMGR
Dirección Financiera	contabilidad y finanzas	Dirección				3	3	3	3	AT
Responsable del SIG	documentación referente a sistemas de gestión	Dirección				3	2	1	2	AT
Comercial	datos de clientes	Dirección				3	2	1	2	AT
Administrador de Sistemas y DBA	sistemas y bases de datos	Dirección				5	4	1	3	AT
Subcontratas	contabildiad, facturación, RRHH, codigo fuente y clientes	Dirección				3	2	1	2	AT

Riesgos Asociados a los Servicios

SERVICIO	INFORMACIÓN		RESPONSABLE			DISPONIB	CONFID	INTEGR	VALOR ACTIVO	REPONSABLE RIESGO
Gestión Web	Información publica		Dirección			4	2	4	3	AT
Gestión de Servicios de Ingeniería y Consultoria	Información de proyectos de ingeniería		Dirección			2	2	2	2	AT
Gestión Comercial	Información de clientes		Dirección			3	2	2	2	AT
Prestación Servicios NormaPro	Documentación de los clientes		Dirección			4	4	3	4	AT
Gestión Administrativa y Económica	Contabilidad y facturación		Dirección			3	2	3	3	AT
Atención Clientes	Sin información		Dirección			4	3	2	3	AT
Gestión de Personal	Nóminas		Dirección			2	4	2	3	AT

Riesgos Asociados a las Instalaciones

INSTALACION	INFORMACIÓN	RESPONSABLE	LOCALIZACIÓN	SERVICIO	DISPONIB	CONFID	INTEGR	VALOR ACTIVO	REPONSABLE RIESGO
Oficinas	Toda la información de la organización	JMGR	Calle Suspiro Verde, Nº35.	Oficinas	1	1	1	1	AT

5.1.2. Resultados de la identificación de Amenazas y Vulnerabilidades.

Las medidas de mitigación prioritarias se deben enfocar en las amenazas y vulnerabilidades que han sido identificadas como las más probables y de mayor impacto para los activos críticos de **InnovaTech Consulting**. Basado en la identificación de riesgos del capítulo anterior, se procede a realizar el análisis de las amenazas y vulnerabilidades cuyos resultados pueden observarse con detalle en la **Tabla 9** siguiente, resaltando en rojo, las amenazas y vulnerabilidades consideradas probables por cada tipología de activo.

A partir de la tabla mencionada, se puede observar que en el proceso de identificación de amenazas y vulnerabilidades, se ha llevado a cabo un análisis detallado según el tipo de activo (servidores, equipos, aplicaciones y servicios).

A continuación, algunos comentarios prácticos como ejemplo de resultados reales basados en lo observado:

1. Amenazas naturales:

- **Fuego y daños por agua:** Estas amenazas han sido consideradas probables para los servidores y equipos, resaltadas en **rojo**, lo cual es un reconocimiento de la alta vulnerabilidad que tienen estas infraestructuras ante eventos físicos. Es razonable que los servidores y equipos, siendo elementos críticos en la operativa de InnovaTech Consulting, estén expuestos a este tipo de desastres, lo que sugiere la necesidad de implementar medidas preventivas como sistemas de extinción de incendios y detección de fugas de agua.
- **Otras amenazas naturales**: No se consideran probables (marcadas en **azul**) para aplicaciones y servicios, lo que puede ser explicado por la naturaleza intangible de estos activos. Aunque son vulnerables, las aplicaciones y servicios suelen alojarse en infraestructuras en la nube que ofrecen altos niveles de seguridad física y protección ante desastres.

2. Amenazas de origen industrial:

- **Contaminación mecánica y electromagnética:** Estas amenazas son marcadas en **rojo** para servidores y equipos, lo cual resalta su exposición a interferencias mecánicas y electromagnéticas en su entorno. Esto podría deberse a la localización física de los servidores, probablemente en un centro de datos donde existen equipos electrónicos potentes que generan campos electromagnéticos. Es vital contar con sistemas de protección electromagnética en estas áreas.

- **Avería de origen físico o lógico:** Es interesante ver que esta amenaza se considera probable para aplicaciones, resaltada en **rojo**. Esto implica que los desarrolladores han identificado posibles fallos lógicos que pueden afectar la operativa de las aplicaciones críticas de InnovaTech Consulting, como bases de datos o control de versiones, que son clave para el negocio. Es necesario implementar controles adicionales para mitigar estos riesgos, como redundancia de sistemas y recuperación ante fallos.
- **Corte del suministro eléctrico y condiciones ambientales inadecuadas:** Estas amenazas están resaltadas para los servidores, lo que refleja un riesgo operacional importante. Es fundamental disponer de sistemas de alimentación ininterrumpida (SAI) y reguladores de temperatura/humedad, ya que cualquier interrupción en el servicio eléctrico o condiciones ambientales desfavorables podrían impactar directamente en la disponibilidad de los servidores y, por ende, en los servicios prestados.

3. Conclusión general:

- El uso del código de colores (rojo y azul) refleja un análisis detallado y estructurado de la probabilidad de ocurrencia de cada amenaza. La priorización de las amenazas más relevantes, resaltadas en **rojo**, es clave para asignar recursos y controles eficaces en los activos más críticos de la organización.
- Este enfoque sistemático muestra que InnovaTech Consulting ha evaluado cuidadosamente su infraestructura y servicios, tanto en entornos físicos como en la nube, lo que contribuye a un SGSI robusto, alineado con las mejores prácticas de la norma ISO 27001.

Este análisis detallado servirá para establecer planes de mitigación y controles precisos en los activos más vulnerables de la organización.

Tabla 9: IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES POR ACTIVO

CONSIDERACIONES:

1.- Se ha utilizado la metodología de MAGERIT para la identificación de amenazas y vulnerabilidades por tipología de activo.

2.- Se resaltan en rojo, las amenzas y vulnerabilidades consideradas probables por cada tipología de activo.

Innovatech Consulting

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES POR ACTIVO				
ACTIVO	SERVIDORES	EQUIPOS	APLICACIONES: - HHRR desarrollo de código y gestor de BBDD (MYSQL WORKBENCH) - Control de versiones GITHUB - Gestor de ficheros (WIN SCP,FILEZILLA)	SERVICIOS Prestación de servicios NormaPro
AMENAZAS Y VULNERABILIDADES	**DESASTRES NATURALES**			
	Fuego.	**Fuego.**	Fuego.	Fuego.
	Daños por Agua.	**Daños por Agua.**	Daños por Agua.	Daños por Agua.
	Otros desastres Naturales.	**Otros desastres Naturales.**	Otros desastres Naturales.	Otros desastres Naturales.
	DE ORIGEN INDUSTRIAL			
	Fuego.	**Fuego.**	Fuego.	Fuego.
	Daños por Agua.	**Daños por Agua.**	Daños por Agua.	Daños por Agua.
	Otros desastres Industriales	**Otros desastres Industriales**	Otros desastres Industriales	Otros desastres Industriales
	Contaminación Mecánica.	**Contaminación Mecánica.**	Contaminación Mecánica.	Contaminación Mecánica.
	Contaminación Electromagnética.	**Contaminación Electromagnética.**	Contaminación Electromagnética.	Contaminación Electromagnética.
	Avería de Origen Físico o Lógico.	**Avería de Origen Físico o Lógico.**	**Avería de Origen Físico o Lógico.**	**Avería de Origen Físico o Lógico.**
	Corte del Suministro Eléctrico.	**Corte del Suministro Eléctrico.**	Corte del Suministro Eléctrico.	Corte del Suministro Eléctrico.
	Condiciones Inadecuadas de Temperatura y/o Humedad.	**Condiciones Inadecuadas de Temperatura y/o Humedad.**	Condiciones Inadecuadas de Temperatura y/o Humedad.	Condiciones Inadecuadas de Temperatura y/o Humedad.
	Fallo de Servicios de Comunicaciones	Fallo de Servicios de Comunicaciones	Fallo de Servicios de Comunicaciones	Fallo de Servicios de Comunicaciones
	Interrupción de Otros Servicios y Suministros Esenciales.	**Interrupción de Otros Servicios y Suministros Esenciales.**	Interrupción de Otros Servicios y Suministros Esenciales.	Interrupción de Otros Servicios y Suministros Esenciales.
	Degradación de los Soportes de Almacenamiento de la Información.	Degradación de los Soportes de Almacenamiento de la Información.	Degradación de los Soportes de Almacenamiento de la Información.	Degradación de los Soportes de Almacenamiento de la Información.
	Emanaciones Electromagnéticas.	**Emanaciones Electromagnéticas.**	Emanaciones Electromagnéticas.	Emanaciones Electromagnéticas.
	ERRORES Y FALLOS NO INTENCIONADOS			
	Errores de los Usuarios.	**Errores de los Usuarios.**	**Errores de los Usuarios.**	**Errores de los Usuarios.**
	Errores del Administrador.	**Errores del Administrador.**	**Errores del Administrador.**	**Errores del Administrador.**
	Errores de Configuración.	**Errores de Configuración.**	**Errores de Configuración.**	**Errores de Configuración.**
	Deficiencias en la Organización.	**Deficiencias en la Organización.**	Deficiencias en la Organización.	Deficiencias en la Organización.
	Difusión de Software Dañino.	**Difusión de Software Dañino.**	**Difusión de Software Dañino.**	**Difusión de Software Dañino.**
	Errores de [re–]Encaminamiento.	Errores de [re–]Encaminamiento.	**Errores de [re–]Encaminamiento.**	**Errores de [re–]Encaminamiento.**
	Errores de Secuencia.	Errores de Secuencia.	**Errores de Secuencia.**	**Errores de Secuencia.**
	Escapes de Información.	**Escapes de Información.**	Escapes de Información.	Escapes de Información.
	Alteración de la Información.	**Alteración de la Información.**	**Alteración de la Información.**	**Alteración de la Información.**
	Destrucción de Información.	**Destrucción de Información.**	**Destrucción de Información.**	**Destrucción de Información.**
	Fugas de Información	Fugas de Información	**Fugas de Información**	**Fugas de Información**
	Vulnerabilidades de los Programas (Software).	**Vulnerabilidades de los Programas (Software).**	**Vulnerabilidades de los Programas (Software).**	**Vulnerabilidades de los Programas (Software).**
	Errores de Mantenimiento de Programas (Software)	**Errores de Mantenimiento de Programas (Software)**	**Errores de Mantenimiento de Programas (Software)**	**Errores de Mantenimiento de Programas (Software)**
	Errores de Mantenimiento de Equipos (Hardware).	**Errores de Mantenimiento de Equipos (Hardware).**	Errores de Mantenimiento de Equipos (Hardware).	Errores de Mantenimiento de Equipos (Hardware).
	Caída del Sistema por Agotamiento de Recursos.	Caída del Sistema por Agotamiento de Recursos.	Caída del Sistema por Agotamiento de Recursos.	Caída del Sistema por Agotamiento de Recursos.
	Pérdida de equipos	**Pérdida de equipos**	Pérdida de equipos	Pérdida de equipos
	Indisponibilidad del Personal.	**Indisponibilidad del Personal.**	Indisponibilidad del Personal.	Indisponibilidad del Personal.
	ATAQUES INTENCIONADOS			
	Manipulación de los registros de actividad	Manipulación de los registros de actividad	Manipulación de los registros de actividad	**Manipulación de los registros de actividad**
	Manipulación de la Configuración.	Manipulación de la Configuración.	Manipulación de la Configuración.	**Manipulación de la Configuración.**
	Suplantación de la Identidad del Usuario.	**Suplantación de la Identidad del Usuario.**	**Suplantación de la Identidad del Usuario.**	**Suplantación de la Identidad del Usuario.**
	Abuso de Privilegios de Acceso.	**Abuso de Privilegios de Acceso.**	**Abuso de Privilegios de Acceso.**	**Abuso de Privilegios de Acceso.**
	Uso No Previsto.	**Uso No Previsto.**	**Uso No Previsto.**	**Uso No Previsto.**
	Difusión de Software Dañino.	Difusión de Software Dañino.	**Difusión de Software Dañino.**	**Difusión de Software Dañino.**
	[Re–] Encaminamiento de Mensajes.	[Re–] Encaminamiento de Mensajes.	**[Re–] Encaminamiento de Mensajes.**	**[Re–] Encaminamiento de Mensajes.**
	Alteración de Secuencia.	Alteración de Secuencia.	**Alteración de Secuencia.**	**Alteración de Secuencia.**
	Acceso No Autorizado.	**Acceso No Autorizado.**	**Acceso No Autorizado.**	**Acceso No Autorizado.**
	Análisis de Tráfico.	Análisis de Tráfico.	Análisis de Tráfico.	Análisis de Tráfico.
	Repudio.	Repudio.	Repudio.	Repudio.
	Interceptación de Información (Escucha).	Interceptación de Información (Escucha).	Interceptación de Información (Escucha).	Interceptación de Información (Escucha).
	Modificación de la Información.	Modificación de la Información.	**Modificación de la Información.**	**Modificación de la Información.**
	Destrucción de la Información.	Destrucción de la Información.	**Destrucción de la Información.**	**Destrucción de la Información.**
	Divulgación de Información.	Divulgación de Información.	**Divulgación de Información.**	**Divulgación de Información.**
	Manipulación de Programas.	Manipulación de Programas.	**Manipulación de Programas.**	**Manipulación de Programas.**
	Manipulación de los equipos	**Manipulación de los equipos**	Manipulación de los equipos	Manipulación de los equipos
	Denegación de Servicio.	**Denegación de Servicio.**	Denegación de Servicio.	**Denegación de Servicio.**
	Robo.	**Robo.**	Robo.	Robo.
	Ataque Destructivo.	**Ataque Destructivo.**	Ataque Destructivo.	**Ataque Destructivo.**
	Indisponibilidad del Personal.	**Indisponibilidad del Personal.**	Indisponibilidad del Personal.	**Indisponibilidad del Personal.**
	Extorsión.	Extorsión.	Extorsión.	Extorsión.
	Ingeniería Social.	Ingeniería Social.	Ingeniería Social.	Ingeniería Social.

5.1.3. Resultados destacados del cálculo del Riesgo Real.

El análisis de riesgos cuyos resultados se observan en la **Tabla 10** permite identificar los diferentes niveles de amenaza para los activos críticos de la empresa InnovaTech Consulting, destacando aquellos riesgos que, según su probabilidad de ocurrencia y el impacto potencial, requieren una acción prioritaria. Las evaluaciones realizadas tienen como objetivo definir las acciones de mitigación más adecuadas y los controles a implementar para reducir el riesgo a niveles aceptables.

Este análisis destaca la importancia de implementar controles de seguridad y políticas de mitigación adecuadas, especialmente en aquellos casos donde el riesgo inicial es medio o alto. La revisión de los controles debe ser constante, y es fundamental asignar responsables claros para cada riesgo identificado, asegurando que los procesos se mantengan bajo control y que las amenazas no se materialicen en eventos críticos que afecten la operación de InnovaTech Consulting.

Como riesgos críticos destacados se puede ver el caso de **Equipos de Inmaculada H. y Julio A.**, se han identificado amenazas relacionadas con desastres naturales, desastres industriales, errores no intencionados y ataques intencionados. Por ejemplo, **los daños por agua** tienen una probabilidad inicial de ocurrencia media y un impacto potencial alto, lo que da como resultado un riesgo real inicial de 2.5. Esto sugiere que, aunque el riesgo no es crítico, se deben implementar medidas de prevención como la protección física adecuada de los equipos y copias de seguridad para evitar la pérdida de datos.

Sin embargo, un aspecto destacable es la evaluación de la amenaza **“fugas de información”**, que presenta un riesgo moderado de 3 (señalado en rojo), lo cual indica que este es un punto crítico que requiere revisiones periódicas de los procedimientos y controles adicionales para reducir los errores humanos, especialmente en la configuración de equipos y sistemas ya que se ha comprobado que con los controles aplicados el riesgo sigue sin disminuir.

Otro ejemplo de riesgo relevante es el de **suplantación de identidad** en los **equipos y aplicaciones**. Este riesgo tiene una probabilidad baja, pero un impacto considerable de 4. El control propuesto incluye medidas de autenticación avanzada, como el uso de sistemas multifactor (MFA) y una estricta política de gestión de accesos que es vital para mitigar este tipo de amenazas.

También, En el caso de las aplicaciones como **GitHub Desktop** y **MySQL Workbench**, se han identificado riesgos importantes asociados a **errores de usuario** y **difusión de software dañino**, ambos clasificados con un riesgo moderado de 3. Esto implica que, aunque

no representan una amenaza crítica inmediata, tienen el potencial de afectar la integridad y seguridad de los datos si no se gestionan adecuadamente. Los errores de usuario, como la configuración incorrecta o la ejecución de comandos no previstos, pueden comprometer los repositorios de código o las bases de datos, lo que afectaría la estabilidad y el rendimiento de las aplicaciones.

Por otro lado, la **difusión de software dañino** a través de estas plataformas podría introducir vulnerabilidades que afecten tanto la confidencialidad como la disponibilidad de la información. Es crucial que se implementen controles preventivos como la capacitación constante del personal, la revisión periódica de las configuraciones, así como la adopción de soluciones de **antivirus robustos** y **sistemas de detección de amenazas** en los entornos de trabajo para mitigar estos riesgos. Además, es recomendable revisar y mejorar las políticas de control de acceso, asegurando que solo personal autorizado pueda realizar cambios críticos en el sistema.

Tabla 10: CÁLCULO DEL RIESGO REAL

Nivel de Probabilidad	Criterios de Evaluación	Descripción del Nivel de Probabilidad
1 - Muy baja	Pocas o ninguna amenaza documentada en el pasado.	La amenaza identificada es extremadamente improbable y no hay historial de ocurrencias similares en la organización. Históricamente, no ha ocurrido esta amenaza en InnovaTech Consulting o en organizaciones similares, y es altamente improbable que ocurra en el futuro.
2 - Baja	Amenazas raras pero posibles.	La amenaza es poco frecuente, aunque puede ocurrir en casos excepcionales. La organización ha experimentado pocos eventos similares. Ha habido casos limitados de ocurrencias en el pasado, pero no es común que suceda. Se asocia con eventos aislados.
3 - Media	Amenazas que pueden ocurrir ocasionalmente.	La amenaza ha ocurrido en la organización o en contextos similares con cierta frecuencia, pero no es recurrente. Ha ocurrido ocasionalmente en la organización o en su industria. La probabilidad de que ocurra en el futuro es moderada.
4 - Alta	Amenazas con historial frecuente o condiciones que aumentan la probabilidad.	La amenaza es recurrente o las condiciones actuales aumentan la exposición del activo a dicha amenaza. Es probable que ocurra debido a las condiciones actuales o históricas. La organización tiene antecedentes de eventos similares.
5 - Muy alta	Amenaza prácticamente asegurada.	La amenaza ha ocurrido regularmente o es muy probable que ocurra en el futuro cercano dado el contexto del activo. Es casi seguro que ocurra. Las condiciones internas o externas indican un riesgo inminente y recurrente.

Nivel de Impacto	Criterios de Evaluación	Descripción del Nivel de Impacto
1 - Impacto bajo (-)	Consecuencias mínimas para la operación.	La amenaza tiene un impacto prácticamente insignificante sobre la operación, con consecuencias leves que pueden pasar desapercibidas. La amenaza tendría un impacto mínimo sobre el activo y sobre la operación de la empresa. Por ejemplo, pequeñas modificaciones en documentos internos sin mayor repercusión.
2 - Impacto bajo (+)	Consecuencias menores y manejables.	La amenaza podría causar leves interrupciones o inconvenientes, pero la operación puede continuar sin grandes dificultades. La amenaza podría causar inconvenientes menores, pero su impacto es manejable. Ejemplo: Pequeñas interrupciones en sistemas secundarios.
3 - Impacto medio (-)	Consecuencias moderadas, que requieren atención.	La amenaza provoca una interrupción en algunos procesos, afectando la operación o los servicios temporalmente. La amenaza podría generar una interrupción temporal o daños parciales que afectan a la operativa o a la calidad del servicio, pero se puede gestionar de forma relativamente rápida.
4 - Impacto medio (+)	Consecuencias significativas que requieren intervención.	La amenaza afecta gravemente la operación o algunos servicios, requiriendo acciones correctiva inmediatas para evitar daños mayores. El impacto de la amenaza es serio y requiere una intervención rápida para evitar mayores consecuencias. Ejemplo: Fallo temporal en servicios críticos para la empresa.
5 - Impacto alto	Consecuencias críticas y duraderas.	La amenaza tendría consecuencias catastróficas para la confidencialidad, integridad o disponibilidad de la información, con impactos financieros, reputacionales o legales graves. El impacto es catastrófico, afectando gravemente a la operación, la reputación o las finanzas de la empresa. Ejemplo: Pérdida total de datos críticos o paralización de operaciones claves.

Valor de Riesgo Real	Nivel de Riesgo	Descripción del Nivel de Riesgo
1	Riesgo Bajo (-)	**El riesgo es considerado bajo y no se requiere intervención inmediata. Los controles actuales son suficientes para mitigar las amenazas sin un impacto significativo.** Este nivel indica un riesgo muy bajo, que no representa una amenaza para la operación de los activos. El sistema de seguridad actual es efectivo, y no se espera un impacto considerable. No se requiere acción inmediata, pero se puede realizar una revisión periódica.
2	Riesgo Bajo (+)	**El riesgo es todavía bajo, pero debe ser monitorizado. Aunque no requiere una acción inmediata, puede que se necesite ajustar algunos controles para mayor seguridad.** Este nivel implica que el riesgo sigue siendo bajo, pero debe vigilarse de cerca. Es posible que algunos controles existentes necesiten ser ajustados o reforzados, dependiendo de cómo evolucione el entorno de amenazas.
3	Riesgo Medio (-)	**El riesgo es moderado y podría causar problemas en ciertos activos. Se recomienda una revisión de los controles actuales para prevenir un impacto mayor.** Aquí se observa un riesgo moderado, que podría comprometer los activos si no se aborda correctamente. Se recomienda evaluar las medidas preventivas y, si es necesario, mejorar los controles de seguridad existentes para evitar posibles impactos.
4	Riesgo Medio (+)	**El riesgo es alto-moderado y requiere tratamiento. Los controles actuales no son totalmente efectivos y pueden necesitar mejoras para evitar posibles daños.** Este nivel representa un riesgo significativo que necesita ser tratado con prioridad. Aunque no es crítico, existe la posibilidad de que las amenazas se materialicen si no se implementan medidas adicionales. Una revisión completa de los controles es necesaria.
5	Riesgo Alto	**El riesgo es significativo y debe ser mitigado lo antes posible. Se debe implementar un plan de acción inmediato para reducir tanto la probabilidad como el impacto.** Este es el nivel más alto de riesgo, que probablemente causará impactos graves si no se aborda de inmediato. Las medidas correctivas deben implementarse de manera urgente para evitar daños significativos en la seguridad de la información o la operación de la empresa.

Eficacia	Nivel de Madurez	Significado
0%	L0	**Inexistente**, la medida de seguridad no existe
10%	L1	**Inicial**, la medida la medida de seguridad se aplica cuando se considera adecuado, pero No queda establecido
50%	L2	**Reproducible**
90%	L3	**Proceso Definido**. La medida de seguridad se aplica y queda definida documentalmente.
95%	L4	Medida de seguridad **Gestionada y Medible**
100%	L5	Medida de Seguridad **Optimizada** . A la mmedida de seguridad implementada y gestionada se le aplica proceso de mejora y optimización.

CONSIDERACIONES:

1.- Se analizan como RIESGOS todos los activos con valor [ALTO] ó [CRÍTICO y se les asocia los tipos de amenza catalogadas como probables.

2.- Se asocia una probabilidad de ocurrencia a cada amenza de [1-5] y una probabilidad de impacto de [1-5).

3.- Se calcula el riesto en base a la suma de la probabilidad con el impacto dividida entre dos.

4.- Se considera RIESGO NO ACEPTABLE - TRATABLE aquel cuyo resultado sea >=3.

INNOVATECH CONSULTING

ACTIVO	DESCRIPCIÓN	TIPO DE AMENAZA	AMENAZA	PROBABILIDAD OCURRENCIA INICIAL	IMPACTO INICIAL	CÁLCULO RIESGO REAL INICIAL	RIESGO REAL	NIVEL MADUREZ INICIAL	CONTROLES ASOCIADOS	NIVEL MADUREZ PREVISTO 2023	PROBABILIDAD OCURRENCIA final año	IMPACTO final año	CÁLCULO RIESGO REAL final año	RIESGO REAL final año
EQUIPOS INMACULADA H., JULIO A.	[JULIO A.] [INMACULADA H.] con número de serie según indicación en "valoración-activos". No existe ubicación fija para los equipos de los usuarios.	DESASTRES NATURALES	Fuego	1	2	1,5	2,5	L3	A.5.1.1; A.6.2; A.7.2.2; A.8.1.3; A.8.3.1; A.8.3.3; A.9.1.1; A.11.1, A.11.2.1; A.11.2.3; A.12.3.1; A.17.1; A.18.2	L3	1	2	1,5	2,5
			Daños por Agua	2	3	2,5					2	3	2,5	
			Otros Desastres Naturales	1	2	1,5					1	2	1,5	
		DESASTRES DE ORIGEN INDUSTRIAL	Contaminación mecánica	1	2	1,5	1,5	L3		L3	1	2	1,5	1,5
			Contaminación electromágnetica	1	2	1,5					1	2	1,5	
			Avería de origen físico o lógico	1	2	1,5					1	2	1,5	
			Corte del Suministro Eléctrico	1	2	1,5					1	2	1,5	
			Condiciones inadecuadas de temperatura o humedad	1	2	1,5					1	2	1,5	
			Interrupción de otros servicios y Suministros esenciales	1	2	1,5					1	2	1,5	
			Emanaciones electromagnéticas	1	2	1,5					1	2	1,5	
		ERRORES Y FALLOS NO INTENCIONADOS	Errores del Administrador	2	3	2,5	3	L3	A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.4, A.11.2.4, A.12.2.1, A.13.2.1, A.17.1.1, A.17.1.3, A.18.2.2	L3	2	3	2,5	3
			Errores de Configuración	2	2	2					2	2	2	
			Errores del usuario	2	3	2,5					2	3	2,5	
			Difusión de software dañino	2	2	2					2	2	2	
			Alteración de la información	2	3	2,5					2	3	2,5	
			Escapes de Información	1	4	2,5					1	4	2,5	
			Destrucción de la Información	1	4	2,5					1	4	2,5	
			Fugas de Información	3	3	3					3	3	3	
			Errores de mantenimiento de programas (SW)	2	3	2,5					2	3	2,5	
			Errores de mantenimiento de equipos (HW)	2	3	2,5					2	3	2,5	
			Pérdida de equipos	1	2	1,5					1	2	1,5	
			Indisponibilidad del personal	2	3	2,5					2	3	2,5	
		ATAQUES INTENCIONADOS	Suplantación de la identidad del Usuario	1	4	2,5	2,5	L3	A.11.2.9, A.12.2.1, A.12.6.2, A.13.2.1, A.13.2.4, A.17.1.2, A.17.1.3, A.18.2.2	L3	1	4	2,5	2,5
			Abuso de Privilegios de Acceso	1	3	2					1	3	2	
			Uso no Previsto	2	3	2,5					2	3	2,5	
			Acceso no Autorizado	1	3	2					1	3	2	
			Manipulación de los equipos	1	4	2,5					1	4	2,5	
			Denegación de Servicio	2	3	2,5					2	3	2,5	
			Robo	2	3	2,5					2	3	2,5	
			Ataque Destructivo	1	3	2					1	3	2	
			Indisponibilidad del personal	2	3	2,5					2	3	2,5	
APLICACIONES	Github Descktop / MySQL Workbench/ WIN SCP/ Filezilla/ Responsable Licenciamiento y mantenimiento : Antonio T.	DESASTRES DE ORIGEN INDUSTRIAL	Avería de origen físico o lógico	2	3	2,5	2,5				2	3	2,5	2,5
		ERRORES Y FALLOS NO INTENCIONADOS	Errores del Administrador	2	3	2,5	3	L3	Todos los controles del Anexo A referente a errores y fallos no intencionados de software	L3	2	3	2,5	3
			Errores de Configuración	3	2	2,5					3	2	2,5	
			Errores del usuario	3	3	3					3	3	3	
			Difusión de software dañino	2	4	3					2	4	3	
			Errores de [re--]Encaminamiento.	3	2	2,5					3	2	2,5	
			Errores de Secuencia	2	3	2,5					2	3	2,5	
			Alteración de la información	1	3	2					1	3	2	
			Destrucción de la Información	2	2	2					2	2	2	
			Fugas de información	1	3	2					1	3	2	
			Vulnerabilidades de los programas software	2	2	2					2	2	2	
			Errores de mantenimiento de programas (SW)	2	3	2,5					2	3	2,5	
		ATAQUES INTENCIONADOS	Suplantación de la identidad del Usuario	1	4	2,5	2,5	L3		L3	1	4	2,5	2,5
			Abuso de Privilegios de Acceso	1	3	2					1	3	2	
			Uso no Previsto	1	3	2					1	3	2	
			Difusión de software dañino	2	3	2,5					2	3	2,5	
			Errores de [re--]Encaminamiento.	3	2	2,5					3	2	2,5	
			Alteración de secuencia	1	3	2					1	3	2	
			Acceso no Autorizado	2	3	2,5					2	3	2,5	
			Modificación de Información	2	3	2,5					2	3	2,5	
			Destrucción de la Información	2	3	2,5					2	3	2,5	
			Divulgación de información	2	3	2,5					2	3	2,5	
			Manipulación de los programas	2	3	2,5					2	3	2,5	
SERVIDORES	ENTORNO: PRODUCCION / DESARROLLO/ Azure / Empresa responsable de mantenimiento SW: INICIE	ERRORES Y FALLOS NO INTENCIONADOS	Errores de los usuarios	2	2	2	2,5	L3	Todos los controles del Anexo A referente a errores y fallos no intencionados en servidores	L3	2	2	2	2,5
			Errores del Administrador	2	2	2					2	2	2	
			Errores de Configuración	2	2	2					2	2	2	
			Difusión de software dañino	1	4	2,5					1	4	2,5	
			Alteración de la información	1	3	2					1	3	2	
			Destrucción de la Información	1	4	2,5					1	4	2,5	
			Fugas de Información	1	3	2					1	3	2	
			Errores de mantenimiento de programas (SW)	1	3	2					1	3	2	
			Errores de mantenimiento de equipos (HW)	2	3	2,5					2	3	2,5	
			Indisponibilidad del personal	2	3	2,5					2	3	2,5	
		ATAQUES INTENCIONADOS	Suplantación de identidad del usuario	1	4	2,5	2,5	L3		L3	1	4	2,5	2,5
			Abuso de Privilegios de Acceso	1	3	2					1	3	2	
			Uso no Previsto	2	2	2					2	2	2	
			Acceso no Autorizado	2	3	2,5					2	3	2,5	
			Manipulación de los equipos	2	3	2,5					2	3	2,5	
			Denegación de Servicio	2	3	2,5					2	3	2,5	
			Robo	2	3	2,5					2	3	2,5	
			Ataque destructivo	1	3	2					1	3	2	
SERVICIOS Prestación de Servicios NormaPro	Prestación de Servicios NormaPro	ERRORES Y FALLOS NO INTENCIONADOS	Errores del Administrador	2	3	2,5	2,5	L3	Todos los controles del Anexo A referente a errores y fallos no intencionados en servicios. Nuevo instrucciones ténicas de desarrrollos seguros, politicas de devsecops	L3	2	3	2,5	2,5
			Errores de Configuración	2	1	1,5					2	1	1,5	
			Errores del usuario	2	1	1,5					2	1	1,5	
			Difusión de software dañino	1	4	2,5					1	4	2,5	
			Errores de [re--]Encaminamiento.	3	2	2,5					3	2	2,5	
			Errores de Secuencia	2	3	2,5					2	3	2,5	
			Alteración de la información	1	3	2					1	3	2	
			Destrucción de la Información	2	2	2					2	2	2	
			Fugas de información	2	3	2,5					2	3	2,5	
			Vulnerabilidades de los programas software	1	2	1,5					1	2	1,5	
			Errores de mantenimiento de programas (SW)	1	2	1,5					1	2	1,5	
		ATAQUES INTENCIONADOS	Manipulación de los registros de actividad	1	3	2	2,5	L3	Todos los controles del Anexo A referente a ataques intencionados en servicios	L3	1	3	2	2,5
			Manipulación de la Configuración	1	4	2,5					1	4	2,5	
			Suplantación de la identidad del Usuario	1	4	2,5					1	4	2,5	
			Abuso de Privilegios de Acceso	1	3	2					1	3	2	
			Uso no Previsto	1	3	2					1	3	2	
			Difusión de software dañino	1	3	2					1	3	2	
			Errores de [re--]Encaminamiento.	3	2	2,5					3	2	2,5	
			Alteración de secuencia	1	3	2					1	3	2	
			Acceso no Autorizado	2	3	2,5					2	3	2,5	
			Modificación de Información	1	3	2					1	3	2	
			Destrucción de la Información	2	3	2,5					2	3	2,5	
			Divulgación de información	2	3	2,5					2	3	2,5	
			Manipulación de los programas	1	3	2					1	3	2	

5.1.4. Resultados del análisis del Riesgo.

Tanto para el análisis del riesgo como el cálculo del riesgo residual se utilizó la **Tabla 11** que se adjunta a continuación. De acuerdo con el análisis realizado en base a los criterios de valoración establecidos según las **Tablas 4 y 5**, los activos con amenazas y riesgos más elevados son los siguientes:

1. **EQUIPOS:**

   ERRORES Y FALLOS NO INTENCIONADOS.

- **Difusión de software dañino**, con una probabilidad de 2 y un impacto de 4 presentan un riesgo de 3, moderado, pero en el límite de actuación preferente.

- **Fugas de información c**on una probabilidad de 3 y un impacto de 3 presentan un riesgo de 3, moderado, pero en el límite de actuación preferente se sitúa en 2,5 por lo que hay que actuar.

  ATAQUES INTENCIONADOS.

- **Acceso no autorizado:** Presenta una probabilidad de 2 pero un impacto de 4 muy a tener en cuenta.

  Por lo tanto, en el caso del tipo de activo “Equipos” el riesgo global que presenta es de un 3. Se recuerda que el riesgo considerado aceptable es el inferior a 2,5 por lo que se necesario aplicar controles para lo cual se recurre al Anexo A de la norma ISO 27001 y se determinan cuales son los que hay que aplicar (Ver **Tabla 11**). Ahora bien, se le asigna un nivel de madurez inicial de acuerdo a la **Tabla 7** en la que se definen los niveles de madurez, determinándose a continuación el nivel a alcanzar. El riesgo residual se obtiene de multiplicar el riesgo resultante por tipo de activo multiplicado por el nivel de eficacia asignado a cada nivel de madurez según la misma **Tabla 7. Así, en este caso, e**l Riesgo residual en el caso de “Equipos” es de 1,9 si se aplican los controles determinados en la matriz de análisis.

2. **APLICACIONES:** En este caso el riesgo real alcanza el valor de 2,5 por lo que hay que aplicar los controles del Anexo A de la norma que aparecen en la columna correspondiente para poder mitigar el riesgo y que de forma residual quede en 1,6.

3. **SERVIDORES:**

   ERRORES Y FALLOS NO INTENCIONADOS.

- **Errores del administrador e Indisponibilidad del personal:** en este apartado se encuentran dos casos con la misma puntuación, es decir, probabilidad 2 pero un impacto de 4. El riesgo se queda en 3 que supera el umbral por encima del cual hay que actuar, por lo que se determina la aplicabilidad de los controles del Anexo A que aparecen en la tabla. Una vez aplicado el coeficiente de eficacia que corresponde a un nivel L3 de madurez, el riesgo residual queda en un 2.

4. **SERVICIOS:**

En este caso, todas las amenazas derivadas de los ERRORES Y FALLOS NO INTENCIONADOS hacen que se supere el umbral de 2,5 de nivel de riesgo que se requiere para priorizar la implementación de los controles necesarios de mitigación. Así, por ejemplo, la amenaza "**Errores del administrador"** aparece con el nivel de impacto más alto posible (5), lo que sitúa al nivel de riesgo para este caso concreto en 3,5 ya que la probabilidad está en 2 de acuerdo con la tabla 4.

Por otro lado, en los **Errores de mantenimiento de programas (SW)** el impacto también es alto (4) y la probabilidad es de 3 con lo que queda un riesgo de 3,5.

ATAQUES INTENCIONADOS.
Manipulación de los registros de actividad con un 3 de nivel de riesgo también será tratado de forma prioritaria.

Manipulación de la configuración que alcanza igualmente un nivel de 3,5 de riesgo ya que parte de una probabilidad de 3 y un impacto de 4.

Estos resultados indican que la organización ha implementado un conjunto adecuado de controles de seguridad que han permitido mitigar los riesgos asociados a sus activos críticos. Sin embargo, algunos riesgos, especialmente aquellos relacionados con errores humanos y la difusión de software dañino, siguen siendo áreas de preocupación que deben gestionarse proactivamente para garantizar la seguridad de la información en la organización. Para ello se establece el siguiente paso que será el diseño de un plan de acción.

Tabla 11: ANALISIS DE RIESGOS - Cálculo del Riesgo Residual

Identificación de Activos que requieren tratamiento de riesgos

CONSIDERACIONES:

1.- Se considera RIESGO NO ACEPTABLE - TRATABLE aquel cuyo resultado sea >3.

2.- El Riesgo medio inicial por activo, se calcula COMO EL VALOR MÁS ALTO de los riesgos NO ACEPTABLES de cada amenza, por activo

3.- Los nivel de maduración de los controles se alcanzan aplicando el Plan de Tratamiento de Riesgos, del año en curso

INNOVATECH CONSULTING

ACTIVO: EQUIPOS

DESCRIPCIÓN:
[ANTONIO T.] Nº SERIE: HMW291CC100022Z
[JULIO A.] Nº SERIE: R9N0B5924001
[JUAN M.G.] Nº SERIE: R9N0B5924001
[INMACULADA H.] Nº SERIE: 832011/001
Ubicación de todos los equipos en C/ Suspiro Verde, Nº34, Jaén.

TIPO DE AMENAZA	AMENAZA	PROBABILIDAD OCURRENCIA	IMPACTO	CÁLCULO RIESGO REAL
DESASTRES NATURALES	Fuego	1	2	1,5
	Daños por Agua	1	3	2
	Otros Desastres Naturales	1	2	1,5
DESASTRES DE ORIGEN INDUSTRIAL	Contaminación mecánica	1	2	1,5
	Contaminación electromágnetica	1	2	1,5
	Avería de origen físico o lógico	1	2	1,5
	Corte del Suministro Eléctrico	1	2	1,5
	Condiciones inadecuadas de temperatura o humedad	1	1	1
	Interrupción de otros servicios y Suministros esenciales	1	2	1,5
	Emanaciones electromagnéticas	1	2	1,5
ERRORES Y FALLOS NO INTENCIONADOS	Errores del Administrador	2	3	2,5
	Errores de Configuración	2	2	2
	Errores del usuario	2	3	2,5
	Difusión de software dañino	2	4	3
	Alteración de la información	2	3	2,5
	Escapes de Información	1	4	2,5
	Destrucción de la Información	1	4	2,5
	Fugas de Información	3	3	3
	Errores de mantenimiento de programas (SW)	2	3	2,5
	Errores de mantenimiento de equipos (HW)	2	3	2,5
	Pérdida de equipos	1	2	1,5
	Indisponibilidad del personal	2	3	2,5
ATAQUES INTENCIONADOS	Suplantación de la identidad del Usuario	1	4	2,5
	Abuso de Privilegios de Acceso	1	3	2
	Uso no Previsto	2	3	2,5
	Acceso no Autorizado	2	4	3
	Manipulación de los equipos	1	4	2,5
	Denegación de Servicio	2	3	2,5
	Robo	2	3	2,5
	Ataque Destructivo	1	3	2
	Indisponibilidad del personal	2	3	2,5

RIESGO INICIAL POR TIPO/ACTIVO	RIESGO ACEPTABLE POR ACTIVO	CONTROLES ANEXO A (ver Declaración de Aplicabilidad SOA)	NIVEL DE MADUREZ INICIAL	Avance (valor 1 es el avance del 100%)	RIESGO RESIDUAL
3,0	< 2,5	6.2.1 Política de dispositivos móviles	L3	0,9	2,1
		6.2.2 Teletrabajo	L3	0,9	
		8.1.1 Inventario de Activos	L3	0,9	
		8.1.2 Propiedad de los Activos	L3	0,9	
		8.1.3 Uso aceptable de los Activos	L3	0,9	
		8.1.4 Devolución de activos	L3	0,9	
		9.1.1 Política de Control de Acceso	L3	0,9	
		9.1.2 Acceso a las redes y a los servicios de red	L3	0,9	
		9.2.3 Gestión de Privilegios de acceso	L3	0,9	
		9.2.4 Gestión de la Información Secreta de Autenticación	L3	0,9	
		9.3.1 Uso de la Información secreta de Autenticación	L3	0,9	
		9.4.1 Restricción del acceso a la información	L3	0,9	
		9.4.2 Procedimientos Seguros de Inicio de Sesión	L3	0,9	
		9.4.3 Sistemas de Gestión de Contraseñas	L3	0,9	
		9.4.4 Uso de utilidades con privilegios de sistemas	L3	0,9	
		11.1.1 Perímetros de Seguridad Física	L3	0,9	
		11.1.3 Seguridad de Oficinas, despachos y recursos	L3	0,9	
		11.1.5 El trabajo en áreas seguras	L3	0,9	
		11.1.6 Áreas de carga y descarga	L3	0,9	
		11.2.1 Emplazamiento y protección de Equipos	L3	0,9	
		11.2.2 instalaciones de Suministro	L3	0,9	
		11.2.3 Seguridad del cableado	L3	0,9	
		11.2.4 Mantenimiento de los equipos	L3	0,9	
		11.2.5 Retirada de materiales propiedad de la empresa	L3	0,9	
		11.2.6 Seguridad de los equipos fuera de las instalaciones	L3	0,9	
		11.2.7 Reutilización o eliminación segura de equipos	L3	0,9	
		11.2.8 Equipo de usuario desatendido	L3	0,9	
		11.2.9 Política de Puesto de trabajo despejado y pantalla limpia	L3	0,9	
		12.2.1 Controles contra el código malicioso	L3	0,9	
		12.6.2 Restricción en la instalación de software	L3	0,9	
		13.2.1 Políticas y procedimientos de intercambio de información	L3	0,9	
		13.2.2 Acuerdos de intercambio de información	L3	0,9	
		13.2.3 Mensajería electrónica	L3	0,9	
		13.2.4 Acuerdos de confidencialidad o no revelación	L3	0,9	
		17.1.1 Planificación de la continuidad de la seguridad de la información	L3	0,9	
		17.1.2 Implementar la continuidad de la seguridad de la información	L3	0,9	
		17.1.3 Verificación, revisión y evaluación de la continuidad de la SI	L3	0,9	
		18.1.2 Derechos de propiedad intelectual	L3	0,9	
		18.2.2 Cumplimiento de las políticas y normas de seguridad	L3	0,9	

ACTIVO: APLICACIONES

DESCRIPCIÓN: Github Descktop / MySQL Workbench/ WIN SCP/ Filezilla/ Responsable Licenciamiento y mantenimiento : Antonio T.

TIPO DE AMENAZA	AMENAZA	PROBABILIDAD OCURRENCIA	IMPACTO	CÁLCULO RIESGO REAL
ERRORES Y FALLOS NO INTENCIONADOS	Errores del Administrador	2	3	2,5
	Difusión de software dañino	2	3	2,5
		3	2	
	Errores de mantenimiento de programas (SW)	2	3	2,5

RIESGO INICIAL POR TIPO/ACTIVO	RIESGO ACEPTABLE POR ACTIVO	CONTROLES ANEXO A (ver Declaración de Aplicabilidad SOA)	NIVEL DE MADUREZ INICIAL	Avance (valor 1 es el avance del 100%)	RIESGO RESIDUAL
2,5	< 2,5	6.1.4 Contacto con Grupos de Interés Especial	L3	0,9	1,6
		8.1.1 Inventario de Activos	L3	0,9	
		8.1.2 Propiedad de los Activos	L3	0,9	
		8.1.3 Uso aceptable de los Activos	L3	0,9	
		9.1.1 Política de Control de Acceso	L3	0,9	
		9.2.3 Gestión de Privilegios de acceso	L3	0,9	
		9.2.5 Revisión de los derechos de acceso de usuario	L3	0,9	
		9.2.6 Retirada o reasignación de los derechos de acceso	L3	0,9	
		9.4.1 Restricción del acceso a la información	L3	0,9	
		9.4.2 Prcedimientos Seguros de Inicio de Sesión	L3	0,9	
		9.4.3 Sistemas de Gestión de Contraseñas	L3	0,9	
		9.4.4 Uso de utilidades con privilegios de sistemas	L3	0,9	
		9.4.5 Control de Acceso al código fuente de programas	L3	0,9	
		12.1.2 Gestión de Cambios	L3	0,9	
		12.2.1 Controles contra el código malicioso	L3	0,9	
		12.3.1 Copias de seguridad de la información	L3	0,9	
		12.4.1 Registro de eventos	L3	0,9	
		12.4.3 Registro de administración y operación	L3	0,9	
		13.1.1 Controles de Red	L3	0,9	
		13.1.2 Seguridad de los servicios de red	L3	0,9	
		13.1.3 Segregación en redes	L3	0,9	
		14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	L3	0,9	
		14.1.2 Asegurar los servicios de aplicaciones en redes públicas	L3	0,9	
		14.1.3 Protección de las transacciones de servicios de aplicaciones	L3	0,9	
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el S.O.	L3	0,9	
		14.2.4 Restricciones en los cambios en los paquetes de software	L3	0,9	
		15.1.1 Control y Revisión de la provisión de servicios del proveedor	L3	0,9	
		18.1.2 Derechos de Propiedad Intelectual	L3	0,9	
		18.1.4 Protección y privacidad de la información de carácter personal	L3	0,9	
		18.2.2 Cumplimiento de las políticas y normas de seguridad	L3	0,9	
		18.2.3 Comprobación del cumplimiento técnico	L3	0,9	

ACTIVO: SERVIDORES

DESCRIPCIÓN: ENTORNO: PRODUCCION / DESARROLLO/ Ubicación Edificio Innovatech Jaén / Empresa responsable de Mantenimiento HW : Azure / Empresa responsable de mantenimiento SW: Innovatech

TIPO DE AMENAZA	AMENAZA	PROBABILIDAD OCURRENCIA	IMPACTO	CÁLCULO RIESGO REAL
ERRORES Y FALLOS NO INTENCIONADOS	Errores de usuarios	2	2	2
	Errores del Administrador	2	4	3
	Difusión de software dañino	1	4	2,5
	Errores de mantenimiento de programas (SW)	1	3	2
	Errores de mantenimiento de equipos (HW)	2	3	2,5
	Indisponibilidad del personal	2	4	3

RIESGO INICIAL POR TIPO/ACTIVO	RIESGO ACEPTABLE POR ACTIVO	CONTROLES ANEXO A (ver Declaración de Aplicabilidad SOA)	NIVEL DE MADUREZ INICIAL	Avance (valor 1 es el avance del 100%)	RIESGO RESIDUAL
3,0	<2,5	5.1.1 Políticas para la seguridad de la información	L3	0,9	2,0
		5.1.2 Revisión de las políticas para la seguridad de la información	L3	0,9	
		6.1.1 Roles y responsabilidades para la seguridad de la información	L3	0,9	
		6.1.2 Segregación de tareas	L3	0,9	
		6.1.3 Contacto con las autoridades	L3	0,9	
		6.1.4 Contacto con grupos de interés especial	L3	0,9	
		6.1.5 Seguridad de la Información en la gestión de proyectos	L3	0,9	
		8.1.1 Inventario de activos	L3	0,9	
		8.2.1 Clasificación de la información	L3	0,9	
		8.2.2 Etiquetado de la información	L3	0,9	
		8.2.3 Manipulado de la información	L3	0,9	
		9.1.1 Política de Control de Acceso	L3	0,9	
		11.1.1 Perímetro de seguridad Física	L3	0,9	
		11.1.2 Controles físicos de entrada	L3	0,9	
		11.1.4 Protección contra las amenazas externas y ambientales	L3	0,9	
		12.1.1 Documentación de procedimientos de la operación	L3	0,9	
		12.1.2 Gestión de cambios	L3	0,9	
		12.1.3 Gestión de capacidades	L3	0,9	
		12.1.4 Separación de los recursos de desarrollo, prueba y operación	L3	0,9	
		12.3.1 Copias de seguridad de la información	L3	0,9	
		12.4.1 Registro de eventos	L3	0,9	
		12.4.2 Protección de la información de registro	L3	0,9	
		12.4.3 Registro de Administración y Operación	L3	0,9	
		12.4.4 Sincronización del reloj	L3	0,9	
		12.5.1 Instalación del sotware en explotación	L3	0,9	
		12.6.1 Gestión de las Vulnerabilidades Técnicas	L3	0,9	
		12.7.1 Controles de Auditorias de Sistemas de Información	L3	0,9	
		15.1.1 Política de Seguridad de la información en la relación-proveedores	L3	0,9	
		15.1.2 Requisitos de Seguridad en contrato con terceros	L3	0,9	
		15.1.3 Cadena de suministro de tecnología de la información y comunicaciones	L3	0,9	
		15.2.1 Control y Revisión de la provisión del servicio por el proveedor	L3	0,9	
		15.2.2 Gestión de cambios en la provisión del servicio por el proveedor	L3	0,9	
		16.1.1 Responsabilidades y Procedimientos	L3	0,9	
		16.1.2 Notificación de los eventos de seguridad de la información	L3	0,9	
		16.1.3 Notificación de los puntos débiles de la seguridad	L3	0,9	
		17.1.1 Planificación de la continuidad de la seguridad de la información	L3	0,9	
		17.1.2 Implementar la continuidad de la seguridad de la información	L3	0,9	
		17.1.3 Verificación, revisión y evaluación de la continuidad de negocio	L3	0,9	
		17.2.1 Disponibilidad de los recursos de tratamiento de la información	L3	0,9	
		18.2.1 Revisión independiente de la seguridad de la información	L3	0,9	
		18.2.2 Cumplimiento de las políticas y normas de seguridad	L3	0,9	
		18.2.3 Comprobación del cumplimiento técnico	L3	0,9	

ACTIVO: Servicios con NormaPro

DESCRIPCIÓN: Gestión de servicios de NormaPro

TIPO DE AMENAZA	AMENAZA	PROBABILIDAD OCURRENCIA	IMPACTO	CÁLCULO RIESGO REAL
ERRORES Y FALLOS NO INTENCIONADOS	Errores del Administrador	2	5	3,5
	Difusión de software dañino	1	4	2,5
	Errores de mantenimiento de programas (SW)	3	4	3,5
ATAQUES INTENCIONADOS	Manipulación de los registros de acctividad	2	4	3
	Manipulación de la configuración	3	4	3,5

RIESGO INICIAL POR TIPO/ACTIVO	RIESGO ACEPTABLE POR ACTIVO	CONTROLES ANEXO A (ver Declaración de Aplicabilidad SOA)	NIVEL DE MADUREZ INICIAL	Avance (valor 1 es el avance del 100%)	RIESGO RESIDUAL
3,5	< 2,5	5.1.1 Políticas para la seguridad de la información	L3	0,9	2,5
		5.1.2 Revisión de las políticas para la seguridad de la información	L3	0,9	
		6.1.1 Compromiso de la Dirección con la Seguridad de la Información	L3	0,9	
		6.1.4 Contacto con Grupos de Interés Especial	L3	0,9	
		7.2.1 Responsabilidades de Gestión	L3	0,9	
		7.2.2 Concienciación, educación y capacitación en seguridad de la información	L3	0,9	
		7.2.3 Proceso Disciplinario	L3	0,9	
		7.3.1 Responsabilidades ante la finalización o cambio	L3	0,9	
		8.1.1 Inventario de Activos	L3	0,9	
		8.1.2 Propiedad de los Activos	L3	0,9	
		8.1.3 Uso aceptable de los Activos	L3	0,9	
		8.2.1 Clasificación de la Información	L3	0,9	
		8.2.2 Etiquetado de la información	L3	0,9	
		8.2.3 Manipulado de la información	L3	0,9	
		8.3.1 Gestioón de soportes extraíbles	L3	0,9	
		8.3.2 Eliminación de soportes	L3	0,9	
		8.3.3 Soportes físicos en tránsito	L3	0,9	
		9.1.1 Política de Control de Acceso	L3	0,9	
		9.1.2 Acceso a las redes y a los servicios de red	L3	0,9	
		9.2.1 Registro y Baja de usuario	L3	0,9	
		9.2.2 Provisión de acceso de usuario	L3	0,9	
		9.2.3 Gestión de Privilegios de acceso	L3	0,9	
		9.2.4 Gestión de la información secreta de autenticación de los usuarios	L3	0,9	
		9.2.5 Revisión de los derechos de acceso de usuario	L3	0,9	
		9.2.6 Retirada o reasignación de los derechos de acceso	L3	0,9	
		9.3.1 Uso de la información secreta de autenticación	L3	0,9	
		9.4.1 Restricción del acceso a la información	L3	0,9	
		9.4.2 Prcedimientos Seguros de Inicio de Sesión	L3	0,9	
		9.4.3 Sistemas de Gestión de Contraseñas	L3	0,9	
		9.4.4 Uso de utilidades con privilegios de sistemas	L3	0,9	
		9.4.5 Control de Acceso al código fuente de programas	L3	0,9	
		12.1.1 Documentación de los procedimientos de operación	L3	0,9	
		12.1.2 Gestión de Cambios	L3	0,9	
		12.1.3 Gestión de capacidades	L3	0,9	
		12.1.4 Separación de los recursos de desarrollo, prueba y operación-	L3	0,9	
		12.2.1 Controles contra el código malicioso	L3	0,9	
		12.3.1 Copias de seguridad de la información	L3	0,9	
		12.4.1 Registro de eventos	L3	0,9	
		12.4.2 Protección de la información de registro	L3	0,9	
		12.4.3 Registro de administración y operación	L3	0,9	
		12.5.1 instalación del software en explotación	L3	0,9	
		12.6.1 Gestión de las Vulnerabilidades Técnicas	L3	0,9	
		12.6.2 Restricción en la instalación de software	L3	0,9	
		13.1.1 Controles de Red	L3	0,9	
		13.1.2 Seguridad de los servicios de red	L3	0,9	
		13.1.3 Segregación en redes	L3	0,9	
		13.2.4 Acuerdos de confidencialidad o no revelación	L3	0,9	
		14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	L3	0,9	
		14.1.2 Asegurar los servicios de aplicaciones en redes públicas	L3	0,9	
		14.1.3 Protección de las transacciones de servicios de aplicaciones	L3	0,9	
		14.2.1 Política de desarrollo seguro	L3	0,9	
		14.2.2 Procedimiento de control de cambios en sitemas	L3	0,9	
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el S.O.	L3	0,9	
		14.2.4 Restricciones en los cambios en los paquetes de software	L3	0,9	
		14.2.5 Principios de ingeniería seguros	L3	0,9	
		14.2.6 Entorno de Desarrollo seguro	L3	0,9	
		14.2.7 Externalización del desarrollo de software	L3	0,9	
		14.2.8 Pruebas funcionales de seguridad de sistemas	L3	0,9	
		14.2.9 Pruebas de aceptación de sistemas	L3	0,9	
		14.3.1 Protección de datos de prueba	L3	0,9	
		15.1.1 Control y Revisión de la provisión de servicios del proveedor	L3	0,9	
		16.1.1 Responsabilidades y procedimientos	L3	0,9	
		16.1.2 Notificación de los eventos de seguridad de la información	L3	0,9	
		16.1.3 Notificación de puntos débiles de la seguridad	L3	0,9	
		16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	L3	0,9	
		16.1.5 Respuesta a incidentes de seguridad	L3	0,9	
		16.1.6 Aprendizaje de los incidentes de seguridad	L3	0,9	
		16.1.7 Recopilación de evidencias	L3	0,9	
		18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	L3	0,9	
		18.1.2 Derechos de Propiedad Intelectual	L3	0,9	
		18.1.3 Protección de los registros de la organización	L3	0,9	
		18.1.4 Protección y privacidad de la información de carácter personal	L3	0,9	
		18.2.2 Cumplimiento de las políticas y normas de seguridad	L3	0,9	
		18.2.3 Comprobación del cumplimiento técnico	L3	0,9	

Nivel de Probabilidad	Criterios de Evaluación	Descripción del Nivel de Probabilidad
1 - Muy baja	Pocas o ninguna amenaza documentada en el pasado.	La amenaza identificada es extremadamente improbable y no hay historial de ocurrencias similares en la organización. Históricamente, no ha ocurrido esta amenaza en InnovaTech Consulting o en organizaciones similares, y es altamente improbable que ocurra en el futuro.
2 - Baja	Amenazas raras pero posibles.	La amenaza es poco frecuente, aunque puede ocurrir en casos excepcionales. La organización ha experimentado pocos eventos similares. Ha habido casos limitados de ocurrencias en el pasado, pero no es común que suceda. Se asocia con eventos aislados.
3 - Media	Amenazas que pueden ocurrir ocasionalmente.	La amenaza ha ocurrido en la organización o en contextos similares con cierta frecuencia, pero no es recurrente. Ha ocurrido ocasionalmente en la organización o en su industria. La probabilidad de que ocurra en el futuro es moderada.
4 - Alta	Amenazas con historial frecuente o condiciones que aumentan la probabilidad.	La amenaza es recurrente o las condiciones actuales aumentan la exposición del activo a dicha amenaza. Es probable que ocurra debido a las condiciones actuales o históricas. La organización tiene antecedentes de eventos similares.
5 - Muy alta	Amenaza prácticamente asegurada.	La amenaza ha ocurrido regularmente o es muy probable que ocurra en el futuro cercano dado el contexto del activo. Es casi seguro que ocurra. Las condiciones internas o externas indican un riesgo inminente y recurrente.

Nivel de Impacto	Criterios de Evaluación	Descripción del Nivel de Impacto
1 - Impacto bajo (-)	Consecuencias mínimas para la operación.	La amenaza tiene un impacto prácticamente insignificante sobre la operación, con consecuencias leves que pueden pasar desapercibidas. La amenaza tendría un impacto mínimo sobre el activo y sobre la operación de la empresa. Por ejemplo, pequeñas modificaciones en documentos internos sin mayor repercusión.
2 - Impacto bajo (+)	Consecuencias menores y manejables.	La amenaza podría causar leves interrupciones o inconvenientes, pero la operación puede continuar sin grandes dificultades. La amenaza podría causar inconvenientes menores, pero su impacto es manejable. Ejemplo: Pequeñas interrupciones en sistemas secundarios.
3 - Impacto medio (-)	Consecuencias moderadas, que requieren atención.	La amenaza provoca una interrupción en algunos procesos, afectando la operación o los servicios temporalmente. La amenaza podría generar una interrupción temporal o daños parciales que afectan a la operativa o a la calidad del servicio, pero se puede gestionar de forma relativamente rápida.
4 - Impacto medio (+)	Consecuencias significativas que requieren intervención.	La amenaza afecta gravemente la operación o algunos servicios, requiriendo acciones correctivas inmediatas para evitar daños mayores. El impacto de la amenaza es serio y requiere una intervención rápida para evitar mayores consecuencias. Ejemplo: Fallo temporal en servicios críticos para la empresa.
5 - Impacto alto	Consecuencias críticas y duraderas.	La amenaza tendría consecuencias catastróficas para la confidencialidad, integridad o disponibilidad de la información, con impactos financieros, reputacionales o legales graves. El impacto es catastrófico, afectando gravemente a la operación, la reputación o las finanzas de la empresa. Ejemplo: Pérdida total de datos críticos o paralización de operaciones claves.

Valor de Riesgo Real	Nivel de Riesgo	Descripción del Nivel de Riesgo
1	Riesgo Bajo (-)	**El riesgo es considerado bajo y no se requiere intervención inmediata. Los controles actuales son suficientes para mitigar las amenazas sin un impacto significativo.** Este nivel indica un riesgo muy bajo, que no representa una amenaza para la operación de los activos. El sistema de seguridad actual es efectivo, y no se espera un impacto considerable. No se requiere acción inmediata, pero se puede realizar una revisión periódica.
2	Riesgo Bajo (+)	**El riesgo es todavía bajo, pero debe ser monitorizado. Aunque no requiere una acción inmediata, puede que se necesite ajustar algunos controles para mayor seguridad.** Este nivel implica que el riesgo sigue siendo bajo, pero debe vigilarse de cerca. Es posible que algunos controles existentes necesiten ser ajustados o reforzados, dependiendo de cómo evolucione el entorno de amenazas.
3	Riesgo Medio (-)	**El riesgo es moderado y podría causar problemas en ciertos activos. Se recomienda una revisión de los controles actuales para prevenir un impacto mayor.** Aquí se observa un riesgo moderado, que podría comprometer los activos si no se aborda correctamente. Se recomienda evaluar las medidas preventivas y, si es necesario, mejorar los controles de seguridad existentes para evitar posibles impactos.
4	Riesgo Medio (+)	**El riesgo es alto-moderado y requiere tratamiento. Los controles actuales no son totalmente efectivos y pueden necesitar mejoras para evitar posibles daños.** Este nivel representa un riesgo significativo que necesita ser tratado con prioridad. Aunque no es crítico, existe la posibilidad de que las amenazas se materialicen si no se implementan medidas adicionales. Una revisión completa de los controles es necesaria.
5	Riesgo Alto	**El riesgo es significativo y debe ser mitigado lo antes posible. Se debe implementar un plan de acción inmediato para reducir tanto la probabilidad como el impacto.** Este es el nivel más alto de riesgo, que probablemente causará impactos graves si no se aborda de inmediato. Las medidas correctivas deben implementarse de manera urgente para evitar daños significativos en la seguridad de la información o la operación de la empresa.

Eficacia	Nivel de Madurez	Significado
0%	L0	**Inexistente**, la medida de seguridad no existe
10%	L1	**Inicial**, la medida la medida de seguridad se aplica cuando se considera adecuado, pero No queda establecido
50%	L2	**Reproducible**
90%	L3	**Proceso Definido**. La medida de seguridad se aplica y queda definida documentalmente.
95%	L4	Medida de seguridad **Gestionada y Medible**
100%	L5	Medida de Seguridad **Optimizada** . A la mmedida de seguridad implementada y gestionada se le aplica proceso de mejora y optimización.

5.2. RESULTADOS DEL PLAN DE ACCIÓN BASADO EN LA EVALUACIÓN DE RIESGOS.

La implementación del plan de acción basado en la evaluación de riesgos realizado por Innovatech Consulting ha arrojado resultados significativos, alineados con los objetivos establecidos en materia de seguridad de la información. Este plan de acción que puede analizarse pormenorizadamente en la **Tabla 12** siguiente, ha permitido no solo fortalecer la postura de seguridad de la organización, sino también optimizar los procesos relacionados con la protección de los activos de información, cumpliendo con los requisitos normativos de la ISO 27001 en su versión 2022.

Dicho plan de acción desarrollado se basa en los resultados obtenidos de la evaluación de riesgos previamente realizada, con el objetivo de mitigar las amenazas identificadas y fortalecer los controles de seguridad dentro de la organización. Este proceso ha permitido definir un conjunto de acciones correctivas y preventivas, plasmadas en una matriz detallada de riesgos, acciones y responsables, que ha sido crucial para establecer las prioridades dentro de la gestión de la seguridad de la información. Concretamente se han establecido medidas preventivas o mitigadoras para 111 controles prescritos por la aplicación de la norma ISO 27001.

El proceso de creación del plan de acción se realiza siguiendo la metodología descrita en el apartado 4.3.2. de este TFG., para lo cual se inicia con la identificación de los dominios y controles afectados, siguiendo el esquema del anexo A de la norma ISO 27001. Cada control ha sido analizado en detalle para determinar su nivel de madurez actual (inicial) y el nivel de madurez objetivo, indicando claramente las acciones a realizar para mejorar la seguridad de la información. Posteriormente, se determina el grado de avance y se establecen fechas de inicio y finalización para cada acción, asignando los recursos necesarios y el responsable de llevar a cabo la acción.

En términos generales, el plan de acción ha permitido avanzar de manera considerable en la madurez de los controles de seguridad implementados, con la mayoría de los controles alcanzando o superando los niveles de madurez objetivo. Los controles asociados a políticas y procedimientos internos, como la segregación de tareas y la revisión de políticas, han demostrado ser especialmente efectivos para minimizar los riesgos más críticos identificados en la evaluación inicial de riesgos.

El uso de herramientas de seguridad como Azure Defender ha sido un componente fundamental para el éxito de este plan, asegurando una monitorización constante de los posibles riesgos y automatizando acciones de mitigación cuando es posible. Esto ha permitido

una respuesta más rápida y efectiva a las amenazas, optimizando los recursos y reduciendo la carga operativa en la gestión de riesgos.

Se exponen en los siguientes apartados de este capítulo, las acciones más relevantes de este Plan de acción reflejado en la **Tabla 12**.

5.2.1. Política de seguridad de la información.

En esta área destaca la implementación de las **Políticas para la seguridad de la información** y la **Revisión periódica de la Política de Seguridad**. La organización ha avanzado de forma notable, alcanzando un 80% de progreso en la configuración de controles manuales y automáticos. La dirección ha tomado un papel clave en comunicar y aprobar los documentos de seguridad a todos los empleados, lo que garantiza una cobertura adecuada y cumplimiento de normativas. La madurez actual se encuentra en un **Nivel L3**, con un objetivo de alcanzar el **L4**, lo que implica una mejora en la gestión sistemática de la seguridad.

Un caso concreto de relevancia es el dominio 5, relacionado con la política de seguridad de la información. Se identificó que la política de seguridad necesitaba ser revisada de manera periódica (control 5.1.2) y que el nivel de madurez inicial era L3. A través de acciones específicas, como la configuración de Azure Defender para incluir controles manuales y automáticos, se logró alcanzar un nivel de madurez objetivo L4. Esta acción específica muestra el compromiso de la dirección con la seguridad de la información, ya que estas revisiones permiten garantizar que las políticas se ajusten a las necesidades y cambios de la organización de manera continua.

5.2.2. Organización de la seguridad de la información.

La empresa ha avanzado considerablemente en la coordinación de actividades de seguridad, especialmente en la **Segregación de Tareas** y el **Compromiso de la dirección con la Seguridad de la Información**, ambos alcanzando un 80% de implementación. Esta segregación reduce los riesgos asociados a accesos no autorizados o modificaciones accidentales de los activos. El objetivo es alcanzar una madurez **L3-L4** que garantice una coordinación fluida entre las distintas áreas de la organización, asegurando que todas las responsabilidades están bien delimitadas.

5.2.3. Dispositivos móviles y teletrabajo.

Las políticas relacionadas con el **uso seguro de dispositivos móviles** y la **protección del teletrabajo** son áreas clave que han mostrado un progreso del 80%. Dada la creciente relevancia del trabajo remoto, asegurar la protección de la información accesible y almacenada en ubicaciones externas es vital. Las medidas aplicadas incluyen políticas que

gestionan el riesgo del uso de dispositivos móviles, protegiendo la información sensible sin importar la ubicación de los usuarios. Aquí también se ha establecido una madurez inicial de **L3**, con el objetivo de fortalecer las políticas a **L4**.

5.2.4. Recursos Humanos.

Este dominio aborda varios aspectos relacionados con la seguridad desde el inicio hasta la finalización de la relación laboral. Un punto clave es la **Investigación de antecedentes**, donde la empresa garantiza que las personas que se incorporan cumplen con los estándares éticos y legales requeridos, contribuyendo a la mitigación de riesgos internos. Además, se han implementado **medidas de concienciación y capacitación** en seguridad para todos los empleados, con un progreso del 80% en la configuración de los controles de seguridad. Estos esfuerzos son fundamentales para minimizar riesgos humanos, como errores y accesos no autorizados.

La combinación de políticas estrictas desde el proceso de contratación hasta la salida de empleados refuerza la protección de la organización, especialmente en términos de manejo de información sensible. Estos esfuerzos han sido clave para mantener un **Nivel L3** de madurez, con objetivos de continuar mejorando hacia un **L4**, lo que implicaría un enfoque aún más sistemático y controlado en la gestión de los recursos humanos en términos de seguridad.

5.2.5. Gestión de Activos.

Este apartado de controles se enfoca en asegurar que los activos de información estén debidamente gestionados a lo largo de su ciclo de vida, desde la identificación y clasificación hasta su manipulación y eventual eliminación, para lo cual, se establece la necesidad de una **gestión clara de los activos**, asegurando que todos los recursos asociados a la información estén debidamente inventariados y clasificados. El progreso actual es del **80%**, lo que indica que ya se han implementado controles manuales y automáticos a través de Azure Defender, pero se está trabajando para optimizar aún más este proceso.

Los objetivos en este ámbito han sido:

- Asegurar que todos los activos están claramente identificados y documentados en un inventario actualizado. Esto ayuda a la organización a tener control sobre los recursos críticos y los riesgos asociados.
- Garantizar que cada activo tenga un responsable designado, asegurando una cadena clara de responsabilidad en la gestión de los recursos.
- Uso aceptable de los Activos, para lo cual, las políticas definen los usos aceptables para cada tipo de activo, limitando los riesgos de uso indebido o accidental.

- Asegurar que, al finalizar la relación contractual o laboral, todos los activos, tanto físicos como digitales, sean devueltos y controlados para evitar fugas de información.
- Los activos deben ser clasificados correctamente para asegurar que las medidas de seguridad sean proporcionales a su criticidad. Este proceso asegura que la información sensible reciba una protección adecuada.
- Identificar correctamente la información en función de su nivel de sensibilidad, facilitando su gestión y protegiendo datos confidenciales de manera eficaz.
- Controlar el uso de dispositivos como memorias USB, discos duros externos, entre otros. Se asegura que estos dispositivos sean utilizados de manera controlada, minimizando el riesgo de fugas de información.
- Implementar procedimientos formales para la eliminación segura de soportes cuando ya no sean necesarios. Este proceso es fundamental para prevenir la recuperación no autorizada de información sensible.
- Garantizar que los soportes que se transportan fuera de las instalaciones están protegidos contra accesos no autorizados y daños físicos, reduciendo el riesgo de exposición durante el tránsito.

5.2.6. Control de Accesos.

Uno de los aspectos críticos que se ha abordado durante la evaluación de riesgos ha sido el control de acceso a los sistemas, redes y aplicaciones de la organización. La adecuada gestión de los privilegios de acceso es fundamental para mitigar los riesgos asociados a accesos no autorizados y la manipulación indebida de los activos de información.

En este ámbito, se han identificado controles específicos que abarcan tanto la política de control de acceso como la gestión de usuarios y la protección de credenciales. Algunos de los resultados más relevantes incluyen:

1. Política de Control de Acceso: Se ha establecido la necesidad de documentar y revisar de manera periódica una política de control de acceso basada en los requisitos del negocio y las necesidades de seguridad. Se han implementado acciones como la "Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsoft", con un grado de avance del 80%. Este control asegura que solo los usuarios autorizados puedan acceder a los sistemas y servicios de la red.

2. Gestión de Acceso de Usuarios: En este apartado, se ha implementado un procedimiento formal para el registro y baja de usuarios, además de una provisión de acceso que garantiza que solo los usuarios autorizados puedan acceder a los sistemas y servicios necesarios para su función. El plan de acción también ha contemplado la gestión de privilegios de acceso, asegurando que el uso de estos privilegios esté registrado y controlado. Estos controles han sido reforzados mediante herramientas de gestión de identidad y acceso (IAM), lo que ha permitido un control más riguroso sobre quién accede y qué acciones puede realizar cada usuario.

3. Responsabilidades del Usuario: Se ha definido un conjunto de responsabilidades claras en torno al uso de información secreta de autenticación, estableciendo procedimientos para proteger la confidencialidad de contraseñas y otros elementos de autenticación. Las medidas incluyen la activación de políticas más estrictas en cuanto al uso de contraseñas interactivas y mecanismos de autenticación de múltiples factores para garantizar la integridad del acceso.

4. Control de Acceso a Sistemas y Aplicaciones: Este apartado ha resultado fundamental para garantizar que el acceso a sistemas y aplicaciones sea limitado a funciones específicas. Los controles implementados incluyen restricciones en el acceso a la información crítica y procedimientos seguros para el inicio de sesión (9.4.2). También se han establecido controles rigurosos en el uso de utilidades con privilegios del sistema (9.4.4) y el acceso al código fuente de los programas (9.4.5), asegurando que solo personal autorizado pueda realizar modificaciones en los sistemas críticos.

5.2.7. Seguridad física y del entorno.

El Plan de Acción ha incluido de manera significativa la implementación de controles relacionados con la seguridad física y la protección del entorno donde se almacenan y procesan los activos de información. Este aspecto es clave para garantizar no solo la seguridad digital, sino también la protección física de los equipos y recursos que soportan los sistemas de información.

Entre los controles establecidos, destacan los siguientes:

1. Áreas seguras: El análisis de riesgos identificó la necesidad de establecer perímetros de seguridad física que protejan las áreas sensibles y los recursos de tratamiento de la información. Se han implementado controles físicos de entrada (11.1.2) para asegurar que solo personal autorizado pueda acceder a las oficinas, despachos y áreas críticas. Las medidas también incluyen la instalación de procedimientos de protección contra amenazas ambientales (11.1.4), asegurando que las áreas seguras cumplan con estándares físicos para

minimizar los riesgos de fuego, inundaciones o robos. Estos controles presentan un avance del 80%, con la implementación de configuraciones de seguridad en sistemas como Azure Defender, que complementan las protecciones físicas con medidas digitales avanzadas.

2. Seguridad de los equipos: Los equipos que almacenan o procesan información crítica deben estar protegidos frente a amenazas físicas y ambientales. En este sentido, los controles establecidos en el plan incluyen medidas para el emplazamiento y protección de equipos (11.2.1), protegiendo tanto su ubicación como su exposición a fallos de alimentación o alteraciones ambientales. Asimismo, se ha reforzado la seguridad en el cableado (11.2.3) para evitar interferencias electromagnéticas o daños físicos que puedan comprometer la disponibilidad de los servicios. De igual importancia, se han implementado procedimientos para la reutilización y eliminación segura de equipos (11.2.7), asegurando que cualquier dispositivo que salga de las instalaciones sea previamente limpiado y protegido, eliminando cualquier dato confidencial que pudiera quedar en él.

3. Mantenimiento y protección de Activos: Otro aspecto clave ha sido el mantenimiento adecuado de los equipos para garantizar su disponibilidad y evitar fallos inesperados. Este control también está vinculado a la política de retiro de equipos (11.2.6), asegurando que los activos sean gestionados de manera segura cuando sean sacados de las instalaciones. Estos controles han sido implementados con éxito, alcanzando un 80% de avance, y complementan los controles digitales que monitorizan la actividad de los sistemas en tiempo real.

5.2.8. Seguridad de las operaciones.

El análisis de riesgos identificado en este ámbito ha conducido a la implementación de múltiples controles enfocados en la seguridad de las operaciones. Esto incluye procedimientos para asegurar la continuidad, la protección frente a código malicioso y la implementación de controles técnicos que refuercen la seguridad de la infraestructura tecnológica de la organización.

Entre los controles implementados, destacan los siguientes:

1. Procedimientos y Responsabilidades Operacionales: Un aspecto fundamental en la gestión de operaciones seguras es la correcta documentación de los procedimientos de operación y la gestión de cambios (12.1.2). Esto permite garantizar que cualquier modificación en los sistemas de información sea correctamente registrada y gestionada para minimizar los riesgos. En este sentido, se ha logrado un avance del 80% en la implementación de los controles necesarios, que han sido integrados en las configuraciones de Azure Defender y controles automáticos adicionales. La correcta separación de los entornos de desarrollo,

pruebas y operación (12.1.4) también ha sido priorizada para evitar errores de implementación en sistemas productivos.

2. Protección contra Código Malicioso: La protección frente a software malicioso es crítica para la continuidad de las operaciones. Se ha implementado una política de detección y bloqueo de software dañino (12.2.1), utilizando herramientas de escaneo avanzadas integradas con Azure Defender. Este control ha sido aplicado junto con una campaña de concienciación a los usuarios sobre los riesgos asociados al software malicioso. Este control ya se encuentra al 100% de implementación, gracias a la integración con DevOps y prácticas de desarrollo seguro.

3. Copias de Seguridad: Para asegurar la integridad y disponibilidad de la información, se ha reforzado el procedimiento de realización de copias de seguridad periódicas (12.3.1). Este control ha sido implementado en su totalidad, con un enfoque en garantizar que todas las copias de seguridad se realicen conforme a los procedimientos establecidos. Además, se ha integrado con la gestión de la integración continua del software, lo que asegura que cualquier dato crítico sea respaldado de manera automática.

4. Registros y Supervisión: La revisión periódica de los registros de actividad de los usuarios y administradores es otro aspecto fundamental en la seguridad de las operaciones. Los controles de supervisión (12.4.1 y 12.4.3) se han enfocado en proteger la información crítica y garantizar que cualquier actividad irregular sea identificada y gestionada de manera proactiva. Estos controles, integrados en las soluciones de seguridad, están en un 80% de avance, con planes de completar la implementación total antes de finalizar el período.

5. Control del Software en Explotación: Otro componente esencial es el control de las vulnerabilidades en el software instalado. La gestión de estas vulnerabilidades (12.6.1) ha sido reforzada mediante la implementación de controles automáticos que identifican y solucionan las debilidades técnicas antes de que puedan ser explotadas. Este control ha alcanzado un 100% de implementación, asegurando que los riesgos relacionados con software desactualizado o inseguro sean mitigados de manera eficaz.

5.2.9. Seguridad de las Comunicaciones.

El enfoque en este dominio ha sido reforzar la seguridad en las redes y asegurar un intercambio de información controlado y seguro entre sistemas y usuarios. Este dominio abarca principalmente la gestión de redes y el intercambio de información, factores críticos para mantener la integridad, confidencialidad y disponibilidad de la información transmitida por la red.

Los principales resultados obtenidos son:

1. **Gestión de la Seguridad de Redes**: Se han implementado controles adecuados para la protección de los sistemas de red, destacándose la segregación de redes (13.1.3) y la implementación de controles automáticos y manuales, a través de Azure Defender, para monitorear los niveles de seguridad de todos los servicios de red. Estos controles, que alcanzan un grado de avance del 80%, aseguran que los usuarios y sistemas accedan únicamente a las redes y servicios para los cuales están autorizados.
2. **Intercambio de Información**: La política de intercambio de información (13.2.1) y el uso de mensajería electrónica segura (13.2.3) han sido áreas clave en este dominio. La organización ha establecido procedimientos para asegurar que el intercambio de información con terceros cumpla con las normas de seguridad, logrando un avance del 80% en la configuración de controles automáticos, evitando así la divulgación no autorizada de información confidencial.

5.2.10. Desarrollo y mantenimiento de los Sistemas de Información.

El objetivo principal en este dominio es garantizar que los sistemas y aplicaciones desarrollados o adquiridos cuenten con los niveles de seguridad necesarios desde el inicio de su ciclo de vida, asegurando la protección continua durante su uso y mantenimiento.

Los resultados más destacables han sido:

1. **Requisitos de seguridad en sistemas de información**: Se ha trabajado en la definición de requisitos específicos de seguridad para las aplicaciones y sistemas adquiridos o desarrollados. Esto incluye asegurar los servicios de aplicaciones en redes públicas (14.1.2) y proteger las transacciones de servicios de aplicaciones (14.1.3), con un avance del 80%. La integración de controles manuales y automáticos en los servicios ha permitido la protección frente a fraudes y actividades no autorizadas durante la transmisión de información sensible.
2. **Seguridad en el desarrollo y en los procesos de soporte (14.2)**: Se ha integrado un marco de desarrollo seguro (14.2.1), alcanzando el 100% de implementación en este aspecto, gracias a la adopción de DevOps y prácticas de integración continua. El control de los cambios en los sistemas operativos y en los paquetes de software ha sido reforzado mediante controles que aseguran la estabilidad y seguridad de las aplicaciones críticas, con un nivel de madurez optimizado en varios de estos procesos.
3. **Ingeniería y pruebas funcionales (14.2.5 y 14.2.8)**: En este apartado, se han desarrollado principios de ingeniería segura para gestionar los riesgos inherentes a los

entornos de desarrollo y producción. Estos controles aseguran que cualquier cambio implementado en las aplicaciones sea debidamente probado y que las vulnerabilidades técnicas sean identificadas y mitigadas antes de su despliegue en el entorno operativo.

5.2.11. Seguridad en las relaciones con los Proveedores.

En esta área, se han enfocado esfuerzos en asegurar que los proveedores cumplan con los requisitos de seguridad de la información. En particular, la implementación de controles de seguridad en los contratos de los proveedores (15.1.2) ha logrado un avance del 80%, reforzando la responsabilidad compartida en la gestión de la seguridad de la información que fluye a través de servicios externalizados.

Además, la revisión continua de la provisión de servicios de proveedores de TIC (15.2.1) asegura que las organizaciones externas mantengan los mismos estándares de seguridad que la empresa, reduciendo así los riesgos derivados de terceros.

5.2.12. Gestión de incidentes de Seguridad de la Información y mejoras.

Lo fundamental es dar rápida respuesta a incidentes de seguridad. Para ello, uno de los controles críticos es la notificación de los eventos de seguridad de la información (16.1.2), con un avance significativo del 80%, lo que asegura que los incidentes se comuniquen rápidamente a través de canales designados, permitiendo así una respuesta más ágil y efectiva.

Adicionalmente, se ha avanzado en la evaluación y decisión sobre los eventos de seguridad (16.1.4), alcanzando el mismo grado de madurez. Esta acción permite evaluar con precisión cada incidente, determinar las mejores medidas correctivas y garantizar la continuidad de las operaciones de forma segura.

5.2.13. Aspectos de Seguridad de la información para la Gestión de la Continuidad de Negocio.

En este ámbito, el enfoque ha estado en la planificación de la continuidad del sistema de información (17.1.1), con un avance del 80%. Se han establecido planes detallados para asegurar que la información crítica esté protegida en caso de interrupciones. Estos planes han sido fundamentales para garantizar que la organización pueda responder eficazmente ante cualquier evento que amenace la continuidad de los servicios esenciales.

Además, se ha progresado en la verificación y evaluación de la continuidad del servicio de información (17.1.3), asegurando que los controles implementados sean válidos y eficaces en condiciones de contingencia.

5.2.14. Cumplimiento.

En esta área se muestran los avances en la identificación y cumplimiento de los requisitos legales, así como en la revisión independiente de las políticas de seguridad de la información. Uno de los principales avances en este dominio se refiere a la **identificación de la legislación aplicable y los requisitos contractuales** (18.1.1), donde se ha alcanzado un 80% de avance en la implementación de controles automáticos y manuales a través de Azure Defender. Este control asegura que la organización cumple con los marcos legales y regulatorios aplicables, evitando sanciones y riesgos legales relacionados con el uso y manejo de la información.

Otro aspecto relevante es la protección de los **derechos de propiedad intelectual** (18.1.2), que también ha avanzado en un 80%. Este control garantiza que la organización respeta el uso de software patentado y cumple con las normativas relacionadas, evitando posibles infracciones o conflictos legales.

En cuanto a la **revisión independiente de la seguridad de la información** (18.2.1), la organización ha establecido procedimientos periódicos para garantizar que su sistema de gestión de seguridad esté alineado con las mejores prácticas. Esto incluye auditorías externas que permiten identificar cualquier brecha o debilidad en la implementación de políticas de seguridad.

También se han implementado medidas para asegurar el **cumplimiento técnico** de los sistemas de información (18.2.3). Con un avance del 80%, la organización está verificando de manera constante que los sistemas cumplen con las normas establecidas, lo que mitiga riesgos operacionales y garantiza la continuidad del negocio.

El trabajo realizado en este ámbito refleja el compromiso de la organización con la legalidad y la seguridad de la información. A través de la implementación de controles robustos y la revisión periódica de los sistemas, se ha logrado un avance considerable en la mitigación de riesgos asociados al incumplimiento de normativas legales y de seguridad. Esto asegura que la empresa no solo cumple con los requisitos legales, sino que también se mantiene preparada para afrontar los desafíos futuros en un entorno legal y tecnológico en constante evolución.

Tabla 12: Plan de acción basado en la evaluación de riesgos

CONSIDERACIONES:
1.- La Descripción de los dominios y controles así como su aplicabilidad en INICIE está desplegado en la SOA (Declaración de Aplicabilidad), los domininios y controles que no aplican NO APARECEN en el Plan de Riesgos.
2.- En AMARILLO los campos a cumplimentar asociados a las acciones a implementar
3.- ACCIONES: A.O.: Acción Organizativa / A.T.: Acción Técnica

Eficacia	Nivel de Madurez	Significado
0%	L0	**Inexistente**, la medida de seguridad no existe
10%	L1	**Inicial**, la medida la medida de seguridad se aplica cuando se considera adecuado, pero No queda establecido
50%	L2	**Reproducible**
90%	L3	**Proceso Definido**. La medida de seguridad se aplica y queda definida documentalmente.
95%	L4	Medida de seguridad **Gestionada y Medible**
100%	L5	Medida de Seguridad **Optimizada** . A la mmedida de seguridad implementada y gestionada se le aplica proceso de mejora y optimización.

INNOVATECH CONSULTING

DOMINIO	Controles	Descripción	Nivel Madurez Inicial	Nivel Madurez Objetivo	Acciones	Grado de Avance	Fecha Inicio	Fecha Final	Recursos	Responsable Acción	Observaciones
Dominio 5: Política de Seguridad de la Información											
5.1 Política de seguridad de la información	5.1.1 Políticas para la seguridad de la información	La Dirección debe aprobar un documento de Política de Seguridad que debe ser pública y debe ser comunicada a todos los empleados y entidades externas relevantes.	L3	L4	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	5.1.2 Revisión de la Política de Seguridad de la Información	La política de Seguridad debe ser revisada de forma regular y cuando exista cualquier cambio relevante en la Organización.	L3	L4	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	04/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 6: Organización de la Seguridad de la Información											
6.1 Organización interna	6.1.1 Compromiso de la Dirección con la Seguridad de la Información	La Dirección debe apoyar la Seguridad de la Información a través del compromiso, dirección y definición de responsabilidades	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	6.1.2 Segregación de Tareas	Las actividades de Seguridad de la Información deben ser coordinadas por representantes de todas las partes representativas de la Organización. Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	6.1.3 Contacto con las Autoridades	Se deben mantener contactos con las autoridades relevantes.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	6.1.4 Contactos con grupos interés especial	Se deben mantener contactos apropiados con grupos de seguridad especializados y asociaciones profesionales.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	6.1.5 Seguriddad de la información en la gestión de proyectos	La seguridad de la Información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
6.2 Los dispositivos móviles y el teletrabajo	6.2.1 Política de dispositivos móviles	Se debe adoptar un política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	6.2.2 Teletrabajo	Se deben implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	L3	L4	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 7: Seguridad Relativa a los Recursos Humanos											
7.1 Antes del Empleo	7.1.1 Investigación de Antecedentes	La comprobación de los antecedentes de todos los candidatos el puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos	L3	L3	No acciones necesarias año en curso						
	7.1.2 Términos y Condiciones del Empleo	Como parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización	L3	L3	No acciones necesarias año en curso						
7.2 Durante el Empleo	7.2.1 Responsabilidades de Gestión	La Dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	7.2.3 Proceso Disciplinario	Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad	L3	L3	No acciones necesarias año en curso						
7.3 Finalización del Empleo o cambio en el puesto de trabajo	7.3.1 Responsabilidades ante la finalización o cambio	Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir	L3	L3	No acciones necesarias año en curso						
Dominio 8: Gestión de Activos											
8.1 Responsabilidad sobre los activos	8.1.1 inventario de Activos	Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	8.1.2 Propiedad de los activos	Todos los activos que figuran en el inventario deben tener un propietario	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	8.1.3 Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados a los recursos para el tratamiento de la información	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	8.1.4 Devolución de Activos	Todos los empleados y terceras partes deben devolver todos los activos a la organización que estén en su poder al finalizar su empleo, contrato o acuerdo	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
8.2 Clasificación de la información	8.2.1 Clasificación de la Información	La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad, y criticidad ante revelación o modificación no autorizadas	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	8.2.2 Etiquetado de la información	Debe desarrollarse e implementarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	8.2.3 Manipulado de la información	Debe desarrollarse e implementarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
8.3 Manipulación de los soportes	8.3.1 Gestión de Soportes Extraíbles	Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización	L3	L3	No acciones necesarias año en curso						
	8.3.2 Eliminación de los Soportes	Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales	L3	L3	No acciones necesarias año en curso						
	8.3.3 Soportes físicos en tránsito	Durante el trasporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro	L3	L3	No acciones necesarias año en curso						
Dominio 9: Control de Accesos											
9.1 Requisitos de negocio para el control de acceso	9.1.1 Política de Control de Acceso	Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.1.2 Acceso a las redes y a los servicios de red	Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios de red para cuyo uso hayan sido específicamente autorizados	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
9.2 Gestión de Acceso de Usuario	9.2.1 Registro y Baja de usuario	Debe implementarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.2.2 Provisión de acceso de usuario	Debe implementarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.2.3 Gestión de Privilegios de Acceso	La asignación y el uso de privilegios de acceso debe estar registrada y controlada	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.2.4 Gestión de la información secreta de autenticación de los usuarios	La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.2.5 Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.2.6 Retirada o reasignación de los derechos de acceso	Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en casos de cambio.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
9.3 Responsabilidades del usuario	9.3.1 Uso de la información secreta de autenticación	Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
9.4 Control de Acceso a Sistemas y Aplicaciones	9.4.1 Restricción del acceso a la información	Se debe restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.4.2 Procedimientos seguros de inicio de sesión	Cuando así se requiera en la política de control de acceso, el acceso a los sistemas y a las aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.4.3 Sistemas de Gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.4.4 Uso de utilidades con privilegios del sistema	Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	9.4.5 Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas	L2	L2	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 11: Seguridad Física y del Entorno											
11.1 Áreas Seguras	11.1.1 Perímetro de Seguridad Física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.1.2 Controles físicos de entrada	Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.1.3 Seguridad de oficinas, despachos y recursos	Para las oficinas, despachos y recursos, se deben diseñar y aplicar la seguridad física	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.1.4 Protección contra las amenazas externas y ambientales	Se debe diseñar e implementar procedimientos para trabajar en las áreas seguras	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.1.5 El trabajo en áreas seguras	Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.1.6 Áreas de carga y Descarga	Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información.	L3	L3	No acciones necesarias año en curso						
11.2 Seguridad de los Equipos	11.2.1 Emplazamiento y protección de equipos	Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales de que se produzcan accesos no autorizados	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.2 Instalaciones de Suministro	Los equipo deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.3 Seguridad en el cableado	El cableado eléctrico y de telecomunicaciones que trasmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.4 Mantenimiento de los equipos	Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.5 Retirada de materiales propiedad de la empresa	Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.6 Seguridad de los equipos fuera de las instalaciones	Se deben controlar los riesgos de sacar los equipos fuera del local.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.7 Reutilización o eliminación segura de equipos	Se deben proteger los activos en el procedimiento de su borrado o reutilización.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.8 Equipo de usuario desatendido	Los usuarios deben proteger el equipo desatendido.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	11.2.9 Política de puesto de trabajo despejado y pantalla limpia	Se debe adoptar una política de escritorio limpio para documentos y soportes removibles así como una política de pantalla limpia.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 12: Seguridad de las Operaciones											
12.1 Procedimientos y responsabilidades operacionales	12.1.1 Documentación de los procedimientos de operación	Deben documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	12.1.2 Gestión de cambios	Se deben controlar los cambios en los sistemas de procesamiento de la Información.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	12.1.3 Gestión de capacidades	La Organización debe tener mecanismos de gestión de la capacidad en sus sistemas críticos.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	12.1.4 Separación de los recursos de desarrollo, prueba y operación-	Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024	40 Horas	Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso	Se deben implementar controles para la detección de código malicioso y la concienciación de los usuarios.	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024	40 Horas	Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
12.3 Copias de Seguridad	12.3.1 Copias de Seguridad de la información	Se deben realizar copias de seguridad de acuerdo a los procedimientos marcados.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
12.4 Registros y Supervisión	12.4.1 Registro de Eventos	Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	12.4.2 Protección de la información de registro	Se deben proteger los registros de la Organización de acuerdo a los requisitos estatutarios, reguladores, contractuales y de negocio.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	12.4.3 Registros de administración y operación	Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	12.4.4 Sincronización del reloj	Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente precisa y acordada.	L3	L3	No acciones necesarias año en curso						
12.5 Control del software en explotación	12.5.1 instalación del software en explotación	Se deben implementar procedimientos para controlar la instalación del software en explotación.	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2023	30/09/2023	40 Horas	Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
12.6 Gestión de la Vulnerabilidad Técnica	12.6.1 Gestión de las Vulnerabilidades Técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	12.6.2 Restricción en la instalación de software	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información así como tomar las medidas apropiadas para el tratamiento de los riesgos.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
12.7 Consideraciones sobre la auditoría de sistemas de información	12.7.1 Controles de auditoría de sistemas de información	Se deben planificar los requisitos y actividades de auditoría que involucran verificación de los sistemas tratando de minimizar el riesgo de interrupción.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 13: Seguridad de las Comunicaciones											
13.1 Gestión de la Seguridad de Redes	13.1.1 Controles de Red	Las redes deben ser gestionadas y controladas para proteger la información de los sistemas y aplicaciones	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	13.1.2 Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad de redes, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	13.1.3 Segregación en redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en redes.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
13.2 Intercambio de información	13.2.1 Políticas y procedimientos de intercambio de información	Deben establecerse políticas, procedimiento y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	13.2.2 Acuerdos de intercambio de información	Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	13.2.3 Mensajería electrónica	La información objeto de mensajería electrónica debe estar adecuadamente protegida	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	13.2.4 Acuerdos de confidencialidad o no revelación	Se deben identificar y revisar los acuerdos de confidencialidad que firma la Organización.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información											
14.1 Requisitos de seguridad en sistemas de información	14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Se deben especificar los requisitos de seguridad de las aplicaciones y sistemas.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	14.1.2 Asegurar los servicios de aplicaciones en redes públicas	La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizada.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	14.1.3 Protección de las transacciones de servicios de aplicaciones	La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración, revelación, duplicación o reproducción	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
14.2 Seguridad en el desarrollo y en los procesos de soporte	14.2.1 Política de Desarrollo seguro	Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	10/05/2024	40 Horas	Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.2 Procedimiento de control de cambios en sistemas	La aplicación de cambios se debe controlar mediante el uso de procedimientos formales de gestión de cambios.	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	10/05/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	El cambio en los sistemas operativos debe ser revisado con el objeto de probar el funcionamiento de las aplicaciones críticas de la Organización.	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	10/05/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.4 Restricciones a los cambios en los paquetes de software	Se debe desaconsejar las modificaciones en los paquetes de software limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	10/05/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.5 Principios de ingeniería seguros	Principios de ingeniería seguros se deben establecer, documentar, mantener y aplicar a todos los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.6 Entorno de Desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo de sistemas	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.7 Externalización del desarrollo de software	El desarrollo de software externalizado debe ser supervisado y controlado por la organización	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.8 Pruebas funcionales de seguridad de sistemas	Se deben llevar a cabo pruebas de seguridad funcional y controlado por la organización	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
	14.2.9 Pruebas de aceptación de sistemas	Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024		Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
14.3 Datos de prueba	14.3.1 Protección de datos de prueba	Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados	L3	L3	Se incopora Azure Devops para la gestión de la integración Continua del software	100%	10/05/2024	30/09/2024	20	Dpto Ti	Se implementa un nuevo procedimiento de revisión y testeo, junto a la incorporación de azure Devops para gestionar los desarrollos.
Dominio 15: Relación con los Proveedores											
15.1 Seguridad en las relaciones con los proveedores	15.1.1 Política de seguridad de la información en las relaciones con los proveedores	Los requisitos de SI para la mitigación de riesgos asociados con el acceso de proveedores a los activos de la organización deben acordarse con el proveedor y dejarlo documentado	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	15.1.2 Requisitos de seguridad en contratos con terceros	Todos los requisitos relacionados con la SI deben establecerse y acordarse con cada proveedor que pueda acceder, tratar, almacenar, comunicar o proporcionar componentes de infraestructura IT	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	15.1.3 Cadena de suministro de TIC	Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos relacionados con las TIC y con la cadena de suministro	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
15.2 Gestión de la provisión de servicios del proveedor	15.2.1 Control y revisión de la provisión de servicios del proveedor	Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	15.2.2 Gestión de cambios en la provisión de servicios del proveedor	Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 16: Gestión de Incidentes de Seguridad											
16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos	Se deben establecer las responsabilidades para asegurar la rápida respuesta frente a posibles incidencias de seguridad.	L3	L3	No acciones necesarias año en curso						
	16.1.2 Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información deben comunicarse a través de los canales diseñados a tal efecto lo antes posible.	L3	L3	No acciones necesarias año en curso						
	16.1.3 Notificación de puntos débiles de la seguridad	Se debe requerir que los usuarios, contratistas y terceros sean conscientes de que deben comunicar posibles debilidades de seguridad en los sistemas o servicios.	L3	L3	No acciones necesarias año en curso						
	16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	Se deben recoger, mantener y preservar las evidencias con el objeto de mantener las pautas de la legislación vigente.	L3	L3	No acciones necesarias año en curso						
	16.1.5 Respuesta a incidentes de seguridad	Los incidentes de seguridad deben ser respondidos de acuerdo con los procedimientos documentados	L3	L3	No acciones necesarias año en curso						
	16.1.6 Aprendizaje de los incidentes de seguridad	Deben existir mecanismos para permitir cuantificar y monitorizar los costes de los incidentes de seguridad de la información.	L3	L3	No acciones necesarias año en curso						
	16.1.7 Recopilación de evidencias	Se deben recoger, mantener y preservar las evidencias con el objeto de mantener las pautas de la legislación vigente.	L3	L3	No acciones necesarias año en curso						
Dominio 17: Aspectos de seguridad de la información para la gestión de la continuidad de negocio											
17.1 Continuidad de la seguridad de la información	17.1.1 Planificación de la Continuidad de SI	Se deben desarrollar planes de continuidad de negocio dentro de la Organización.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	17.1.2 Implementar la continuidad de seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
17.2 Redundancias	17.2.1 Disponibilidad de los recursos de tratamiento de la información	Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
Dominio 18: Cumplimiento											
18.1 Cumplimiento de los requisitos legales	18.1.1 identificación de la legislación aplicable y de los requisitos contractuales	Se deben definir, documentar y actualizar los requisitos estatutarios, reguladores y contractuales para cada sistema de información de la Organización.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	18.1.2 Derechos de propiedad intelectual	Se deben implementar los procedimientos adecuados para asegurar el cumplimiento de los requisitos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los derechos del software patentado.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	18.1.3 Protección de los registros de la organización	Se deben proteger los registros de la Organización de acuerdo a los requisitos estatutarios, reguladores, contractuales y de negocio.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	18.1.4 Protección y privacidad de la información de carácter personal	Se debe asegurar la protección y privacidad tal y como se reconoce en la legislación vigente y, si fuera aplicable, las cláusulas contractuales firmadas.	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
18.2 Revisiones de la seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la SI y su implantación debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de seguridad	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	18.2.2 Cumplimiento de las políticas y normas de seguridad	Los responsables de seguridad deben asegurarse de que todos los procedimientos de seguridad definidos en sus áreas se realicen según los procedimientos marcados dentro de la Organización.	L3	L4	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	
	18.2.3 Comprobación del cumplimiento técnico	Deben comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización	L3	L3	Configuración de Azure Defender para incluir controles manuales por parte del usuario y controles automáticos por parte de Microsft	80%	03/03/2024	16/12/2024	2 horas semanales	Dpto Ti	

5.3. RESULTADOS OBTENIDOS ANÁLISIS DEL RIESGO Y PLAN DE ACCIÓN DE LAS PARTES INTERESADAS.

Los resultados del análisis de riesgo para de las partes interesadas para el periodo 2024 se exponen pormenorizadamente en la **Tabla 13** siguiente y revelan que la mayoría de los stakeholders presentan un riesgo bajo o medio, con valores de riesgo que en su mayoría son aceptables y no requieren acciones de mitigación específicas. Sin embargo, se identificaron dos grupos clave, “Trabajadores” y “Colaboradores”, donde el valor de riesgo alcanzó un nivel de 3, lo que indica la necesidad de acciones correctivas inmediatas.

Por tanto, se estima que las medidas tomadas han sido eficaces a la hora de mitigar los riesgos identificados para las partes interesadas críticas, asegurando que se cumplan los requisitos de seguridad de la información de Innovatech Consulting en esta área y se mantenga un nivel adecuado de protección frente a posibles incidentes.

Concretamente, para los **Trabajadores**, se implementaron las siguientes acciones:

- **A.O. Curso de sensibilización seguridad de la información:** se elaboró la documentación correspondiente y se llevó a cabo dos sesiones formativas en marzo y mayo de 2024.
- **A.O. Firma del Memorandum de Confidencialidad:** Documento firmado por todos los empleados.
- **A.T. Creación de Identificadores de Acceso y Caducidad de Contraseñas:** Se creó un sistema de gestión de accesos y contraseñas, implementado por el Responsable de Tecnologías de la Información.

Para los **Colaboradores**, se implementaron las siguientes acciones:

- **A.O. Curso de Sensibilización Seguridad de la Información:** Similar al curso para los trabajadores, con formación en marzo y mayo de 2024.
- **A.O. Firma del memorandum de confidencialidad:** Firmado por todos los colaboradores.
- **A.O. Establecimiento en los contratos de niveles de servicio para el control de seguridad:** Definición de indicadores de control.
- **A.T. Creación de Identificadores de Acceso y Caducidad de Contraseñas en NormaPro:** Gestión llevada a cabo por el Responsable de Tecnologías de la Información.

Tabla 13: ANÁLISIS DE RIESGOS DE LAS PARTES INTERESADAS Y PLAN DE ACCIÓN PARA LA MITIGACIÓN DEL RIESGO

Nivel de Probabilidad	Criterios de Evaluación	Descripción del Nivel de Probabilidad
1 - Muy baja	Pocas o ninguna amenaza documentada en el pasado.	La amenaza identificada es extremadamente improbable y no hay historial de ocurrencias similares en la organización. Históricamente, no ha ocurrido esta amenaza en InnovaTech Consulting o en organizaciones similares, y es altamente improbable que ocurra en el futuro.
2 - Baja	Amenazas raras pero posibles.	La amenaza es poco frecuente, aunque puede ocurrir en casos excepcionales. La organización ha experimentado pocos eventos similares. Ha habido casos limitados de ocurrencias en el pasado, pero no es común que suceda. Se asocia con eventos aislados.
3 - Media	Amenazas que pueden ocurrir ocasionalmente.	La amenaza ha ocurrido en la organización o en contextos similares con cierta frecuencia, pero no es recurrente. Ha ocurrido ocasionalmente en la organización o en su industria. La probabilidad de que ocurra en el futuro es moderada.
4 - Alta	Amenazas con historial frecuente o condiciones que aumentan la probabilidad.	La amenaza es recurrente o las condiciones actuales aumentan la exposición del activo a dicha amenaza. Es probable que ocurra debido a las condiciones actuales o históricas. La organización tiene antecedentes de eventos similares.
5 - Muy alta	Amenaza prácticamente asegurada.	La amenaza ha ocurrido regularmente o es muy probable que ocurra en el futuro cercano dado el contexto del activo. Es casi seguro que ocurra. Las condiciones internas o externas indican un riesgo inminente y recurrente.

Nivel de Impacto	Criterios de Evaluación	Descripción del Nivel de Impacto
1 - Impacto bajo (-)	Consecuencias mínimas para la operación.	La amenaza tiene un impacto prácticamente insignificante sobre la operación, con consecuencias leves que pueden pasar desapercibidas. La amenaza tendría un impacto mínimo sobre el activo y sobre la operación de la empresa. Por ejemplo, pequeñas modificaciones en documentos internos sin mayor repercusión.
2 - Impacto bajo (+)	Consecuencias menores y manejables.	La amenaza podría causar leves interrupciones o inconvenientes, pero la operación puede continuar sin grandes dificultades. La amenaza podría causar inconvenientes menores, pero su impacto es manejable. Ejemplo: Pequeñas interrupciones en sistemas secundarios.
3 - Impacto medio (-)	Consecuencias moderadas, que requieren atención.	La amenaza provoca una interrupción en algunos procesos, afectando la operación o los servicios temporalmente. La amenaza podría generar una interrupción temporal o daños parciales que afectan a la operativa o a la calidad del servicio, pero se puede gestionar de forma relativamente rápida.
4 - Impacto medio (+)	Consecuencias significativas que requieren intervención.	La amenaza afecta gravemente la operación o algunos servicios, requiriendo acciones correctivas inmediatas para evitar daños mayores. El impacto de la amenaza es serio y requiere una intervención rápida para evitar mayores consecuencias. Ejemplo: Fallo temporal en servicios críticos para la empresa.
5 - Impacto alto	Consecuencias críticas y duraderas.	La amenaza tendría consecuencias catastróficas para la confidencialidad, integridad o disponibilidad de la información, con impactos financieros, reputacionales o legales graves. El impacto es catastrófico, afectando gravemente a la operación, la reputación o las finanzas de la empresa. Ejemplo: Pérdida total de datos críticos o paralización de operaciones claves.

Valor de Riesgo Real	Nivel de Riesgo	Descripción del Nivel de Riesgo
1	Riesgo Bajo (-)	**El riesgo es considerado bajo y no se requiere intervención inmediata. Los controles actuales son suficientes para mitigar las amenazas sin un impacto significativo.** Este nivel indica un riesgo muy bajo, que no representa una amenaza para la operación de los activos. El sistema de seguridad actual es efectivo, y no se espera un impacto considerable. No se requiere acción inmediata, pero se puede realizar una revisión periódica.
2	Riesgo Bajo (+)	**El riesgo es todavía bajo, pero debe ser monitorizado. Aunque no requiere una acción inmediata, puede que se necesite ajustar algunos controles para mayor seguridad.** Este nivel implica que el riesgo sigue siendo bajo, pero debe vigilarse de cerca. Es posible que algunos controles existentes necesiten ser ajustados o reforzados, dependiendo de cómo evolucione el entorno de amenazas.
3	Riesgo Medio (-)	**El riesgo es moderado y podría causar problemas en ciertos activos. Se recomienda una revisión de los controles actuales para prevenir un impacto mayor.** Aquí se observa un riesgo moderado, que podría comprometer los activos si no se aborda correctamente. Se recomienda evaluar las medidas preventivas y, si es necesario, mejorar los controles de seguridad existentes para evitar posibles impactos.
4	Riesgo Medio (+)	**El riesgo es alto-moderado y requiere tratamiento. Los controles actuales no son totalmente efectivos y pueden necesitar mejoras para evitar posibles daños.** Este nivel representa un riesgo significativo que necesita ser tratado con prioridad. Aunque no es crítico, existe la posibilidad de que las amenazas se materialicen si no se implementan medidas adicionales. Una revisión completa de los controles es necesaria.
5	Riesgo Alto	**El riesgo es significativo y debe ser mitigado lo antes posible. Se debe implementar un plan de acción inmediato para reducir tanto la probabilidad como el impacto.** Este es el nivel más alto de riesgo, que probablemente causará impactos graves si no se aborda de inmediato. Las medidas correctivas deben implementarse de manera urgente para evitar daños significativos en la seguridad de la información o la operación de la empresa.

INNOVATECH CONSULTING

LISTADO PARTES INTERESADAS	PROBABILIDAD	IMPACTO	VALOR RIESGO	ACCIONES MITIGACIÓN RIESGO	Grado de Avance	Fecha Inicio	Fecha Fin	Recursos	Responsable Accion	Observaciones
ACCIONISTAS/ INVERSORES	2	3	2,5	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
TRABAJADORES	4	2	3	A.O. Curso de Sensibilización Seguridad de la Información	100%	01/05/2024	01/05/2024	1 horas	Noemí M.	Se ha elaborado la documentación y se ha llevado a cabo la formación según el manual de buenas prácticas en seguridad de la información.
				A.O. Firma por todos los empleados del memorandun de Confidencialidad	100%	01/02/2024	01/02/2024	2 horas	Noemí M.	Elaborado el Memorandum. Firmado por todo el personal.
				A.T. Creación de identificadores de Acceso a los Equipos y caducidad de las contraseñas	100%	02/02/2024	02/02/2024	8 horas	Antonio T.	Realizado por el Responsable de Tecnologías de la Información
PROVEEDORES	3	2	2,5	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
CLIENTES	2	2	2	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
COLABORADORES	4	2	3	A.O. Curso de Sensibilización Seguridad de la Información	100%	01/05/2024	01/05/2024	1 horas	Noemí M.	Se ha elaborado la documentación y se ha llevado a cabo la formación según el manual de buenas prácticas en seguridad de la información.
				A.O. Firma por todos los empleados del memorandun de Confidencialidad	100%	01/02/2024	01/02/2024	2 horas	Noemí M.	Elaborado el Memorandum. Firmado por todo el personal.
				A.O Estableciendo en los contratos de los niveles de servicio para el control de los elementos intervinientes en la seguridad	100%	01/07/2024	02/07/2024	4 horas	Julio A.	Se han establecido los indicadores de control
				A.O Documentación de la Normativa de Gestión de Servicios Ofrecidas por Terceros	100%	01/07/2024	N/A	4 horas	Noemí M.	Elaborada. Se ha aprobado por parte de Dirección y se ha comunicado al personal y publicado a través de la plataforma NormaPro.
				A.O Desarrollo, documentación y Consenso de un modelo de continuidad de negocio alineado con Terceros	100%	01/02/2024	01/05/2024	8 horas	Noemí M.	Se ha aprobado y comunicado el Plan de Continuidad de Negocio a través de la plataforma NormaPro.
				A.O Documentación de los Procesos de Terceros , e implantación de Indicadores de control	100%	14/07/2024	16/07/2024	16 horas	Noemí M.	Se han definido indicadores de control según la operativa de INC y se han medido y analizado para el año 2024.
				A.T. Creación de identificadores de Acceso a los Equipos y Servicios NormaPro y caducidad de las contraseñas	100%	02/02/2024	02/02/2024	8 horas	Antonio T.	Realizado por el Responsable de Tecnologías de la Información
COMITÉ SIG	2	2	2	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
ALTA DIRECCIÓN	2	2	2	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
ENTIDADES FINANCIERAS	2	1	1,5	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
COMPETENCIA	2	1	1,5	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
ORGANISMOS REGULATORIOS	2	2	2	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
ADMINISTRACIÓN PÚBLICA	2	3	2,5	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						
ASOCIACIOENES SECTORIALES	2	2	2	El "valor riesgo" de la parte interesada no precisa acción para la mitigación del riesgo						

5.4. OBJETIVOS E INDICADORES DE SEGURIDAD.

El marco de este Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001, establece como requisito fundamental establecer mecanismos que permitan medir y evaluar de manera continua la eficacia de las políticas, controles y procesos de seguridad. Para ello, se han desarrollado una serie de indicadores clave que proporcionan una visión cuantitativa y cualitativa sobre el estado de la seguridad de la información en la organización.

Estos indicadores han sido diseñados para cumplir con varios objetivos estratégicos, tales como la monitorización constante del cumplimiento normativo, la identificación de áreas de mejora, la optimización de recursos y la mitigación de riesgos potenciales. A través de ellos, no solo se asegura la conformidad con este estándar internacional, sino que también se promueve una cultura de mejora continua en la gestión de la seguridad de la información.

A continuación, en las **Tablas 14 y 15** se presentan un conjunto de tablas que detallan algunos de los diferentes indicadores establecidos, junto con sus métodos de cálculo, periodicidad de seguimiento y los objetivos específicos que se buscan alcanzar. Esta información es fundamental para la toma de decisiones basada en datos, permitiendo a la organización adaptarse proactivamente a las dinámicas cambiantes del entorno de seguridad.

Tabla 14: Cuadros de seguimiento de Objetivos e indicadores (K1 al K5).

Indicador K1

INDICADOR: K1	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de riesgos de seguridad de la información para los cuales se han implantado controles	Responsable Seguridad de la Información	Anual	Mediciones	100%	100%										
			%Media Anual	100%											
			Objetivo	100%											

MÉTODO DE CÁLCULO:
Numero de riesgos identificados sobre los que se ha aplicado controles.

Comentarios:
Se incorpora una persona a comerciales nuevos de los cuales aun no se ha realizado el análisis de riesgos, puesto que aun esta por decidir que información es la que va a manejar El comercial deja de trabajar en la empresa en el mes de agosto y se le retiran todos los permisos de acceso a la información de la empresa.

Indicador K2

INDICADOR: K2	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de cambios aprobados con error conocido por incidencias	Responsable Seguridad de la Información	Mensual	Mediciones	0%	0%										
			%Media Anual	0%											
			Objetivo	<10%											

MÉTODO DE CÁLCULO:
Total de cambios implementados en el entorno de producción que han dado lugar a una incidencia, calculado en % sobre el total de cambios implementados en el entorno de producción.

Comentarios:
Como se ha implementado Nilo y se hacen 2 publicaciones al año y el testeo de las aplicaciones casi se va a 6 meses en nilo antes de pasar a danubio con lo que se están eliminando los cambios que se hayan aprobado con error por incidencia. Este indicador tiende a desaparecer. En 2020 solo se va a realizar una publicación en Danubio prevista para diciembre de 2020. En 2021 continuamos con el sistema de Rolling Release y se van a implementar cambios en el entorno de producción segun lo previsto en el plan de trabajo. En 2022 Hemos implementado un procedimiento nuevo de desarrollo, que contempla los análisis de vulnerabilidades para buscar la integración Continua. En 2023 Gracias a los procesos de verificación y control de código implementados el indicador no se ve afectado, se conserva puesto que la medición es automática y nos parece interesante

Indicador K3

INDICADOR: K3	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de cambios aprobados con error conocido que han necesitado marcha atrás	Responsable Seguridad de la Información	Mensual	Mediciones	0%	0%										
			%Media Anual	0%											
			Objetivo	<5%											

MÉTODO DE CÁLCULO:
Total de cambios implementados en el entorno de producción aprobados por el Responsable de Seguridad y que han necesitado el proceso de marcha.atrás, calculado en % sobre el total de cambios implementados mensualmente.

Comentarios:
Como se ha implementado Nilo y se hacen 2 publicaciones al año y el testeo de las aplicaciones casi se va a 6 meses en nilo antes de pasar a danubio con lo que se están eliminando los cambios que se hayan aprobado con error por incidencia. Este indicador tiende a desaparecer. En 2020 solo se va a realizar una publicación en Danubio prevista para diciembre de 2020. En 2021 continuamos con el sistema de Rolling Release y se van a implementar cambios en el entorno de producción segun lo previsto en el plan de trabajo. En 2022 Hemos implementado un procedimiento nuevo de desarrollo, que contempla los análisis de vulnerabilidades para buscar la integración Continua. En 2023 Idem al anterior.

Indicador K4

INDICADOR: K4	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de incidencias críticas de seguridad atendidas en 24 horas	Responsable Seguridad de la Información	Mensual	Mediciones	100%	100%										
			%Media Anual	100%											
			Objetivo	<95%											

MÉTODO DE CÁLCULO:
Porcentaje de incidencias identificadas como críticas para seguridad, y que han sido atendidas en menos de 24 horas (días laborables), calculado en % , SE CONSIDERA PARA EL CÁLCULO QUE SI NO HAY INCIDENCIAS EN ESE MES , EL PORCENTAJE DE ATENCIÓN ES DEL 100 %

Comentarios:

Indicador K5

INDICADOR: K5	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Número de incidencias causadas por fallo de un Tercero	Responsable Seguridad de la Información	Mensual	Mediciones	0	0										
			Total Anual	1											
			Objetivo	<4											

MÉTODO DE CÁLCULO:
Recuento de incidencias por terceros

Comentarios:
Se Creía culpable de pm2 a la ultima incidencia de caida de servicio de más de 5 minutos, pero analizando los logs se ha verificado que ha sido una mala configuración del servidor que dejaba exahusto los nucleos de proceso.

Tabla 15: Cuadros de seguimiento de Objetivos e indicadores (K6 al K10).

Indicador K6

INDICADOR: K6	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de incidencias causadas por falta de capacidad	Responsable Seguridad de la Información	Mensual	Mediciones	0%	0%										
			Media Anual	0%											
			Objetivo	<5%											

MÉTODO DE CÁLCULO:
Incidencias totales que después de su análisis han resultado ser por falta de capacidad en los servidores o discos, calculado en % sobre el total de incidencias detectadas mensualmente.

Comentarios:
Se está llevando a cabo un mantenimiento preventivo diario analizando la capacidad de los servidores. Se comprueba que se está por debajo del 80% de la capacidad en todos los servidores. Se están cumpliendo las previsiones de capacidad realizadas a inicio del año. Como ya nos encontramos cerca del 80% de capacidad se decide pasar a BLOB con AZURE para no desbordar la capacidad. De ahí que se vaya a hacer el redimensionamiento de la aplicación. En este momento este indicador dejará de medirse.

Indicador K7

INDICADOR: K7	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de incidencias resueltas en un plazo menor de 30 días	Responsable Seguridad de la Información	Mensual	Mediciones	100%	100%										
			Media Anual	0%											
			Objetivo	>95%											

MÉTODO DE CÁLCULO:
Tiempo de resolución de incidencias, calculado en % sobre el total de incidencias detectadas mensualmente. SI UN MES NO HA HABIDO INCIDENCIAS SE CONSIDERA UN CUMPLIMIENTO DEL 100%

Comentarios:
Siempre que se está produciendo una incidencia se detiene el desarrollo de nuevas mejoras y se solventa la incidencia. Se estudiará la posibilidad de reducir el valor objetivo a <15 días.

Indicador K8

INDICADOR: K8	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de suministradores, sin contrato alineado con el SIG	Responsable Seguridad de la Información	Mensual	Mediciones	0%	0%										
			Media Anual	0%											
			Objetivo	<0%											

MÉTODO DE CÁLCULO:
Número de suministradores nuevas que no tienen contrato alineado con el SGSI. En porcentaje frente al total de suministradores existentes

Comentarios:
Solo se tienen como proveedores a Azure, 1&1, Scaleway, MailChimp y como desarrollador externo a Jose Ibáñez González con el que se establecen contratos por encargo.

Indicador K9

INDICADOR: K9	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
% de empleados que han recibido formación en materia de seguridad de la información	Responsable Seguridad de la Información	Mensual	Mediciones	100%	100%										
			Ultimo dato	100%											
			Objetivo	Finalizar el año al 100%											

MÉTODO DE CÁLCULO:
Personas dadas de alta con el curso de seguridad de la información. En porcentaje frente al total de empleados dados de alta en el año.

Comentarios:
Se incorporan dos personas nuevas, por motivos de la alta carga de trabajo no se encuentra tiempo disponbible para la impartición de la formación en buenas prácticas de seguridad de la información hasta el més de septiembre, donde además de a las nuevas incoporaciones se hacen un repaso a todos los trabajadores de las mismas.
Abandonan la empresa en el mes de agosto por motivos de producción

Indicador K10

INDICADOR: K10	RESP. SEGUIMIENTO	PERIODICIDAD SEGUIMIENTO	RESULTADO	SEGUIMIENTO											
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Nº de empleados nuevos sin formación en materia de Seguridad de la Información	Responsable Seguridad de la Información	Mensual	Mediciones	0	0										
			Ultimo dato	0											
			Objetivo	Finalizar el año con 0 personas sin formar											

MÉTODO DE CÁLCULO:
Personas dadas de alta sin la formación en seguridad de la información.

Comentarios:
En 2021 solo se han contratado 2 personas para refozar el equipo y debido a la carga de producción no las hemos podido formar debidamente hasta septiembre. Para preveer problemas durante los tres meses han estado bajo completa supervisión. En 2022 Se incoporó Diana Rámirez para cubrir la baja de maternal de Teresa Martínez. Se ha formado en la última semana de octubre En 2023 Se ha incorporado a la empresa una persona nueva. Esta persona dejar de estar en plantilla en el mes de agosto.

5.5. RESULTADOS OBTENIDOS DE LA DECLARACIÓN DE APLICABILIDAD (SOA).

El análisis de la Declaración de Aplicabilidad (SOA) ha permitido identificar y estructurar los controles de seguridad implementados en Innovatech Consulting en función de su aplicabilidad y la integración de los requisitos del Anexo A de la norma ISO/IEC 27001. Para este TFG se ha utilizado la versión más actual de este Anexo ya que debe estar complementada en las empresas certificadas antes del 31 de diciembre de 2024. Los resultados reflejan el compromiso de la empresa con la seguridad de la información y su alineación con los estándares internacionales, proporcionando una base sólida para la continuidad del negocio y la protección de sus activos más valiosos. A continuación, se destacan aspectos relevantes observados en la **Tabla 16** "Declaración de aplicabilidad (SOA) que se acompaña en este capítulo y en la que se detallan los resultados obtenidos en función de los controles aplicados.

A.5 Controles Organizativos.

1. **Políticas para la seguridad de la información (A.5.1):** La política de seguridad de la información ha sido implementada y comunicada a todos los empleados, lo que refuerza la cultura de seguridad en la organización. Este control es fundamental para establecer un marco de referencia que guíe todas las actividades relacionadas con la seguridad de la información.

2. **Clasificación y etiquetado de la información (A.5.12, A.5.13):** Se han establecido procedimientos claros para la clasificación y el etiquetado de la información según su sensibilidad. Esto permite una gestión adecuada de la información y minimiza los riesgos asociados con su tratamiento.

3. **Control de acceso (A.5.15):** Los mecanismos de control de acceso están alineados con los requisitos de negocio y la criticidad de los sistemas, asegurando que solo el personal autorizado pueda acceder a la información sensible. Este control es clave para prevenir accesos no autorizados y proteger la integridad de los sistemas.

4. **Gestión de identidades y autenticación (A.5.16, A.5.17):** La implementación de un sistema robusto de gestión de identidades y autenticación refuerza la seguridad en el acceso a los sistemas de información. Se han adoptado medidas para garantizar que solo los usuarios autenticados puedan acceder a los recursos críticos.

A.6 Controles Relacionados con las Personas.

1. **Evaluación previa al empleo y términos de empleo (A.6.1, A.6.2):** Se ha establecido un proceso exhaustivo de evaluación previa al empleo y se han definido claramente los términos y condiciones de empleo relacionados con la seguridad de la información. Esto asegura que todos los empleados estén alineados con los objetivos de seguridad de la organización desde el inicio de su contratación.
2. **Formación y concienciación en seguridad (A.6.3, A.6.7):** Innovatch Consulting ha implementado programas continuos de formación y concienciación en seguridad de la información, que son fundamentales para mantener a los empleados actualizados y preparados para gestionar los riesgos de seguridad.
3. **Proceso disciplinario y responsabilidades tras la terminación del empleo (A.6.4, A.6.5):** La existencia de un proceso disciplinario claro y la definición de responsabilidades tras la terminación del empleo garantizan que se aborden adecuadamente las brechas de seguridad provocadas por el comportamiento del personal.

A.7 Controles Físicos.

1. **Control de acceso físico y seguridad en las instalaciones (A.7.2, A.7.3):** Las medidas implementadas para controlar el acceso físico y garantizar la seguridad en oficinas son adecuadas para proteger los activos físicos y la información almacenada en ellos.
2. **Monitorización de la seguridad física (A.7.4):** La monitorización en continuo de la seguridad física proporciona una capa adicional de protección, permitiendo una respuesta rápida ante cualquier incidente de seguridad que pueda comprometer los activos físicos de la organización.
3. **Eliminación segura de equipos y retiro de activos (A.7.10, A.7.11):** Se han establecido procedimientos rigurosos para la eliminación segura o reutilización de equipos, así como para el retiro de activos, asegurando que la información contenida en estos dispositivos no sea accesible después de su baja.

A.8 Controles Tecnológicos.

1. **Protección contra malware y gestión de vulnerabilidades (A.8.7, A.8.8):** Se han implementado controles efectivos para la detección y mitigación de malware, así como para la gestión de vulnerabilidades técnicas, lo que es crucial para mantener la seguridad de los sistemas operacionales.

2. **Enmascaramiento y prevención de fuga de datos (A.8.11, A.8.12):** Estos controles han sido diseñados para proteger la confidencialidad de la información mediante técnicas de enmascaramiento de datos y prevención de fugas, lo que reduce significativamente los riesgos de exposición no autorizada de datos sensibles.
3. **Seguridad de la red y control de acceso (A.8.20, A.8.34):** La seguridad de la red y el control de acceso a la misma han sido reforzados con medidas avanzadas de monitoreo y filtrado del tráfico, asegurando que solo el tráfico autorizado pueda pasar a través de la red corporativa.

En líneas generales, los resultados más importantes se engloban en tres grandes grupos:

- **Eficiencia en la Gestión de Riesgos:** La implementación de controles como la clasificación y etiquetado de la información, junto con la gestión de identidades, ha permitido una gestión más eficiente de los riesgos, reduciendo la probabilidad de incidentes de seguridad.
- **Fortalecimiento de la Cultura de Seguridad:** Los programas continuos de formación y concienciación en seguridad han jugado un papel clave en fortalecer la cultura de seguridad en Innovatech Consulting, asegurando que todos los empleados comprendan la importancia de seguir las políticas y procedimientos de seguridad.
- **Robustez en la Protección de la Información:** Los controles tecnológicos implementados, incluyendo la seguridad de la red, el enmascaramiento de datos y la prevención de fugas, han sido efectivos en proteger la información crítica de la organización contra amenazas internas y externas.

Tabla 16: Declaración de aplicabilidad (SOA).

INNOVATECH CONSULTING

	Control	Aplicabilidad	Justificación de la inclusión	Descripción del control	Responsable	Evidencia de cumplimiento	Localización
1. A.5 Controles Organizacionales	A.5.1 Políticas para la seguridad de la información	Sí	Cumplimiento normativo según la cláusula 5.2	La Dirección debe aprobar un documento de Política de Seguridad que debe ser pública y comunicada a todos los empleados y entidades externas relevantes.	Comité SIG	Documento de la Política de Seguridad de la Información aprobado, publicado y comunicado a los empleados y partes interesadas.	Documento "Política del SIG" de Innovatech Consulting
	A.5.2 Roles y responsabilidades en la seguridad de la información	Sí	Necesidad de clara definición de roles para evitar ambigüedades en responsabilidades	Definir y asignar roles y responsabilidades claras en la seguridad de la información para todos los empleados y partes interesadas.	Comité SIG	Organigrama de seguridad de la información, procedimientos internos de asignación de roles.	Manual del SIG de Innovatech Consulting
	A.5.3 Segregación de deberes	Sí	Mitigación de riesgos de fraude interno y errores humanos	Implementar la segregación de funciones críticas para evitar conflictos de intereses y riesgos de seguridad.	Comité SIG	Procedimientos documentados para la segregación de funciones, auditorías periódicas de cumplimiento.	Procedimiento de control de accesos, auditorías internas de Innovatech Consulting
	A.5.4 Responsabilidades de la gestión	Sí	Asegurar la responsabilidad en la gestión de la seguridad	Establecer y documentar las responsabilidades específicas de gestión en materia de seguridad de la información, con revisiones periódicas.	Dirección de Innovatech Consulting	Actas de reuniones de gestión, documentación de responsabilidades, revisiones anuales.	Manual del SIG, actas de reuniones de la dirección
	A.5.5 Contacto con autoridades	Sí	Requisito legal y necesidad de coordinación con autoridades en caso de incidentes	Mantener contactos y procedimientos de comunicación con autoridades relevantes para la seguridad de la información.	Dirección General	Registro de contactos con autoridades, correspondencia formal.	Manual del SIG, archivo de comunicaciones oficiales
	A.5.6 Contacto con grupos de interés especial	Sí	Importancia de mantenerse actualizado con las mejores prácticas de seguridad	Mantener contactos apropiados con grupos de seguridad especializados y asociaciones profesionales para intercambio de información.	Comité SIG / Dpto. de Tecnologías de la Información	Lista de suscripciones a grupos, actas de participación en asociaciones.	Documentación de participación en asociaciones, listas de contactos relevantes
	A.5.7 Inteligencia sobre amenazas	Sí	Mejora de la capacidad de anticipación a amenazas	Implementar un sistema de inteligencia sobre amenazas para detectar y mitigar riesgos antes de que se materialicen.	Dpto. de Seguridad de la Información	Informes de inteligencia sobre amenazas, resultados de análisis preventivos.	Informes de amenazas, registros de acciones preventivas en Innovatech Consulting
	A.5.8 Seguridad de la información en la gestión de proyectos	Sí	Integración de la seguridad desde el inicio de los proyectos	Asegurar que todos los proyectos consideren la seguridad de la información desde la planificación hasta la ejecución.	Responsable del SIG	Documentación de proyectos con planes de seguridad, auditorías de cumplimiento en fases de proyectos.	Procedimiento de gestión de proyectos, auditorías internas de Innovatech Consulting
	A.5.9 Inventario de información y otros activos asociados	Sí	Control riguroso de los activos de información	Crear y mantener un inventario actualizado de los activos de información, identificando propietarios y clasificándolos según su criticidad.	Responsable del SIG	Inventario de activos actualizado, registros de revisiones periódicas.	Archivo del inventario de activos, Plan de Riesgos actualizado
	A.5.10 Uso aceptable de la información y otros activos asociados	Sí	Asegurar el correcto uso de la información y los recursos	Definir y comunicar reglas claras sobre el uso aceptable de la información y activos, y realizar auditorías de cumplimiento.	Comité SIG	Políticas de uso aceptable documentadas, informes de auditoría de cumplimiento.	Documentación sobre Normas de Buenas Prácticas de Seguridad de la Información, resultados de auditorías
	A.5.11 Devolución de activos	Sí	Cumplimiento normativo y protección de activos al finalizar la relación laboral o contractual	Todos los empleados y terceras partes deben devolver los activos a la organización al finalizar su relación, siguiendo un procedimiento documentado.	Responsable del SIG	Formularios de devolución de activos, registros de inventario actualizados.	Procedimiento "Devolución de Activos" en el Manual del SIG
	A.5.12 Clasificación de la información	Sí	Protección de la información según su criticidad y sensibilidad	Clasificar la información en función de su valor, sensibilidad y criticidad, de acuerdo con los requisitos legales y de negocio.	Responsable del SIG	Sistema de clasificación de la información implementado, revisiones periódicas.	Procedimiento "Clasificación de la Información" en el SIG
	A.5.13 Etiquetado de la información	Sí	Identificación visual de la información según su clasificación	Implementar un sistema de etiquetado de la información que refleje su clasificación y permita un manejo adecuado según su nivel de protección.	Responsable del SIG	Etiquetas implementadas en documentos, revisiones de cumplimiento del etiquetado.	Procedimiento "Etiquetado de la Información" en el SIG
	A.5.14 Transferencia de información	Sí	Protección de la información durante su transferencia, ya sea interna o externa	Establecer procedimientos seguros para la transferencia de información, asegurando la confidencialidad, integridad y disponibilidad durante el proceso.	Responsable del SIG	Registros de transferencias, auditorías de cumplimiento de la política de transferencia.	Procedimiento "Transferencia Segura de Información" en el SIG
	A.5.15 Control de acceso	Sí	Control de acceso a la información en función de roles y responsabilidades	Implementar controles de acceso a los sistemas y la información basados en la política definida, asegurando que solo los usuarios autorizados acceden a la información según sus roles.	Responsable del SIG	Registros de acceso, auditorías de control de acceso, logs de sistemas.	Procedimiento "Control de Accesos" en el SIG
	A.5.16 Gestión de identidades	Sí	Identificación y autenticación de usuarios para acceso seguro	Gestionar la identidad de los usuarios, incluyendo la creación, modificación y eliminación de cuentas, asegurando que los usuarios están correctamente autenticados.	Responsable del SIG	Registros de identidades, auditorías de gestión de identidades.	Procedimiento "Gestión de Identidades" en el SIG
	A.5.17 Información de autenticación	Sí	Protección de los métodos de autenticación y credenciales de acceso	Implementar controles para la protección de la información de autenticación, incluyendo la creación, almacenamiento y transmisión segura de contraseñas y otros datos de autenticación.	Responsable del SIG	Registros de autenticación, auditorías de seguridad de contraseñas.	Procedimiento "Autenticación Segura" en el SIG
	A.5.18 Derechos de acceso	Sí	Asignación y revisión de derechos de acceso según roles y funciones	Establecer y gestionar los derechos de acceso de los usuarios, asegurando que solo se otorguen los permisos necesarios para realizar sus funciones, con revisiones periódicas.	Responsable del SIG	Registros de permisos, auditorías de derechos de acceso, informes de revisión.	Procedimiento "Gestión de Derechos de Acceso" en el SIG
	A.5.19 Seguridad de la información en las relaciones con proveedores	Sí	Protección de la información en manos de terceros	Implementar controles para gestionar y proteger la información compartida con proveedores, asegurando que se cumplen los requisitos de seguridad en los contratos y durante la prestación de servicios.	Responsable del SIG	Contratos con proveedores, auditorías de cumplimiento, acuerdos de confidencialidad.	Procedimiento "Gestión de Proveedores" en el SIG
	A.5.20 Seguridad de la información en la cadena de suministro de TIC	Sí	Gestión de riesgos en la cadena de suministro de TIC	Establecer controles para mitigar los riesgos asociados a la cadena de suministro de tecnologías de la información y comunicaciones, incluyendo proveedores y subcontratistas.	Responsable del SIG	Evaluaciones de riesgos en la cadena de suministro, auditorías de cumplimiento, contratos.	Procedimiento "Gestión de la Cadena de Suministro de TIC" en el SIG
	A.5.21 Planificación y preparación para la gestión de incidentes de seguridad de la información	Sí	Mitigar impactos de incidentes de seguridad	Establecer y documentar planes de acción para la gestión eficaz de incidentes de seguridad, incluyendo roles, responsabilidades y recursos necesarios.	Responsable del SIG	Planes de gestión de incidentes, simulacros realizados, informes de pruebas.	Procedimiento "Gestión de Incidentes de Seguridad" en el SIG
	A.5.22 Evaluación y decisión sobre eventos de seguridad de la información	Sí	Reacción rápida y efectiva ante incidentes	Evaluar y decidir acciones correctivas y preventivas ante eventos de seguridad, con base en criterios preestablecidos para minimizar riesgos.	Responsable del SIG	Informes de evaluación de eventos, registros de decisiones tomadas.	Procedimiento "Evaluación de Incidentes" en el SIG
	A.5.23 Respuesta a incidentes de seguridad de la información	Sí	Protección continua de la información	Implementar un proceso documentado para la respuesta inmediata a incidentes de seguridad, incluyendo comunicación y resolución de incidentes.	Responsable del SIG	Registros de incidentes, informes de respuesta, logs de acciones realizadas.	Procedimiento "Respuesta a Incidentes de Seguridad" en el SIG
	A.5.24 Aprendizaje a partir de incidentes de seguridad de la información	Sí	Mejora continua del SGSI	Desarrollar mecanismos para analizar y aprender de los incidentes de seguridad ocurridos, incorporando las lecciones aprendidas en el SGSI.	Responsable del SIG	Informes de análisis post-incidente, documentación de mejoras implementadas.	Procedimiento "Lecciones Aprendidas de Incidentes" en el SIG
	A.5.25 Recopilación de pruebas	Sí	Soporte a investigaciones y acciones legales	Implementar procesos para la recopilación, protección y conservación de pruebas relacionadas con incidentes de seguridad, asegurando su integridad.	Responsable del SIG	Registros de recopilación de pruebas, auditorías de integridad de evidencias.	Procedimiento "Recopilación y Conservación de Pruebas" en el SIG
	A.5.26 Seguridad de la información durante interrupciones	Sí	Continuidad operativa en situaciones de crisis	Establecer medidas de seguridad para proteger la información y mantener operaciones críticas durante interrupciones o desastres.	Responsable del SIG	Plan de continuidad, informes de pruebas de recuperación, auditorías de resiliencia.	Plan de Continuidad del Negocio en el SIG
	A.5.27 Seguridad de la información para el uso de servicios en la nube	Sí	Protección de datos en entornos de nube	Implementar controles específicos para asegurar la protección de la información al utilizar servicios en la nube, incluyendo evaluación de proveedores y gestión de riesgos.	Responsable del SIG	Evaluaciones de proveedores de nube, auditorías de seguridad en la nube, registros de accesos.	Procedimiento "Seguridad en la Nube" en el SIG
	A.5.28 Ciclo de vida de desarrollo seguro	Sí	Reducción de riesgos en el desarrollo de software	Incorporar prácticas de seguridad en todas las fases del ciclo de vida de desarrollo de software, desde el diseño hasta el despliegue y mantenimiento.	Responsable del SIG	Registros de revisiones de seguridad, auditorías de código, informes de pruebas de seguridad.	Procedimiento "Desarrollo Seguro de Software" en el SIG
	A.5.29 Requisitos de seguridad de las aplicaciones	Sí	Protección de aplicaciones contra amenazas	Definir y aplicar requisitos de seguridad específicos para el desarrollo y operación de aplicaciones, asegurando su resistencia ante amenazas.	Responsable del SIG	Documentación de requisitos de seguridad, auditorías de cumplimiento, pruebas de penetración.	Procedimiento "Requisitos de Seguridad en Aplicaciones" en el SIG
	A.5.30 Protección de datos de prueba	Sí	Evitar filtraciones de datos en entornos de prueba	Implementar controles para proteger los datos utilizados en entornos de prueba, asegurando su anonimización o eliminación tras su uso.	Responsable del SIG	Registros de protección de datos de prueba, auditorías de cumplimiento de políticas de prueba.	Procedimiento "Protección de Datos en Entornos de Prueba" en el SIG
	A.5.31 Seguridad de la información en el desarrollo de software	Sí	Reducción de vulnerabilidades en software	Incorporar medidas de seguridad en todo el ciclo de vida del desarrollo de software para prevenir vulnerabilidades y asegurar la integridad del código.	Responsable de Desarrollo	Registros de revisiones de seguridad, auditorías de código seguro, informes de pruebas de seguridad.	Procedimiento "Desarrollo Seguro de Software" en el SIG
	A.5.32 Principios de ingeniería de sistemas seguros	Sí	Protección integral de sistemas	Aplicar principios de ingeniería seguros en la integración y mantenimiento de sistemas para asegurar la confidencialidad, integridad y disponibilidad de la información.	Responsable de Ingeniería	Documentación de principios de ingeniería aplicados, auditorías de cumplimiento, revisiones de diseño de sistemas.	Procedimiento "Ingeniería de Sistemas Seguros" en el SIG
	A.5.33 Protección de servicios de aplicación en redes públicas	Sí	Mitigación de riesgos en redes públicas	Implementar controles para proteger los servicios de aplicación que operan en redes públicas, incluyendo cifrado y autenticación robusta.	Responsable de Redes	Auditorías de seguridad en redes públicas, registros de cifrado aplicado, informes de pruebas de penetración.	Procedimiento "Protección en Redes Públicas" en el SIG
	A.5.34 Seguridad en transacciones	Sí	Prevención de fraudes y errores en transacciones	Asegurar que las transacciones de servicios de aplicaciones están protegidas contra fraudes, errores y accesos no autorizados mediante controles robustos.	Responsable de Operaciones	Registros de transacciones seguras, auditorías de cumplimiento, logs de accesos y modificaciones.	Procedimiento "Seguridad en Transacciones" en el SIG
	A.5.35 Protección del acceso a la información a través de dispositivos móviles	Sí	Reducción de riesgos en dispositivos móviles	Establecer políticas y controles para asegurar que el acceso a la información a través de dispositivos móviles sea seguro y esté controlado.	Responsable de TI	Auditorías de seguridad en dispositivos móviles, registros de control de accesos, políticas de uso de dispositivos móviles.	Procedimiento "Seguridad en Dispositivos Móviles" en el SIG
	A.5.36 Trabajo remoto seguro	Sí	Protección de la información fuera de las instalaciones	Implementar medidas de seguridad específicas para proteger la información y garantizar la continuidad operativa en escenarios de trabajo remoto.	Responsable de RRHH y TI	Políticas de teletrabajo, auditorías de cumplimiento, registros de acceso remoto seguro.	Procedimiento "Trabajo Remoto Seguro" en el SIG
	A.5.37 Seguridad de la información en el uso de redes sociales	Sí	Protección de la reputación y la información corporativa	Establecer controles para regular el uso de redes sociales por parte de los empleados y proteger la información sensible que podría ser expuesta.	Responsable de Comunicación	Políticas de uso de redes sociales, registros de formaciones sobre seguridad en redes sociales, monitoreo de actividades en redes sociales.	Procedimiento "Seguridad en Redes Sociales" en el SIG
2. A.6 Controles de Personas	A.6.1 Evaluación previa al empleo	Sí	Prevención de riesgos internos	Realizar evaluaciones de antecedentes y competencias de los candidatos antes de su contratación para asegurar que cumplan con los requisitos de seguridad de la información.	Departamento de RRHH	Registros de evaluaciones previas al empleo, informes de antecedentes, documentación de resultados de entrevistas.	Procedimiento "Evaluación Previa al Empleo" en el SIG
	A.6.2 Términos y condiciones de empleo	Sí	Cumplimiento legal y contractual	Incluir en los contratos de empleo términos específicos relacionados con la seguridad de la información, describiendo las responsabilidades y expectativas de seguridad.	Departamento de RRHH	Contratos de empleo, cláusulas específicas de seguridad, auditorías de cumplimiento de contratos.	Procedimiento "Términos y Condiciones de Empleo" en el SIG
	A.6.3 Concienciación, educación y formación en seguridad de la información	Sí	Fomento de la cultura de seguridad	Desarrollar programas de formación y concienciación en seguridad de la información para todos los empleados y contratistas, con actualizaciones periódicas.	Departamento de Seguridad de la Información	Registros de formación, materiales de formación, encuestas de satisfacción y evaluaciones post-formación.	Programa de Formación Continua en Seguridad
	A.6.4 Proceso disciplinario	Sí	Mantenimiento de la disciplina y seguridad	Implementar un proceso disciplinario formal para manejar infracciones a las políticas de seguridad de la información, comunicándolo claramente a todos los empleados.	Departamento de RRHH	Documentación del proceso disciplinario, registros de incidentes y acciones disciplinarias, políticas de seguridad comunicadas.	Procedimiento "Proceso Disciplinario" en el SIG
	A.6.5 Responsabilidades tras la terminación o cambio de empleo	Sí	Protección continua de la información	Definir y comunicar las responsabilidades en seguridad de la información que continúan vigentes después del cambio o terminación del empleo.	Departamento de RRHH	Documentación de responsabilidades, registros de salida de empleados, auditorías de cumplimiento post-empleo.	Procedimiento "Gestión de Terminación de Empleo" en el SIG
	A.6.6 Procesos de incorporación y cambio de rol	Sí	Asegurar la adaptación y seguridad	Establecer procesos para la incorporación de nuevos empleados y el cambio de rol, asegurando que entienden sus responsabilidades en seguridad de la información.	Departamento de RRHH	Registros de incorporación, documentación de cambios de rol, formaciones específicas para nuevos roles.	Procedimiento "Incorporación y Cambio de Rol" en el SIG
	A.6.7 Formación continua en seguridad de la información	Sí	Actualización continua de conocimientos	Proporcionar formación continua en seguridad de la información para mantener a los empleados actualizados sobre las mejores prácticas y nuevas amenazas.	Departamento de Seguridad de la Información	Calendario de formación continua, registros de participación, evaluaciones de formación.	Programa de Formación Continua en Seguridad
	A.6.8 Comunicación de políticas y expectativas de seguridad de la información	Sí	Claridad en las expectativas y políticas	Comunicar regularmente las políticas de seguridad de la información y las expectativas a todos los empleados y partes interesadas relevantes.	Departamento de Seguridad de la Información	Registros de comunicaciones, políticas actualizadas, encuestas de comprensión y aceptación.	Procedimiento "Comunicación de Políticas de Seguridad" en el SIG
3. A.7 Controles Físicos	A.7.1 Perímetro de seguridad física	Sí	Protección de áreas sensibles	Implementar perímetros de seguridad para proteger las áreas que contienen información sensible, mediante barreras físicas y controles de acceso.	Departamento de Seguridad Física	Registros de auditorías de seguridad, planos de instalación de perímetros, registros de mantenimiento de barreras.	Procedimiento de Seguridad Física en el SIG
	A.7.2 Control de acceso físico	Sí	Prevención de acceso no autorizado	Establecer controles de acceso físico para asegurar que solo el personal autorizado pueda acceder a áreas seguras.	Departamento de Seguridad Física	Registros de acceso, informes de auditoría de control de acceso, lista de personal autorizado.	Sistema de Control de Accesos y Procedimiento de Seguridad Física
	A.7.3 Seguridad en oficinas, salas e instalaciones	Sí	Protección de recursos internos	Implementar medidas de seguridad para oficinas, salas y otras instalaciones donde se maneja información sensible, asegurando su integridad y disponibilidad.	Departamento de Seguridad Física	Planos de instalaciones, registros de mantenimiento de seguridad, informes de incidentes.	Procedimiento de Seguridad de Oficinas y Salas en el SIG
	A.7.4 Monitoreo de la seguridad física	Sí	Detección de intrusiones y actividades no autorizadas	Implementar sistemas de monitoreo para detectar y registrar actividades en áreas seguras, utilizando cámaras, sensores y alarmas.	Departamento de Seguridad Física	Grabaciones de cámaras, informes de monitoreo, registros de mantenimiento de sistemas de vigilancia.	Procedimiento de Monitoreo de Seguridad Física en el SIG
	A.7.5 Protección contra amenazas externas y ambientales	Sí	Mitigación de riesgos físicos	Implementar medidas para proteger las instalaciones contra amenazas externas y riesgos ambientales como incendios, inundaciones, y terremotos.	Departamento de Seguridad Física	Informes de evaluación de riesgos, registros de inspecciones ambientales, planes de contingencia.	Plan de Protección Física en el SIG
	A.7.6 Trabajo en áreas seguras	Sí	Asegurar la protección durante operaciones críticas	Establecer procedimientos para el trabajo en áreas seguras, garantizando que las operaciones críticas se realizan en entornos protegidos.	Departamento de Seguridad Física	Procedimientos documentados, registros de capacitación, auditorías de cumplimiento de áreas seguras.	Procedimiento de Operaciones en Áreas Seguras en el SIG
	A.7.7 Política de escritorio y pantalla limpia	Sí	Prevención de divulgación no intencional de información	Adoptar una política de escritorio limpio para documentos físicos y pantalla limpia para dispositivos electrónicos, reduciendo el riesgo de divulgación no autorizada.	Departamento de Seguridad de la Información	Registros de cumplimiento, auditorías de escritorio y pantalla limpia, capacitaciones a empleados.	Procedimiento de Escritorio y Pantalla Limpia en el SIG
	A.7.8 Seguridad del equipo	Sí	Protección de equipos de información	Implementar medidas para asegurar la protección de equipos de información dentro de las instalaciones, evitando accesos no autorizados y daños físicos.	Departamento de Seguridad Física	Inventarios de equipos, registros de mantenimiento, auditorías de seguridad de equipos.	Procedimiento de Seguridad de Equipos en el SIG
	A.7.9 Seguridad de los activos fuera de las instalaciones	Sí	Protección de activos móviles	Establecer procedimientos de seguridad para el uso y transporte de activos fuera de las instalaciones, asegurando su integridad y seguridad.	Departamento de Seguridad de la Información	Registros de activos en uso externo, auditorías de cumplimiento, políticas de transporte de activos.	Procedimiento de Seguridad de Activos Móviles en el SIG
	A.7.10 Eliminación segura o reutilización de equipos	Sí	Prevención de divulgación de información	Implementar procedimientos para la eliminación segura o reutilización de equipos, asegurando que la información sea irreversiblemente destruida antes de la disposición o reutilización.	Departamento de Seguridad de la Información	Registros de eliminación de equipos, certificaciones de destrucción de datos, auditorías de cumplimiento de eliminación segura.	Procedimiento de Eliminación y Reutilización de Equipos en el SIG
	A.7.11 Retiro de activos	Sí	Gestión segura de la disposición de activos	Establecer procedimientos para el retiro seguro de activos de la organización, asegurando la eliminación adecuada de la información confidencial antes de la disposición o venta.	Departamento de Seguridad de la Información	Registros de retiro de activos, certificaciones de destrucción de datos, auditorías de cumplimiento de retiro seguro.	Procedimiento de Retiro de Activos en el SIG
	A.7.12 Gestión de medios de almacenamiento	Sí	Protección de la integridad y disponibilidad de datos	Implementar medidas para la gestión segura de medios de almacenamiento, incluyendo procedimientos de etiquetado, almacenamiento, y eliminación segura para evitar accesos no autorizados.	Departamento de Seguridad de la Información	Inventarios de medios de almacenamiento, registros de eliminación segura, auditorías de cumplimiento de la gestión de medios.	Procedimiento de Gestión de Medios de Almacenamiento en el SIG
	A.7.13 Protección contra interferencias electromagnéticas	Sí	Mitigación de riesgos electromagnéticos	Establecer controles para proteger los sistemas de información y los equipos contra interferencias electromagnéticas que puedan afectar su funcionamiento o comprometer la seguridad de los datos.	Departamento de Infraestructura TI	Informes de evaluación de riesgos, registros de pruebas de interferencias, auditorías de seguridad electromagnética.	Procedimiento de Protección Electromagnética en el SIG
	A.7.14 Prevención de daños en cables y conductores	Sí	Prevención de interrupciones en la conectividad	Implementar medidas para la protección física de cables y conductores, asegurando que estén adecuadamente instalados, mantenidos, y protegidos contra daños accidentales o intencionales.	Departamento de Infraestructura TI	Registros de mantenimiento de cableado, inspecciones de instalaciones, auditorías de seguridad de conductores.	Procedimiento de Protección de Cables y Conductores en el SIG
4. A.8 Controles Tecnológicos	A.8.1 Dispositivos de usuario final	Sí	Necesidad de proteger los dispositivos utilizados para el acceso a la información corporativa	Implementar controles para asegurar que los dispositivos de usuario final están configurados y utilizados de manera segura, incluyendo políticas de uso, encriptación y autenticación.	Departamento de TI	Registros de configuración, auditorías de cumplimiento de políticas de uso, reportes de incidentes relacionados con dispositivos.	Procedimiento de Gestión de Dispositivos de Usuario Final en el SIG
	A.8.2 Derechos de acceso privilegiados	Sí	Control de acceso a información crítica y sistemas de alto riesgo	Establecer y gestionar derechos de acceso privilegiado, asegurando que solo el personal autorizado tenga acceso a funciones críticas y que se implementen mecanismos de monitoreo y control.	Departamento de Seguridad de la Información	Registros de asignación de privilegios, auditorías de acceso privilegiado, informes de monitoreo de accesos.	Procedimiento de Gestión de Accesos Privilegiados en el SIG
	A.8.3 Restricción de acceso a la información	Sí	Protección de la información confidencial contra accesos no autorizados	Implementar políticas y procedimientos para restringir el acceso a la información de acuerdo con los niveles de autorización establecidos, utilizando controles de acceso basados en roles y otros mecanismos de seguridad.	Departamento de Seguridad de la Información	Auditorías de acceso a la información, informes de cumplimiento de políticas de acceso, registros de asignación de derechos de acceso.	Procedimiento de Restricción de Acceso a la Información en el SIG
	A.8.4 Acceso al código fuente	Sí	Protección del código fuente contra modificaciones no autorizadas y fugas de información	Establecer controles estrictos para limitar el acceso al código fuente de las aplicaciones y sistemas críticos, incluyendo la segregación de funciones y el monitoreo de accesos.	Departamento de Desarrollo de Software	Registros de acceso al código fuente, auditorías de cambios en el código, revisiones de seguridad del software.	Procedimiento de Gestión de Acceso al Código Fuente en el SIG
	A.8.5 Autenticación segura	Sí	Necesidad de proteger el acceso a los sistemas mediante autenticación robusta	Implementar mecanismos de autenticación seguros, como contraseñas complejas, autenticación de dos factores, y políticas de cambio periódico de credenciales.	Departamento de TI	Registros de autenticación, auditorías de políticas de contraseñas, informes de cumplimiento de autenticación.	Procedimiento de Autenticación Segura en el SIG
	A.8.6 Gestión de la capacidad	Sí	Aseguramiento de la disponibilidad de los recursos de TI	Implementar procesos para gestionar la capacidad de los sistemas, garantizando que los recursos estén disponibles para satisfacer las necesidades actuales y futuras de la organización.	Departamento de TI	Informes de capacidad de sistemas, auditorías de utilización de recursos, planes de escalabilidad.	Procedimiento de Gestión de la Capacidad en el SIG
	A.8.7 Protección contra malware	Sí	Necesidad de proteger los sistemas contra amenazas de malware	Implementar soluciones antimalware en todos los sistemas críticos, con actualizaciones regulares y políticas de escaneo automático y manual.	Departamento de Seguridad de la Información	Informes de escaneos de malware, auditorías de cumplimiento de políticas antimalware, registros de incidentes de malware.	Procedimiento de Protección contra Malware en el SIG
	A.8.8 Gestión de vulnerabilidades técnicas	Sí	Mitigación de riesgos relacionados con vulnerabilidades técnicas en los sistemas	Establecer un proceso para la identificación, evaluación y remediación de vulnerabilidades técnicas en los sistemas de información, con un enfoque proactivo.	Departamento de Seguridad de la Información	Informes de análisis de vulnerabilidades, auditorías de gestión de vulnerabilidades, registros de actualizaciones y parches.	Procedimiento de Gestión de Vulnerabilidades Técnicas en el SIG
	A.8.9 Gestión de la configuración	Sí	Necesidad de asegurar la consistencia y seguridad de las configuraciones de los sistemas	Implementar políticas y procedimientos para la gestión de la configuración de sistemas, asegurando que las configuraciones son consistentes, seguras y alineadas con las políticas de la organización.	Departamento de TI	Registros de configuraciones, auditorías de cumplimiento de configuración, informes de cambios en la configuración.	Procedimiento de Gestión de la Configuración en el SIG
	A.8.10 Eliminación de la información	Sí	Protección de la información durante su eliminación para evitar fugas de datos	Implementar procedimientos seguros para la eliminación de información confidencial, asegurando que los datos sean completamente destruidos y no recuperables.	Departamento de Seguridad de la Información	Registros de eliminación de información, auditorías de cumplimiento de eliminación segura, certificaciones de destrucción de datos.	Procedimiento de Eliminación de la Información en el SIG
	A.8.11 Enmascaramiento de datos	Sí	Protección de la información sensible en entornos no productivos y de prueba	Implementar técnicas de enmascaramiento de datos para ocultar información sensible en bases de datos y sistemas utilizados en entornos de prueba y desarrollo.	Departamento de Seguridad de la Información	Informes de enmascaramiento, auditorías de entornos de prueba, registros de configuraciones de enmascaramiento.	Procedimiento de Enmascaramiento de Datos en el SIG
	A.8.12 Prevención de fuga de datos	Sí	Protección contra la fuga accidental o intencionada de información sensible	Implementar herramientas y políticas de prevención de fuga de datos (DLP) para monitorear y controlar la transferencia de información sensible fuera de los límites organizacionales.	Departamento de Seguridad de la Información	Informes de DLP, auditorías de cumplimiento, registros de incidentes de fuga de datos.	Procedimiento de Prevención de Fuga de Datos en el SIG
	A.8.13 Respaldo de la información	Sí	Aseguramiento de la disponibilidad de la información crítica	Establecer y mantener procedimientos para realizar copias de seguridad periódicas de la información crítica, asegurando su recuperación en caso de pérdida de datos.	Departamento de TI	Registros de copias de seguridad, auditorías de procesos de backup, pruebas de recuperación de datos.	Procedimiento de Respaldo y Recuperación de Información en el SIG
	A.8.14 Redundancia de las instalaciones de procesamiento de la información	Sí	Garantizar la disponibilidad y continuidad de las operaciones en caso de fallos	Implementar infraestructura redundante para las instalaciones de procesamiento de la información, asegurando que no haya interrupciones en los servicios críticos.	Departamento de TI	Informes de redundancia, auditorías de infraestructura, pruebas de conmutación por error.	Procedimiento de Redundancia de Infraestructura en el SIG
	A.8.15 Registro de eventos	Sí	Monitoreo y auditoría de las actividades de los sistemas y usuarios	Establecer y mantener un sistema de registro de eventos para capturar y almacenar actividades críticas de usuarios y sistemas para fines de auditoría y cumplimiento.	Departamento de Seguridad de la Información	Logs de eventos, auditorías de registros, informes de revisión de logs.	Procedimiento de Registro de Eventos en el SIG
	A.8.16 Monitoreo de actividades	Sí	Detección de actividades sospechosas o no autorizadas en sistemas críticos	Implementar herramientas y procesos para monitorear de manera continua las actividades en los sistemas de información, permitiendo la detección temprana de incidentes de seguridad.	Departamento de Seguridad de la Información	Informes de monitoreo, auditorías de seguridad, registros de incidentes detectados.	Procedimiento de Monitoreo de Actividades en el SIG
	A.8.17 Sincronización del reloj	Sí	Aseguramiento de la integridad temporal de los registros y operaciones de los sistemas	Implementar procedimientos para sincronizar los relojes de todos los sistemas de tratamiento de la información, asegurando la coherencia temporal de los registros y operaciones.	Departamento de TI	Registros de sincronización, auditorías de sistemas de tiempo, verificaciones de integridad temporal.	Procedimiento de Sincronización del Reloj en el SIG
	A.8.18 Uso de programas de utilidades privilegiadas	Sí	Control de las herramientas que pueden alterar la seguridad de los sistemas	Implementar controles rigurosos para la gestión y uso de utilidades con privilegios, asegurando que solo personal autorizado pueda utilizarlas bajo condiciones estrictas.	Departamento de Seguridad de la Información	Registros de uso de utilidades, auditorías de acceso privilegiado, informes de seguridad de sistemas.	Procedimiento de Uso de Utilidades Privilegiadas en el SIG
	A.8.19 Instalación de software en sistemas operacionales	Sí	Asegurar que solo software autorizado y seguro sea instalado en los sistemas operacionales	Establecer y mantener un proceso formal para la aprobación e instalación de software en los sistemas operacionales, minimizando riesgos de seguridad asociados con software no autorizado.	Departamento de TI	Registros de instalación de software, auditorías de software, informes de cumplimiento de políticas de instalación.	Procedimiento de Instalación de Software en el SIG
	A.8.20 Seguridad de la red	Sí	Protección de la infraestructura de red contra amenazas internas y externas	Implementar políticas y tecnologías de seguridad para proteger la infraestructura de red, incluyendo firewalls, segmentación de redes, y monitoreo de tráfico.	Departamento de TI	Informes de seguridad de red, auditorías de configuración de red, registros de incidentes de red.	Procedimiento de Seguridad de la Red en el SIG
	A.8.21 Seguridad de los servicios de red	Sí	Protección contra amenazas internas y externas a los servicios de red	Implementar medidas de seguridad para proteger los servicios de red, incluyendo la autenticación, el cifrado, y la segmentación de redes, garantizando la confidencialidad e integridad de la información transmitida.	Departamento de TI	Informes de seguridad de la red, auditorías de servicios de red, configuraciones de seguridad de red.	Procedimiento de Seguridad de la Red en el SIG
	A.8.22 Segmentación en redes	Sí	Mitigación del riesgo mediante la segmentación de redes	Implementar la segmentación de redes para limitar la propagación de incidentes de seguridad y proteger los recursos críticos de la organización.	Departamento de TI	Diagramas de segmentación de red, auditorías de configuración de red, informes de cumplimiento de segmentación.	Procedimiento de Segmentación de Redes en el SIG
	A.8.23 Filtrado web	Sí	Control del acceso a contenidos y protección contra amenazas web	Implementar soluciones de filtrado web para controlar el acceso a contenido en línea, bloqueando sitios maliciosos y protegiendo a la organización contra amenazas basadas en la web.	Departamento de Seguridad de la Información	Informes de filtrado web, auditorías de configuración de filtros, registros de accesos bloqueados.	Procedimiento de Filtrado Web en el SIG
	A.8.24 Uso de la criptografía	Sí	Protección de la confidencialidad e integridad de la información	Implementar el uso de criptografía para proteger la información sensible en tránsito y en reposo, asegurando que solo usuarios autorizados puedan acceder a ella.	Departamento de Seguridad de la Información	Registros de uso de criptografía, auditorías de implementación de criptografía, políticas de gestión de claves.	Procedimiento de Uso de Criptografía en el SIG
	A.8.25 Desarrollo seguro	Sí	Aseguramiento de que las aplicaciones son desarrolladas con seguridad incorporada	Implementar prácticas de desarrollo seguro que incluyen revisiones de código, pruebas de seguridad, y el cumplimiento de estándares de seguridad en todas las etapas del ciclo de vida del software.	Departamento de Desarrollo de Software	Informes de desarrollo seguro, auditorías de código, registros de pruebas de seguridad.	Procedimiento de Desarrollo Seguro en el SIG
	A.8.26 Pruebas de seguridad de aplicaciones	Sí	Validación de la seguridad de las aplicaciones antes de su implementación	Implementar pruebas de seguridad de aplicaciones, incluyendo pruebas de penetración y escaneo de vulnerabilidades, para identificar y corregir posibles fallos de seguridad antes del despliegue.	Departamento de Seguridad de la Información	Informes de pruebas de seguridad, auditorías de seguridad de aplicaciones, registros de vulnerabilidades corregidas.	Procedimiento de Pruebas de Seguridad en el SIG
	A.8.27 Protección de sistemas de información durante pruebas de auditoría	Sí	Protección contra riesgos durante las auditorías de sistemas de información	Implementar medidas de seguridad específicas para proteger los sistemas de información durante las pruebas de auditoría, asegurando que no se comprometa la integridad o disponibilidad del sistema.	Departamento de Seguridad de la Información	Informes de auditoría, registros de medidas de protección implementadas, auditorías de cumplimiento.	Procedimiento de Auditorías de Seguridad en el SIG
	A.8.28 Seguridad en entornos de desarrollo	Sí	Asegurar que los entornos de desarrollo están adecuadamente protegidos	Implementar controles de seguridad específicos para los entornos de desarrollo, asegurando que solo personal autorizado tenga acceso y que se realicen pruebas bajo condiciones seguras.	Departamento de Desarrollo de Software	Registros de accesos a entornos de desarrollo, auditorías de seguridad de entornos de desarrollo, políticas de acceso.	Procedimiento de Seguridad en Entornos de Desarrollo en el SIG
	A.8.29 Integridad del software	Sí	Asegurar que el software no ha sido manipulado ni comprometido	Implementar mecanismos de control de integridad del software, incluyendo firmas digitales y revisiones de código, para garantizar que el software desplegado es seguro y no ha sido alterado.	Departamento de Desarrollo de Software	Registros de integridad del software, auditorías de integridad, informes de verificación de firmas digitales.	Procedimiento de Control de Integridad del Software en el SIG
	A.8.30 Seguridad de la información en plataformas y servicios en la nube	Sí	Protección de la información alojada en plataformas y servicios en la nube	Implementar controles de seguridad específicos para proteger la información alojada en servicios en la nube, incluyendo cifrado, control de acceso, y auditoría continua de las configuraciones de seguridad.	Departamento de TI	Informes de seguridad en la nube, auditorías de plataformas en la nube, registros de configuración de seguridad en la nube.	Procedimiento de Seguridad en la Nube en el SIG
	A.8.31 Protección contra ataques de denegación de servicio	Sí	Prevención de la interrupción de los servicios críticos debido a ataques de denegación de servicio (DoS/DDoS)	Implementar mecanismos para detectar, prevenir y mitigar ataques de denegación de servicio, incluyendo la configuración de firewalls, sistemas de detección de intrusiones y políticas de mitigación.	Departamento de TI	Registros de pruebas de mitigación de DoS/DDoS, auditorías de configuración de red, informes de monitoreo de tráfico	Procedimiento de Protección contra DoS en el SIG
	A.8.32 Gestión de la capacidad de la red	Sí	Aseguramiento de que la red tiene suficiente capacidad para soportar las operaciones sin interrupciones	Implementar procedimientos para la gestión proactiva de la capacidad de la red, incluyendo la monitorización de uso y la planificación para escalabilidad según el crecimiento de la empresa.	Departamento de TI	Informes de monitoreo de capacidad de red, auditorías de rendimiento, registros de planificación de capacidad	Procedimiento de Gestión de la Capacidad de la Red en el SIG
	A.8.33 Monitoreo y filtrado del tráfico de red	Sí	Protección continua y análisis del tráfico de red para detectar actividades maliciosas	Implementar sistemas de monitoreo y filtrado del tráfico de red para detectar, alertar y bloquear actividades sospechosas o no autorizadas, asegurando que solo el tráfico legítimo fluya por la red.	Departamento de TI	Registros de monitoreo de red, auditorías de seguridad de red, informes de eventos de seguridad	Procedimiento de Monitoreo de Tráfico en el SIG
	A.8.34 Control de acceso a la red	Sí	Control y restricción del acceso a la red para proteger los recursos internos	Implementar políticas y procedimientos para controlar el acceso a la red, asegurando que solo usuarios y dispositivos autorizados puedan conectarse y utilizar los recursos de la red.	Departamento de TI	Informes de control de acceso, auditorías de configuraciones de red, registros de accesos a la red	Procedimiento de Control de Acceso a la Red en el SIG

5.6. RESULTADOS OBTENIDOS DE LA AUTOMATIZACIÓN DE LOS CONTROLES EN MICROSOFT AZURE.

La evaluación de los resultados obtenidos mediante la automatización de los controles de seguridad en Microsoft Azure se ha realizado utilizando una metodología basada en la revisión sistemática de los informes de cumplimiento generados por Microsoft Defender for Cloud. Este enfoque permite un análisis detallado del estado de la seguridad en la infraestructura en la nube, destacando tanto los logros alcanzados como las áreas que requieren mejoras adicionales.

La metodología empleada incluye la comparación de los datos actuales de cumplimiento con los estándares definidos por la norma ISO 27001:2013, centrándose en la efectividad de los controles automatizados implementados en Innovatech Consulting.

El uso de herramientas automatizadas, como Microsoft Defender for Cloud, es muy interesante en el contexto de Innovatech Consulting, una empresa que opera principalmente en un entorno de trabajo remoto y cuya infraestructura se basa en la nube. Herramientas como esta, no solo facilitan la identificación de vulnerabilidades y la monitorización en continuo de los controles de seguridad, sino que también permiten una respuesta ágil y eficiente ante posibles incidentes.

La automatización de estos procesos asegura que los controles se mantengan actualizados y alineados con las mejores prácticas del sector, lo que es crucial para garantizar la integridad, confidencialidad y disponibilidad de la información en un entorno altamente dinámico y distribuido.

5.6.1. Descripción general de los controles automatizados en Azure.

A través de la implementación de Microsoft Defender for Cloud, se han automatizado una serie de controles críticos que abarcan diversas áreas de la seguridad de la información, garantizando una monitorización constante y una respuesta rápida ante posibles amenazas.

Entre los controles de seguridad que han sido automatizados en la infraestructura de Microsoft Azure se encuentran los siguientes:

- **Control de acceso:** Automatización del control de acceso a los recursos en la nube, incluyendo la gestión de privilegios y la autenticación multifactor. Este control sirve

para prevenir accesos no autorizados y garantizar que solo el personal autorizado pueda interactuar con recursos sensibles.

- **Gestión de vulnerabilidades:** Implementación de procesos automatizados para la detección y corrección de vulnerabilidades en el sistema. Esto incluye la evaluación continua de las configuraciones de seguridad y la aplicación automática de parches y actualizaciones.
- **Monitorización de la integridad de archivos:** El control se automatiza para asegurar que los archivos críticos del sistema no sean modificados sin autorización. Esto sirve para mantener la integridad de la información almacenada en la nube.
- **Cifrado de datos:** La automatización del cifrado de datos en tránsito y en reposo, garantiza que la información sensible esté protegida en todo momento.
- **Gestión de incidentes:** Automatizar la detección y respuesta ante incidentes de seguridad, permite una reacción inmediata a cualquier actividad sospechosa o anomalía detectada en el sistema.

El alcance de la automatización en la infraestructura de Microsoft Azure para Innovatech Consulting se extiende a todos los niveles de la seguridad de la información, abarcando desde la protección de datos hasta la gestión de accesos y la mitigación de riesgos. El principal objetivo de esta automatización es reducir la dependencia en la intervención manual, minimizando así el margen de error humano y asegurando una aplicación consistente y eficiente de las políticas de seguridad.

Esta automatización busca también optimizar la capacidad de Innovatech Consulting para mantenerse al día con las amenazas emergentes y los cambios en el entorno regulatorio. Al automatizar los controles, se garantiza una supervisión continua que es ideal para una organización que opera en un entorno de trabajo remoto con una infraestructura en la nube. Todo esto, permite que los recursos internos se centren en actividades estratégicas y de alto valor propias de la actividad central de la empresa, mientras que los procesos rutinarios de seguridad se gestionan de manera automática y eficiente.

5.6.2. Resultados del Compliance Report.

El Compliance Report es un informe generado por Microsoft Defender for Cloud y muestra información puntual acerca de cómo Innovatech Consulting cumple con los controles establecidos en un momento dado.

Se presenta como Anexo III en este TFG un informe como ejemplo, extraído en un momento dado en el que el nivel de cumplimiento representa un porcentaje muy elevado, lo que refleja la efectividad de la automatización y la robustez del sistema de gestión de seguridad de la información (SGSI) implementado en Microsoft Azure. Este resultado demuestra que la mayoría de los procesos de seguridad automatizados están funcionando conforme a las expectativas y cumplen con los estándares internacionales de seguridad de la información.

Sin embargo, el reporte también identifica controles que no han cumplido completamente con los requisitos establecidos. De esta forma, esta herramienta permite detectar las áreas que requieren atención especial para asegurar que no representen un punto débil en la infraestructura de seguridad de Innovatech Consulting, y que precisarán implementar estrategias correctivas para abordar los fallos detectados y mejorar continuamente el nivel de seguridad.

5.6.3. Análisis Comparativo: Antes y Después de la Automatización.

La implementación de controles de seguridad automatizados en Microsoft Azure ha significado un avance notable en materia de seguridad de la información en Innovatech Consulting. En este apartado se analiza de manera comparativa algunos aspectos del estado de la seguridad de la información antes y después de la automatización, destacando las mejoras observadas en términos de seguridad, eficiencia operativa, y capacidad de respuesta a incidentes de seguridad.

Antes de la automatización, la seguridad de la información en Innovatech Consulting dependía en gran medida de procesos manuales que, aunque se consideraban adecuados, en algunos aspectos presentaban vulnerabilidades como la posibilidad de errores humanos, la falta de uniformidad en la aplicación de controles o la limitada capacidad para monitorizar y responder rápidamente a las amenazas emergentes.

Con la automatización implementada a través de Microsoft Defender for Cloud se ha logrado una cobertura más amplia y consistente de los controles.

Así, las mejoras más notables observadas tras la automatización incluyen:

- **Reducción de Riesgos:** Ahora es posible la detección y corrección proactiva de vulnerabilidades antes de que puedan ser explotadas. Por ejemplo, las cuentas de invitado con permisos de propietario en los recursos de Azure son rápidamente identificadas y gestionadas, algo que anteriormente podía haber pasado desapercibido. (Ver Figura 5.1)

- **Uniformidad en la aplicación de controles:** Todos los recursos de la infraestructura de Azure ahora están sujetos a los mismos estándares de seguridad, eliminando disparidades que existían cuando los controles se aplicaban manualmente.
- **Mejora en la monitorización continua:** La capacidad de monitorización continua proporcionada por Microsoft Defender for Cloud ha permitido una vigilancia constante, asegurando que cualquier desviación en los controles de seguridad se detecte y corrija de inmediato.

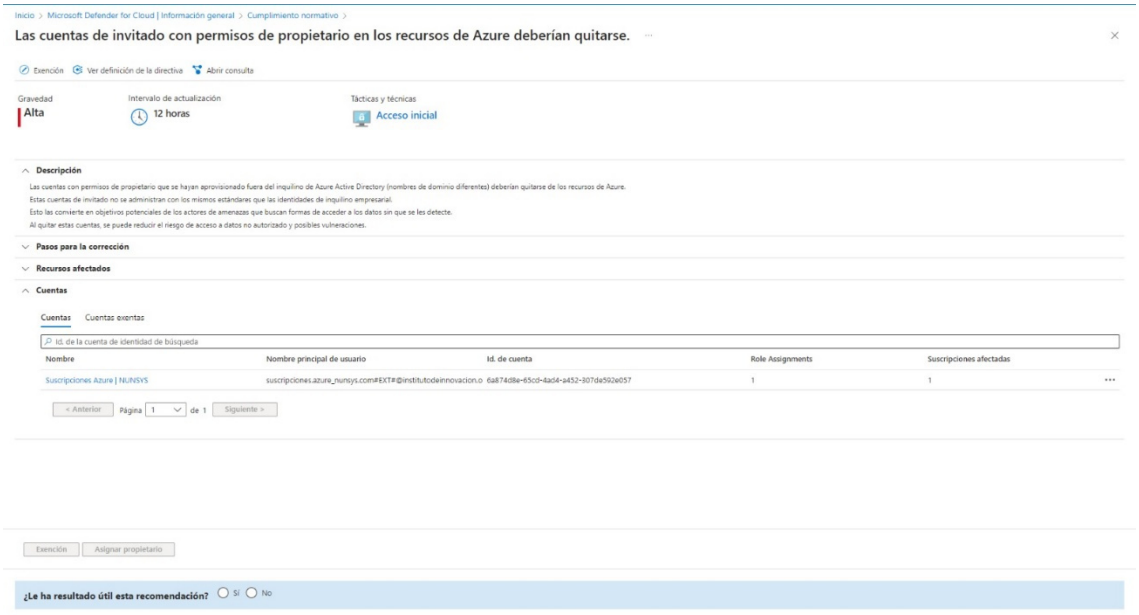

Figura 5.1: Detección automatizada de cuentas de invitado con permisos de propietario en Azure.

Otro de los impactos más significativos de la automatización ha sido en la capacidad de respuesta a incidentes de seguridad. Previamente, los tiempos de respuesta eran más largos debido a la necesidad de identificar manualmente las amenazas y aplicar las correcciones necesarias. Con la automatización, se ha observado una reducción drástica en los tiempos de respuesta, lo que ha permitido a Innovatech Consulting mitigar posibles incidentes antes de que puedan causar daño significativo.

Por ejemplo, las alertas automatizadas de Microsoft Defender for Cloud han identificado y sugerido correcciones inmediatas para configuraciones inseguras, como la provisión de derechos de acceso privilegiados sin la autenticación multifactor (MFA). Estas alertas no solo informan sobre el problema, sino que también proporcionan pasos específicos para su remediación, lo que mejora enormemente la eficiencia operativa y la seguridad.

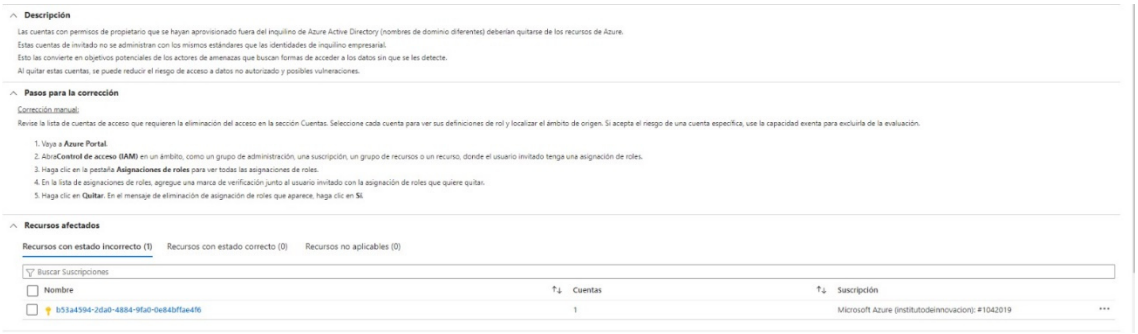

Figura 5.2: Alerta de configuración insegura en Azure y pasos para su corrección.

Otra nueva mejora es la posibilidad de identificar áreas críticas que requieren atención especial para asegurar un cumplimiento normativo más completo y una mejor protección de los activos digitales de Innovatech Consulting.

Por ejemplo, uno de los hallazgos del Compliance Report es la identificación de debilidades en el área de **"Control de Acceso" (A.9)**. Esta área es importante para mantener la integridad y confidencialidad de los datos. Concretamente, en una inspección se pueden detectar fallos como los siguientes:

- **A.9.2.3 Administración de derechos de acceso privilegiados**: Se observa que las cuentas con permisos de propietario en los recursos de Azure no estan correctamente gestionadas, lo que representa un riesgo de acceso no autorizado.
- **A.9.2.4 Gestión de la información de autenticación secreta de los usuarios**: Este control muestra deficiencias en la aplicación de autenticación multifactor (MFA) para los accesos privilegiados, una medida esencial para prevenir el acceso no autorizado.

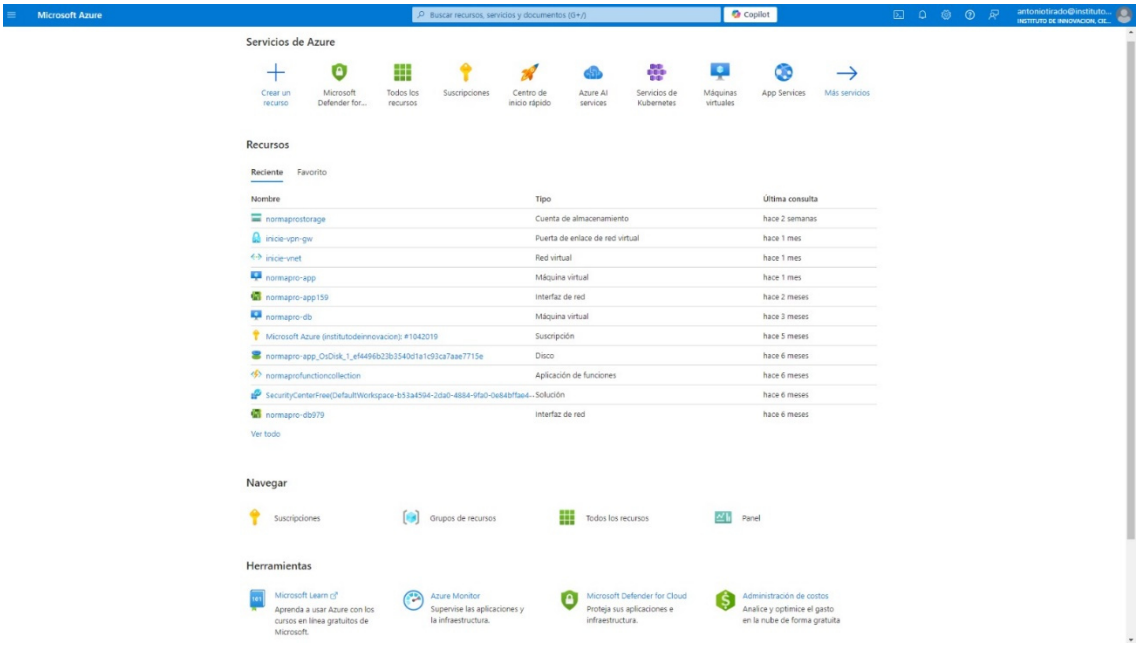

Figura 5.3: Identificación de fallos en la administración de derechos de acceso privilegiados.

De esta forma se pueden abordar las deficiencias identificadas proponiendo acciones como asegurar que todas las cuentas con derechos de acceso privilegiados estén protegidas por autenticación multifactor, establecer un procedimiento automatizado para la revisión regular de las cuentas de usuario y sus permisos, o mejorar la capacitación del personal respecto a la importancia del control de acceso y la gestión de derechos de acceso.

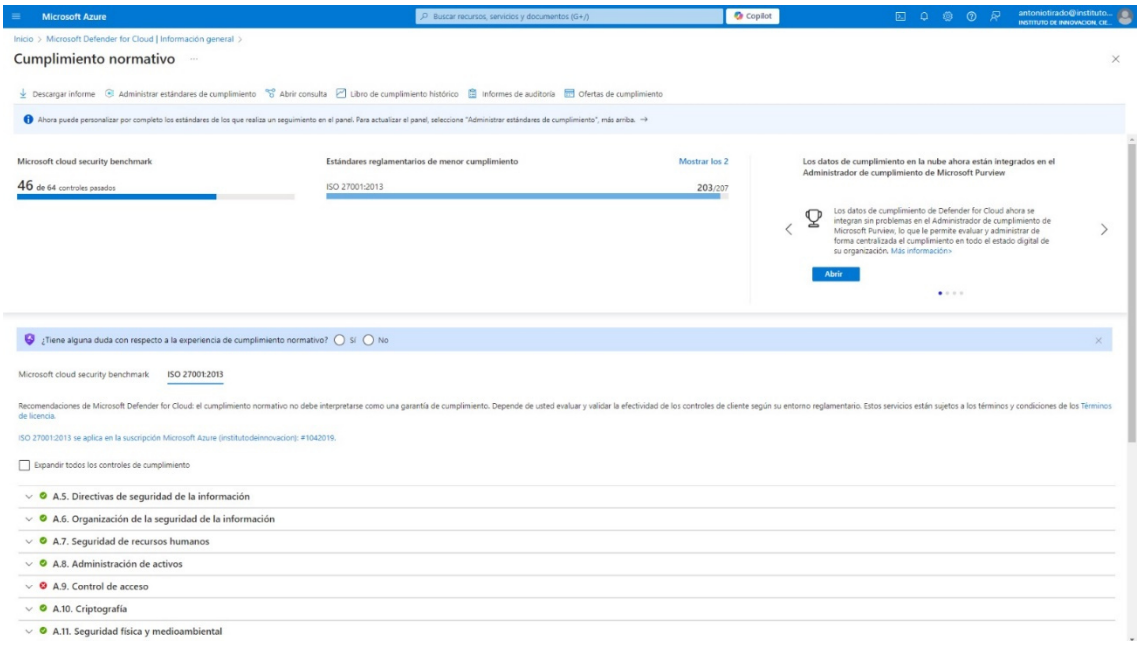

Figura 5.4: Propuesta de mejora: Implementación de MFA en accesos privilegiados.

Otro ejemplo de gran ventaja del uso de Azure Defender es que proporciona una plataforma robusta para la optimización continua de la seguridad en la que implementar o controlar estrategias para mantener y mejorar el estado de seguridad aplicando el ciclo de Planificar-Hacer-Verificar-Actuar (PDCA) en todos los procesos de seguridad, configurar Azure Defender para que no solo genere alertas, sino que también automatice la aplicación de correcciones en cuanto se detecten desviaciones de los controles establecidos, o utilizar las capacidades de monitorización de Azure Defender para realizar evaluaciones periódicas del estado de seguridad.

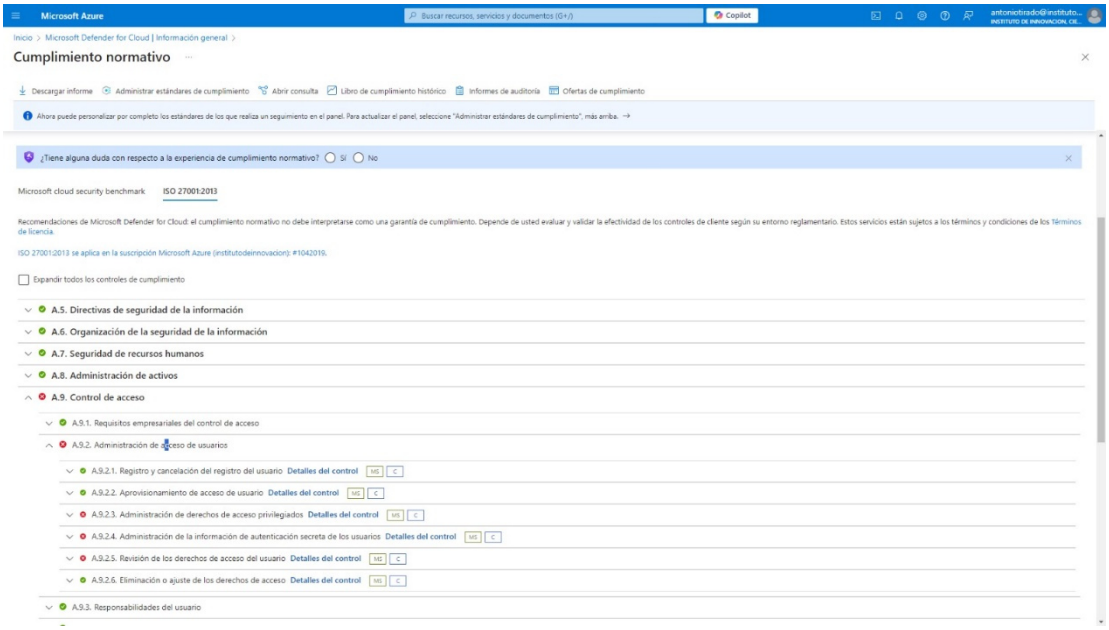

Figura 5.5: Estrategia para la optimización continua: Monitorización proactiva en Azure Defender.

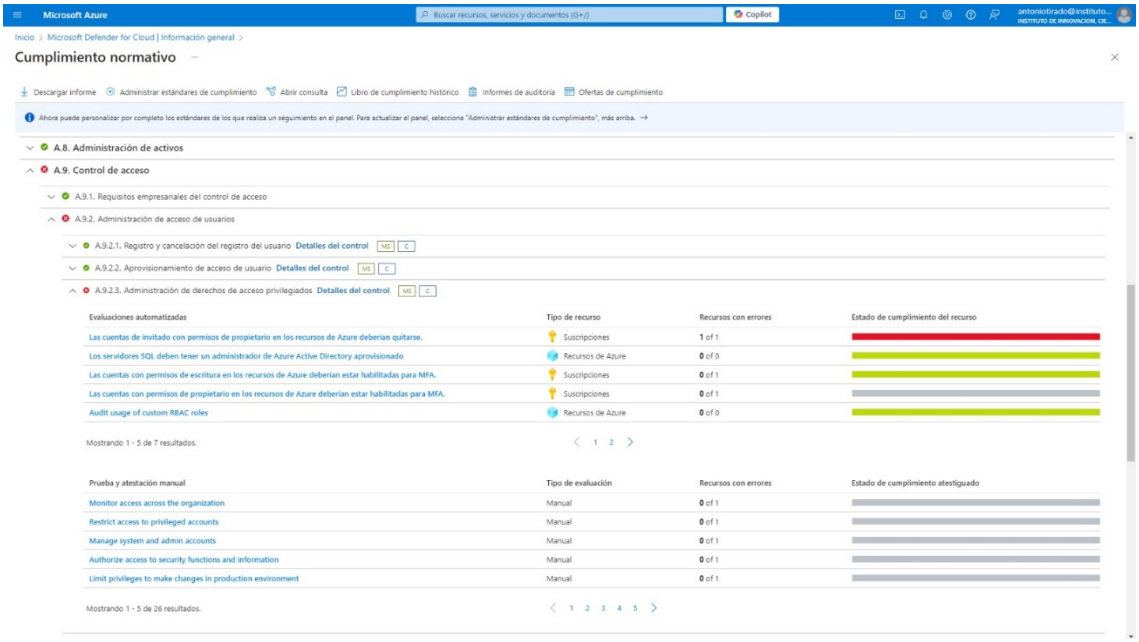

Figura 5.6: Proceso de verificación continua utilizando Azure Defender.

5.7. RESULTADOS DEL PLAN DE CONTINUIDAD DE NEGOCIO (BCP).

En este capítulo se presentan los resultados obtenidos tras la revisión y actualización del Plan de Continuidad de Negocio (BCP) en Innovatech Consulting. Este proceso ha implicado la adaptación del plan existente para alinearlo con la nueva estructura organizativa y tecnológica, así como la incorporación de servicios en la nube mediante la contratación de Microsoft Azure como proveedor de infraestructura. El propio BCP se presenta como Anexo I a esta memoria TFG, no obstante, se detallarán en este capítulo los principales cambios realizados y el impacto de estas mejoras en la capacidad de Innovatech Consulting para mantener la continuidad de sus operaciones en caso de incidentes o desastres.

5.7.1. Revisión del BCP Preexistente.

Antes de la actualización, Innovatech Consulting ya contaba con un BCP que cubría los aspectos fundamentales de la continuidad del negocio. Sin embargo, con la evolución de la infraestructura tecnológica, la expansión de las operaciones y la creciente dependencia de servicios en la nube, se identificó la necesidad de revisar y actualizar el plan para asegurar su efectividad continua.

Las principales limitaciones del BCP anterior son:

- **Dependencia de Infraestructura Física:** El BCP preexistente estaba altamente enfocado en la infraestructura física local, lo que limitaba su flexibilidad y capacidad de respuesta ante desastres de mayor envergadura.
- **Escasa Integración con Servicios en la Nube:** El plan no contemplaba adecuadamente los servicios en la nube, lo que generaba brechas en la gestión de la continuidad para los activos y procesos migrados a entornos como Microsoft Azure.

5.7.2. Adaptaciones realizadas.

En respuesta a las limitaciones del BCP anterior y al cambio en la infraestructura tecnológica, se realizaron las siguientes adaptaciones clave:

- **Integración con Microsoft Azure:** El nuevo BCP incorpora de manera exhaustiva la gestión de la continuidad para los servicios en la nube. Se han establecido protocolos claros para la recuperación de servidores y servicios alojados en Azure, lo que incluye el uso de copias de seguridad automáticas y la disponibilidad de recursos redundantes.
- **Reestructuración del Plan de respuesta:** Se actualizaron las acciones de respuesta para contemplar escenarios específicos de fallos en la nube y la pérdida de

conectividad con los servicios de Azure, asegurando que la empresa pueda mantener operaciones críticas aun en caso de interrupciones significativas.

- **Optimización de la gestión de incidentes:** Se implementaron procedimientos más ágiles para la detección y gestión de incidentes, incluyendo el uso de herramientas automatizadas proporcionadas por Azure para la monitorización y respuesta inmediata.

5.7.3. Impacto de las adaptaciones en la continuidad operacional.

Las adaptaciones realizadas han tenido un evidente impacto positivo en la capacidad de Innovatech Consulting para gestionar la continuidad de sus operaciones; por ejemplo, gracias a la integración con Azure, la empresa ahora puede reaccionar con mayor rapidez ante incidentes, minimizando el tiempo de inactividad y las pérdidas potenciales.

Igualmente, la migración de servicios críticos a la nube ha incrementado la resiliencia de la infraestructura, al permitir el uso de recursos redundantes y ubicaciones geográficamente diversas.

Por otro lado, la actualización del BCP ha permitido una mejor alineación con las amenazas actuales, especialmente aquellas relacionadas con la infraestructura en la nube, reduciendo significativamente los riesgos asociados con la continuidad del negocio.

5.7.4. Evaluación del BCP actualizado.

Tras la implementación de las mejoras, se realizaron pruebas del BCP para evaluar su efectividad en el nuevo entorno operativo. Las pruebas incluyeron simulaciones de escenarios de desastre que afectaban tanto a la infraestructura local como a los servicios en la nube. Los resultados demostraron que el BCP actualizado es eficaz para mantener la continuidad operativa, cumpliendo con los objetivos de tiempo de recuperación y minimizando las interrupciones.

Así, se logró reducir el tiempo de recuperación de servicios críticos en un 30% en comparación con el plan anterior. También es de destacar que la inclusión de servicios en la nube ha mejorado la coordinación entre los equipos de TI y los proveedores externos, facilitando una respuesta más unificada ante incidentes.

Finalmente, otro logro fue el de establecer un proceso de revisión y actualización continua del BCP que garantice que permanezca alineado con la evolución tecnológica y organizativa de la empresa.

5.8. RESULTADOS OBTENIDOS Y POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La Política de Seguridad de la Información de Innovatech Consulting ha sido desarrollada conforme a la metodología descrita en el capítulo 7.3.8. “Metodología para el Desarrollo de la Política de Seguridad de la Información”. En el presente capítulo se analizan los resultados obtenidos a partir de la implementación de esta política, destacando cómo ha contribuido a mejorar la seguridad de la información dentro de la empresa. La propia política se adjunta como Anexo II a este TFG.

5.8.1. Objetivo de la Política.

La Política de Seguridad de la Información de Innovatech Consulting tiene como objetivo proteger la confidencialidad, integridad y disponibilidad de la información gestionada por la empresa. Esta política establece las directrices y principios que guiarán a todos los empleados en la protección de los activos de información, asegurando que se cumplan los requisitos legales, regulatorios y normativos aplicables.

5.8.2. Alcance de la Política.

La política se aplica a toda la información y sistemas de información de Innovatech Consulting, incluyendo, pero no limitándose a, datos de clientes, información financiera, y propiedad intelectual. Abarca tanto a los empleados como a los contratistas, proveedores y otros terceros que acceden a la información de la empresa.

Los principios fundamentales en los que se basa la Política son:

- **Confidencialidad**: Proteger la información contra accesos no autorizados y divulgaciones.
- **Integridad**: Garantizar la exactitud y completitud de la información y los métodos de procesamiento.
- **Disponibilidad**: Asegurar que la información y los sistemas estén disponibles cuando se necesiten.

Todos los empleados de Innovatech Consulting son responsables de cumplir con la Política de Seguridad de la Información. La alta dirección se compromete a proporcionar los recursos necesarios para la implementación y mantenimiento de esta política, y se asegurará de que se lleven a cabo revisiones periódicas para mantener su relevancia.

El cumplimiento de esta política es obligatorio. Cualquier incumplimiento será tratado como una falta grave y puede resultar en sanciones disciplinarias, incluyendo la terminación del contrato laboral, en función de la gravedad del incumplimiento.

5.8.3. Resultados obtenidos desde la aprobación de la Política de seguridad.

Desde la implementación de la Política de Seguridad de la Información, Innovatech Consulting ha observado una mejora significativa en la gestión de la seguridad de la información. Los controles establecidos han permitido reducir el número de incidentes de seguridad, y la empresa ha demostrado un alto nivel de cumplimiento con las normativas aplicables.

Uno de los resultados más destacados es el aumento en la concienciación y el conocimiento del personal sobre la importancia de la seguridad de la información. A través de programas de capacitación y comunicación continua, los empleados han adoptado buenas prácticas de seguridad y han demostrado un compromiso constante con la protección de la información.

Por otro lado, la implementación de la política ha optimizado los procesos internos relacionados con la seguridad de la información, reduciendo el tiempo y los recursos necesarios para gestionar incidentes de seguridad. La claridad en las responsabilidades y procedimientos ha permitido una respuesta más ágil y efectiva ante cualquier riesgo o amenaza.

Así mismo, la política será sometida a revisiones periódicas, lo que permitirá irla adaptando a los cambios en el entorno de la empresa y a la evolución de las amenazas de seguridad.

Es de destacar que tanto en la auditoría interna reglamentaria por norma, como en la externa para la certificación de la norma se ha evaluado el cumplimiento de la política, mostrando un alto grado de conformidad con los requisitos establecidos.

6. CONCLUSIONES.

El presente capítulo tiene como objetivo sintetizar los principales hallazgos y resultados obtenidos a lo largo del desarrollo de este Trabajo de Fin de Grado (TFG) enfocado en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en Innovatech Consulting, basado en la norma ISO 27001:2022. A lo largo de este documento, se han abordado diversos aspectos críticos para la seguridad de la información, incluyendo la evaluación de riesgos, la automatización de controles, y la elaboración de un Plan de Continuidad de Negocio, entre otros.

6.1. RESUMEN DE RESULTADOS.

En las secciones siguientes de este capítulo, se presenta un resumen de los resultados alcanzados en cada uno de estos componentes, destacando la relevancia y el impacto que tienen en la protección de los activos de información de la organización. Además, se discute el aporte de este trabajo fin de grado al campo de la seguridad de la información, subrayando las metodologías y prácticas que pueden servir de referencia para futuras implementaciones. Finalmente, se ofrecen recomendaciones basadas en las lecciones aprendidas durante el proyecto, orientadas a optimizar y mejorar la gestión de la seguridad de la información en entornos similares.

Conclusiones acerca de la Evaluación de Riesgos:

La evaluación de riesgos realizada en Innovatech Consulting ha sido un proceso básico para poder identificar y priorizar las amenazas potenciales que podrían comprometer la seguridad de la información de la empresa. A través de un análisis exhaustivo y utilizando herramientas metodológicas alineadas con la norma ISO 27001:2022, se han evaluado tanto los riesgos inherentes como los residuales, lo que ha derivado en una comprensión clara de las vulnerabilidades existentes.

Uno de los principales resultados de este análisis es la identificación de áreas críticas que requieren una atención prioritaria. Los riesgos más significativos han sido aquellos relacionados con la seguridad de la información en la gestión de proveedores y la protección de datos en entornos de nube. La evaluación también ha revelado la necesidad de fortalecer los controles de acceso y mejorar las medidas de prevención contra el malware.

La clasificación de riesgos por su impacto y probabilidad ha permitido desarrollar un plan de acción enfocado en mitigar aquellos riesgos que representan las mayores amenazas para la continuidad y la integridad de los procesos de negocio. Este proceso ha evidenciado

la importancia de mantener una evaluación continua y adaptativa que permita responder de manera efectiva a un entorno en constante cambio.

Conclusiones del Plan de Acción basado en la Evaluación de Riesgos:

El Plan de Acción derivado de la Evaluación de Riesgos ha sido un elemento indispensable para poder transformar los resultados del análisis de riesgos en medidas concretas y efectivas para mitigar las amenazas identificadas. Este plan ha permitido a Innovatech Consulting estructurar y priorizar las acciones necesarias para mejorar la seguridad de la información de manera integral y alineada con los objetivos estratégicos de la empresa.

Las acciones propuestas en el plan se han diseñado para abordar directamente los riesgos más críticos con un enfoque en la implementación de controles tanto organizativos como técnicos. Entre las acciones más destacadas se encuentran la mejora en los procesos de gestión de acceso, la automatización de controles en la nube a través de Microsoft Azure y el fortalecimiento de las políticas de seguridad en la relación con proveedores.

Una conclusión importante es que la implementación de este plan no solo ha mitigado los riesgos inmediatos, sino que también ha creado un marco para la mejora continua. La flexibilidad del plan permite su adaptación a nuevos riesgos o cambios en el entorno de la empresa, asegurando que Innovatech Consulting mantenga un alto nivel de seguridad en sus operaciones.

El Plan de Acción ha demostrado ser una herramienta muy eficaz para cerrar brechas de seguridad, mejorar la resiliencia de la organización y garantizar que las medidas adoptadas se mantengan vigentes y eficaces ante las amenazas emergentes. Esta planificación proactiva refuerza la posición de Innovatech Consulting como una empresa comprometida con la excelencia en la gestión de la seguridad de la información.

Conclusiones del Análisis del Riesgo y Plan de Acción de las partes interesadas:

El análisis del riesgo enfocado en las partes interesadas ha permitido a Innovatech Consulting identificar y gestionar los riesgos específicos asociados con los diferentes grupos que interactúan con la organización, tales como accionistas, empleados, proveedores y clientes. Este enfoque ha subrayado la importancia de considerar no solo los riesgos operativos internos, sino también aquellos derivados de la relación con estas partes externas.

Una conclusión clave de este análisis es que los riesgos asociados a las partes interesadas varían en términos de probabilidad e impacto, lo que requiere una atención diferenciada y específica. Por ejemplo, se han identificado riesgos significativos en la relación

con proveedores, que han sido abordados mediante acciones como la sensibilización en seguridad de la información y la firma de acuerdos de confidencialidad.

El Plan de Acción derivado de este análisis ha establecido medidas concretas para mitigar estos riesgos asegurando que las expectativas y requisitos de cada parte interesada sean gestionados de manera efectiva. Las acciones implementadas incluyen la formación continua de empleados en temas de seguridad, el establecimiento de acuerdos claros con proveedores y la mejora de la comunicación con los clientes sobre las prácticas de seguridad de la información.

Conclusiones del establecimiento de Objetivos e Indicadores de seguridad:

El proceso de establecimiento de objetivos e indicadores de seguridad ha sido un componente exigido por la propia norma para la implementación y certificación del Sistema de Gestión de Seguridad de la Información (SGSI) en Innovatech Consulting. Este enfoque ha permitido alinear las actividades de seguridad con los objetivos estratégicos de la empresa, propiciando que todas las acciones realizadas contribuyan de manera efectiva a la protección de la información y la continuidad del negocio.

Una de las conclusiones principales es que la definición clara de objetivos de seguridad basados en el análisis de riesgos proporciona una dirección estratégica y un marco para medir el rendimiento en materia de seguridad. Los indicadores de seguridad desarrollados permiten a la organización hacer seguimiento de manera continua del cumplimiento de estos objetivos, identificando rápidamente áreas de mejora o potenciales riesgos emergentes.

También, el uso de indicadores específicos ha facilitado la medición del impacto de las acciones de seguridad implementadas, proporcionando datos objetivos que han respaldado la toma de decisiones informadas. Esto ha sido particularmente útil en la priorización de recursos y esfuerzos en áreas críticas donde el riesgo es mayor.

Además, la implementación de estos indicadores ha fomentado una cultura de mejora continua dentro de la organización donde el rendimiento en seguridad es revisado periódicamente y ajustado según sea necesario para responder a nuevos desafíos o cambios en el entorno operativo.

Conclusiones sobre la Declaración de Aplicabilidad (SOA):

La Declaración de Aplicabilidad (SOA) es otro de los requisitos centrales para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en Innovatech Consulting bajo el paraguas de la norma ISO 27001:2022; además, también ha servido como una guía práctica para la gestión efectiva de los controles de seguridad en la empresa.

Una de las principales conclusiones es que la elaboración de la SOA ha permitido a Innovatech Consulting ratificar la identificación idónea de los controles de seguridad relevantes para la organización, basados en un análisis riguroso de los riesgos. Esta identificación ha sido clave para asegurar que solo se implementen controles aplicables y necesarios, optimizando así el uso de recursos y evitando la sobrecarga operativa.

La SOA también ha facilitado la justificación clara y documentada de la inclusión o exclusión de cada control, lo que ha contribuido a una mayor transparencia y a la alineación de las prácticas de seguridad con los objetivos de negocio y las obligaciones normativas de la empresa. Esto ha fortalecido la capacidad de Innovatech Consulting para demostrar el cumplimiento normativo durante auditorías internas y externas.

Además, el proceso de evaluación y actualización de la SOA ha garantizado que el SGSI se mantenga dinámico y adaptado a las nuevas amenazas y cambios en el entorno empresarial. La integración de la SOA en la gestión diaria ha asegurado que los controles de seguridad sean revisados y mejorados de manera continua, lo que ha incrementado la operatividad de la organización ante incidentes de seguridad.

Conclusiones sobre la Automatización de controles en Microsoft Azure:

La automatización de controles del Sistema de Gestión de Seguridad de la Información (SGSI) en Microsoft Azure ha sido un avance muy interesante para Innovatech Consulting, mejorando la eficiencia, la precisión y la capacidad de respuesta en la gestión de la seguridad de la información. Este enfoque ha permitido a la empresa integrar y automatizar controles clave del SGSI, alineados con los requisitos de la norma ISO 27001:2022.

Una de las principales conclusiones es que la automatización ha reducido de manera considerable la dependencia de intervenciones manuales, minimizando el riesgo de errores humanos y asegurando que los controles de seguridad se apliquen de manera consistente y oportuna. Esta consistencia ha sido crucial para mantener un nivel alto y uniforme de seguridad en todas las operaciones de la empresa.

La implementación de controles automatizados en Azure ha facilitado la monitorización continua de la infraestructura y los sistemas, permitiendo a Innovatech Consulting detectar y responder a incidentes de seguridad con mayor rapidez. Esta capacidad de respuesta mejorada ha fortalecido la postura de seguridad de la empresa, reduciendo el tiempo de exposición a posibles amenazas.

Además, la automatización ha permitido la generación de informes y auditorías de cumplimiento de manera más eficiente, lo que ha simplificado las revisiones de seguridad y

ha proporcionado una mayor visibilidad del estado de la seguridad de la información. Esto ha sido especialmente útil para las auditorías de cumplimiento con la ISO 27001, asegurando que los procesos y controles de seguridad cumplan con los requisitos normativos sin necesidad de intervenciones adicionales.

Otro beneficio importante es que la automatización ha permitido a Innovatech Consulting escalar sus operaciones de seguridad de manera eficiente, adaptándose a cambios en la infraestructura y en las necesidades de negocio sin comprometer la seguridad. Este enfoque ha demostrado ser especialmente útil en un entorno de nube.

Conclusiones sobre el Plan de Continuidad de Negocio (BCP):

El Plan de Continuidad de Negocio (BCP) desarrollado para Innovatech Consulting también ha demostrado ser un componente esencial dentro del marco de gestión de la seguridad de la información ya que la implementación y actualización del BCP, de acuerdo con la filosofía de la norma ISO 27001:2022, ha fortalecido la capacidad de la empresa para mantener la operatividad durante situaciones de crisis.

Uno de los principales logros del BCP ha sido la identificación y priorización de los procesos críticos, asegurando que la empresa esté preparada para responder eficazmente a interrupciones que podrían comprometer la continuidad del negocio. La integración de estrategias de recuperación ante desastres y la planificación para escenarios específicos, como la inutilización de servidores o la pérdida de acceso a las instalaciones físicas, han sido clave para minimizar el impacto de posibles eventos adversos.

La actualización del BCP para incluir la nueva infraestructura basada en la nube con Microsoft Azure ha permitido a Innovatech Consulting beneficiarse de una mayor flexibilidad y redundancia en sus operaciones. Esta adaptación ha sido crucial en el contexto de un entorno de trabajo cada vez más distribuido, donde el teletrabajo es la norma. La capacidad de recuperar y restaurar servicios críticos rápidamente, independientemente de la ubicación física, ha demostrado ser un factor de éxito en la continuidad operativa.

Además, el enfoque en la formación y capacitación del personal, así como la realización regular de pruebas y simulacros, ha asegurado que todos los empleados estén familiarizados con sus roles y responsabilidades en caso de un incidente. Este nivel de preparación ha incrementado la capacidad de Innovatech Consulting para responder de manera organizada y efectiva durante una crisis.

El BCP también ha integrado un plan de comunicación para situaciones de crisis, garantizando que todas las partes interesadas, tanto internas como externas, estén

informadas de manera oportuna y precisa. Este enfoque ha reforzado la confianza de clientes, proveedores y otros socios en la capacidad de Innovatech Consulting para gestionar situaciones adversas sin comprometer la seguridad de la información ni la continuidad de los servicios.

Conclusiones sobre la Política de Seguridad de la Información:

La Política de Seguridad de la Información de Innovatech Consulting se ha consolidado como un pilar fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y refleja el compromiso de la empresa con la protección de sus activos de información. Esta política ha sido cuidadosamente diseñada para alinearse con los requisitos de la norma ISO 27001:2022, asegurando que todos los aspectos clave de la seguridad de la información sean abordados de manera efectiva.

Uno de los aspectos más destacados de la Política de Seguridad de la Información es su capacidad para proporcionar una dirección clara y coherente a todos los empleados y partes interesadas. La política garantiza que cada miembro de la organización entienda su papel en la protección de la información ya que establece roles y responsabilidades definidas, lo que refuerza una cultura de seguridad dentro de la empresa.

Además, la política ha sido desarrollada para ser dinámica y adaptable a los cambios en el entorno de amenazas y en las necesidades organizativas. Esto se refleja en su enfoque en la mejora continua y la revisión periódica, lo que permite que la política evolucione junto con la empresa y las amenazas emergentes.

La integración de la política con los demás elementos del SGSI, como la gestión de riesgos, la declaración de aplicabilidad (SOA) y el plan de continuidad de negocio, asegura que la seguridad de la información esté íntimamente vinculada a los objetivos y operaciones diarias de Innovatech Consulting. Este enfoque global fortalece la postura de seguridad de la empresa y también facilita el cumplimiento normativo, así como la mitigación de riesgos.

Otro punto clave es la comunicación efectiva de la política a todos los niveles de la organización. Al hacerla accesible y comprensible para todos los empleados, Innovatech Consulting ha logrado una mayor adhesión a las prácticas de seguridad, minimizando así el riesgo de incidentes causados por el factor humano.

6.2. APORTE DEL TRABAJO AL CAMPO DE LA SEGURIDAD DE LA INFORMACIÓN.

Este Trabajo de Fin de Grado (TFG) realizado en Innovatech Consulting pretende contribuir al campo de la seguridad de la información, particularmente en la implementación y

gestión de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022. A través del desarrollo de metodologías funcionales, la integración de herramientas avanzadas y la aplicación de un enfoque sistemático para la seguridad, este trabajo no solo refuerza las prácticas establecidas, sino que también aporta innovaciones que pueden ser adoptadas por otras organizaciones.

Uno de los aportes más relevantes es la aplicación de un enfoque automatizado para la gestión de controles de seguridad mediante Microsoft Azure. Este enfoque no solo mejora la eficiencia operativa al reducir la intervención humana en procesos repetitivos, sino que también establece un precedente en la automatización de la seguridad dentro de entornos de nube, un área en constante evolución y de creciente importancia en el mundo de las empresas.

Además, el trabajo ha puesto de relieve la importancia de un análisis exhaustivo de riesgos y partes interesadas como base para la toma de decisiones informadas en seguridad de la información. La metodología desarrollada para el análisis de riesgos y la elaboración del Plan de Continuidad de Negocio (BCP) proporciona un marco adaptable y robusto que puede ser replicado y adaptado por otras organizaciones para mejorar su adaptabilidad y flexibilidad frente a incidentes de seguridad.

Otro aspecto innovador es la alineación de la Política de Seguridad de la Información con los objetivos estratégicos de la empresa. Este enfoque garantiza que la seguridad no se vea como un costo o una barrera, sino como un habilitador de negocio que apoya y protege los intereses de la organización.

Finalmente, este TFG pretende modestamente contribuir al conocimiento académico y profesional en seguridad de la información al ofrecer un estudio de un caso detallado y una serie de lecciones aprendidas que pueden informar tanto la práctica profesional como la futura investigación en el campo. Al documentar este proceso de manera estructurada y reflexiva, se proporciona una base para la comprensión y aplicación de la norma ISO 27001:2022, así como para la mejora continua en la gestión de la seguridad de la información en diversas organizaciones.

6.3. PROPUESTAS PARA IMPLEMENTACIONES FUTURAS.

Este apartado tiene como objetivo presentar propuestas para futuras implementaciones y mejoras del Sistema de Gestión de Seguridad de la Información (SGSI) en Innovatech Consulting. Estas propuestas se basan en las experiencias y aprendizajes adquiridos durante el desarrollo del presente TFG y se organizan en varias líneas de trabajo

estratégicas. Estas líneas no solo buscan optimizar y completar la implementación del SGSI, sino también explorar nuevas oportunidades tecnológicas y de automatización.

a) Ampliación de la implementación del SGSI.

A lo largo de este proyecto, se ha avanzado significativamente en la implementación de la norma ISO 27001:2022. Sin embargo, es esencial continuar con la implementación completa de todos los requisitos normativos, especialmente aquellos que no se han abordado en profundidad en este trabajo, como el contexto de la organización, las necesidades y expectativas de las partes interesadas, el compromiso de la dirección, y la elaboración de procedimientos específicos.

Propuesta: Desarrollar un plan detallado para completar la implementación de todos los requisitos de la norma, incluyendo la integración de procesos de auditoría interna y externa, la mejora continua y el tratamiento de no conformidades.

b) Expansión de la automatización a otras plataformas Cloud.

La automatización en Microsoft Azure ha demostrado ser una herramienta eficaz para la gestión de la seguridad de la información. Sin embargo, existen otras plataformas cloud, como Google Cloud y Amazon Web Services (AWS), que pueden beneficiarse de un enfoque de automatización similar.

Propuesta: Investigar las capacidades de automatización en estas plataformas y desarrollar un plan para extender la automatización del SGSI a múltiples entornos cloud. Esto permitirá ampliar conocimientos acerca de maximizar la flexibilidad y la resiliencia de las infraestructuras de seguridad.

c) Innovación en el Ecosistema NormaPro

NormaPro ha sido una herramienta central en la gestión del SGSI en Innovatech Consulting. Para seguir optimizando los recursos y mejorando la eficiencia operativa sería interesante explorar nuevas funcionalidades y herramientas dentro del ecosistema NormaPro.

Propuesta: Colaborar con el equipo de desarrollo de NormaPro para identificar y desarrollar nuevas funcionalidades que permitan automatizar más procesos relacionados con la seguridad de la información. Esto incluiría la implementación de herramientas de análisis y monitorización avanzada que podrían integrarse en futuras versiones del software.

d) Consideraciones sobre la evolución normativa.

El entorno normativo de la seguridad de la información está en constante evolución. Innovatech Consulting debe mantenerse al día con cualquier cambio en las normativas y estándares que puedan impactar su SGSI.

Propuesta: Establecer un proceso de revisión periódica de las normativas y estándares relevantes, asegurando que el SGSI de Innovatech Consulting se mantenga conforme a las mejores prácticas y requisitos normativos actuales.

e) Desarrollo de competencias y capacitación continua.

La formación continua en seguridad de la información es crucial para mantener un alto nivel de conciencia y competencia entre los empleados de Innovatech Consulting. Dado el entorno cambiante y la aparición constante de nuevas amenazas, es esencial que la empresa fortalezca su programa de capacitación.

Propuesta: Implementar un programa de capacitación continua que incluya temas avanzados de seguridad, simulacros de incidentes y actualizaciones constantes sobre nuevas amenazas y tecnologías emergentes. Esto garantizaría que el personal esté siempre preparado para enfrentar los desafíos de seguridad más recientes.

Estas propuestas proporcionan una hoja de ruta clara para Innovatech Consulting y otras organizaciones que deseen fortalecer su SGSI, adaptándose a los cambios tecnológicos y normativos, y asegurando una mejora continua en la gestión de la seguridad de la información.

DOCUMENTO Nº 2: PRESUPUESTO PARA EL MANTENIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

El presente presupuesto tiene como objetivo estimar y detallar los recursos económicos necesarios para llevar a cabo el mantenimiento del Sistema de Gestión de la Seguridad de la Información (SGSI) en Innovatech Consulting, conforme a la norma ISO 27001. El propósito principal de estas labores es asegurar que la organización mantenga su certificación por una entidad externa acreditada, garantizando que todos los controles y procesos de seguridad de la información sigan cumpliendo con los estándares internacionales. La implementación y mantenimiento del SGSI son esenciales para proteger la confidencialidad, integridad y disponibilidad de los activos de información de la empresa.

1. DETALLE DEL PRESUPUESTO.

1. **Recursos humanos**:

Los costes asociados a la intervención del personal involucrado en el mantenimiento del SGSI, incluyendo:

1.1. Coordinación de actividades de mantenimiento del SGSI (Responsable del Sistema): 1 Ingeniero informático (media jornada) cuyo coste de empresa es de 36.000 €/anuales (Impuestos y Seguridad Social incluidos): ……18.000 €.

1.2. Implementación de medidas determinada en el Plan de acción derivado de la Evaluación de riesgos (la carga de trabajo puede observarse en la Matriz del Plan en la **Tabla 12)**:

1.2.1. Mantenimiento de Azure Defender supone una carga de 2 horas semanales, o lo que es igual, 104 horas al año, por 30 €/hora de Técnico especialista: ……..……..3.120 €.

1.2.2. Implementación específica de las acciones programadas para los siguientes controles:

- Procedimientos y responsabilidades operacionales
- Protección contra código malicioso
- Control del software en explotación
- Seguridad en el desarrollo y en los procesos de soporte.

Total 624 h (Ver Tabla 12) a 30 €/h coste de Consultor especialista: ……..…….. 8.520 €

1.3. Formación y concienciación en seguridad de la información para los empleados. El propio responsable del Sistema imparte 2 jornadas de 2 horas de formación a 12 empleados en el que empeña 8 horas para la preparación de la acción formativa y su evaluación posterior. A esto hay que sumar las 4 horas destinadas por los propios empleados haciendo un total de 60 horas cuyo coste aproximado es de 18 €/h ……..……...…. 1.080 €

Total Capítulo 1: ……..……. **30.720 €**

2. **Tecnología**:

Los Costes derivados del uso y mantenimiento de tecnologías y herramientas necesarias para la gestión del SGSI, como:

2.1. Licencias de software seguro Microsoft Office 365 suponen 10 €/mes por usuario siendo 13 usuarios …….. 1.560 €

2.2. Licencia de AZURE Defender (Solo se tiene en cuenta el pago extra sobre la licencia de Microsoft AZURE), 89 €/mes ……..……. 1.068 €

2.3. Licencia Github PRO suponen 9 €/mes …….. 108 €

2.4. Active Directory on Cloud AD en Azure 50€/mes …….. 600 €

Total Capítulo 2: …… **3.336 €**

3. **Auditoría externa**:

Los costes asociados a la contratación de consultores externos y auditores acreditados que realizarán las revisiones necesarias para mantener la certificación, incluyendo:

3.1. Se contrata a una consultora externa privada para la realización de la Auditoría interna. En este caso la Entidad Nacional de Acreditación (ENAC) estima 2 de jornadas de auditoria por lo que se toma ese dato también para la auditoría interna. El presupuesto es de 650 €/jornada: ……..……. 1.300 €.

3.2. Auditoría externa de seguimiento de la certificación por entidad acreditada por ENAC: ……..……... 2.200 €

Total Capítulo 3: ……..……. **3.500 €**

4. **Total presupuesto: ……... 37.556 €**

2. CONSIDERACIONES FINALES.

El presente presupuesto ha sido diseñado con el objetivo de asegurar el correcto funcionamiento del SGSI durante un año, manteniendo en todo momento la conformidad con los requisitos de la norma ISO 27001. Es fundamental que cada área cuente con los recursos adecuados para garantizar que los controles y procedimientos se apliquen de manera efectiva, y que la empresa pueda mantener la certificación sin dificultades.

Este presupuesto es flexible y está sujeto a ajustes en función de las necesidades operativas y del resultado de las auditorías internas y externas que se lleven a cabo durante el periodo contemplado.

BIBLIOGRAFÍA.

Este capítulo recoge todas las fuentes y referencias bibliográficas que se han utilizado a lo largo del trabajo. Es esencial acreditar las fuentes consultadas para desarrollar las metodologías, análisis y propuestas presentadas en este Trabajo de Fin de Grado. A continuación, se presenta la lista de referencias:

1. **ISO/IEC 27001:2022**. *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*. International Organization for Standardization, 2022.
2. **ISO/IEC 27002:2022**. *Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información*. International Organization for Standardization, 2022.
3. **NIST Special Publication 800-30 Rev. 1**. *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology, 2012.
4. **Microsoft Azure Documentation**. *Azure Security Overview*. Microsoft, 2023. Disponible en: https://docs.microsoft.com/azure/security/.
5. **ISO/IEC 22301:2019**. *Seguridad y Resiliencia - Sistemas de gestión de continuidad del negocio - Requisitos*. International Organization for Standardization, 2019.
6. **ISO/IEC 31000:2018**. *Gestión del riesgo - Directrices*. International Organization for Standardization, 2018.
7. **Cloud Security Alliance (CSA)**. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Cloud Security Alliance, 2021.
8. **Disterer, Georg**. *ISO/IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información*. *Journal of Information Security and Applications*, 2013.
9. **Herzog, Peter**. *The OSSTMM: Open Source Security Testing Methodology Manual*. Institute for Security and Open Methodologies, 2018.
10. **Stallings, William**. *Cryptography and Network Security: Principles and Practice*. 7ª edición, Pearson, 2017.
11. **Smith, David J.**. *Data Management and Information Security in Cloud Computing*. *International Journal of Information Management*, 2022.
12. **Ramirez, Juan**. *Risk Management in IT Systems: ISO 27001/27002 Implementation*. Springer, 2020.

13. **NormaPro User Manual**. *Guía de Usuario de NormaPro para la Gestión de la Seguridad de la Información*. Instituto de Innovación, Ciencia y Empresa, 2023.
14. **Peltier, Thomas R.**. *Information Security Risk Analysis*. CRC Press, 2016.
15. **Von Solms, Rossouw y Van Niekerk, Johan**. *Information Security: Governance, Risk, and Compliance*. Wiley, 2013.
16. **International Electrotechnical Commission (IEC)**. *IEC 62443-3-3:2013 - Industrial communication networks - Network and system security*. IEC, 2013.
17. **Gómez, Patricia y Rivas, Manuel**. *El Rol de la Automatización en la Seguridad de la Información en Entornos Cloud*. *Revista Española de Seguridad Informática*, 2021.
18. **SANS Institute**. *Critical Security Controls for Effective Cyber Defense (Version 8)*. SANS, 2021.
19. **Böhme, Rainer**. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Springer, 2017.
20. **CIS Controls v8**. *Center for Internet Security Critical Security Controls for Effective Cyber Defense*. Center for Internet Security, 2021.
21. **Cano, Ulises**. *Aplicación de la ISO 27001 en PYMES: Casos Prácticos y Lecciones Aprendidas*. *Revista Latinoamericana de Seguridad de la Información*, 2022.
22. **Gartner Research**. *Trends in Cybersecurity for 2024*. Gartner, 2023.
23. **Proyecto Metodología de Evaluación de Riesgos INICIE**. Instituto de Innovación, Ciencia y Empresa, 2023.
24. **AENOR**. *Guía práctica para la implementación de un Sistema de Gestión de Seguridad de la Información según la norma ISO/IEC 27001:2022*. Asociación Española de Normalización y Certificación, 2023.

ANEXO I: PLAN DE CONTINUIDAD DE NEGOCIO

PLAN DE CONTINUIDAD DE NEGOCIO 2024

	Nombre	Función	Fecha	Firma
Elaborado	Noemí M.	Responsable SIG	12/06/2024	
Revisado	JMG	Responsable SIG	12/06/2024	
Aprobado	JMG	Dirección	12/06/2024	

MODIFICACIONES VERSIÓN ANTERIOR:

Versión 01: Edición inicial.

Versión 02: corrección de erratas.

Versión 03: adaptación del plan de continuidad a la nueva organización de servidores y contratación de los servicios del nuevo proveedor.

Índice

1. OBJETO

El **Plan de Continuidad de Negocio (BCP)** de Innovatech Consulting tiene como objeto establecer un marco estructurado y detallado de acciones, responsabilidades y procedimientos que permitan a la organización responder eficazmente ante una interrupción significativa de sus operaciones críticas.

El plan se enfoca en asegurar que, ante cualquier evento adverso, Innovatech Consulting pueda restablecer sus funciones esenciales dentro de un período de tiempo aceptable, minimizando el impacto en el negocio y garantizando la continuidad de sus servicios a clientes y partes interesadas.

Este BCP también contempla la recuperación post-desastre, permitiendo que la empresa regrese a su nivel operativo normal tan pronto como sea posible. Asimismo, incluye directrices para realizar pruebas periódicas del plan, con el fin de asegurar su eficacia y actualización continua.

2. ALCANCE

El **alcance del Plan de Continuidad de Negocio (BCP)** de Innovatech Consulting abarca todos los procesos de negocio críticos que son esenciales para la continuidad operativa de la empresa. Esto incluye, pero no se limita a, los sistemas de información, infraestructura tecnológica, comunicaciones, y los servicios clave que soportan las operaciones diarias de la organización.

Particularmente, el plan se centra en la gestión de contingencias relacionadas con los servidores internos y aquellos alojados en la nube a través de Microsoft Azure, así como en la respuesta a eventos que puedan afectar las instalaciones físicas de la empresa.

El BCP cubre todas las áreas funcionales de Innovatech Consulting y establece las directrices para asegurar la continuidad de los servicios, la recuperación de sistemas críticos y la mitigación de riesgos en escenarios de desastre.

3. ACTIVACIÓN DEL PLAN

El Plan de Continuidad de Negocio (BCP) de Innovatech Consulting se activará en caso de la materialización de un evento o desastre que interrumpa significativamente los procesos críticos de la empresa. Dichos eventos pueden incluir, pero no se limitan a:

- Fallo de un equipo o servidor, ya sea físico en las instalaciones de Innovatech Consulting o alojado en la nube mediante Microsoft Azure.

- Inutilización de la infraestructura del centro de datos, como el RACK de servidores.
- Imposibilidad de acceder a las instalaciones físicas de la empresa debido a situaciones como incendios, inundaciones, u otros desastres naturales o incidentes graves.
- Cualquier otro incidente que resulte en la pérdida de acceso a los recursos tecnológicos o infraestructurales clave necesarios para mantener la continuidad operativa.

La activación del plan puede ser iniciada por cualquier miembro del personal que detecte la ocurrencia de un desastre, quien deberá comunicar de inmediato la situación al responsable del Departamento de Tecnologías de la Información. Si dicho responsable no está disponible, la situación debe ser escalada a la Dirección General o al responsable del Sistema de Gestión Integrado (SIG).

Una vez notificada la incidencia, el Comité de Continuidad de Negocio, en colaboración con el responsable del Departamento de Tecnologías de la Información, evaluará la situación y determinará si procede la activación del BCP. La activación se considerará efectiva una vez que se comiencen a ejecutar las acciones de contingencia definidas en este plan para el escenario de desastre correspondiente.

Es importante destacar que, independientemente de la causa del desastre, se considera que los activos críticos afectados no estarán disponibles durante un periodo indeterminado. Por tanto, se debe recurrir a las soluciones alternativas establecidas en el BCP para garantizar la continuidad de las operaciones.

4. ACCIONES DE CONTINGENCIA

Las acciones de contingencia están diseñadas para mitigar el impacto inmediato de un desastre o interrupción significativa en los procesos críticos de Innovatech Consulting. Estas acciones permiten restaurar temporalmente los servicios y operaciones esenciales mientras se ejecutan los planes de recuperación a largo plazo. Las contingencias se han categorizado según diferentes escenarios de desastre identificados, y para cada uno de ellos se han definido pasos específicos a seguir.

Es fundamental que todas las acciones de contingencia se implementen rápidamente para minimizar el tiempo de inactividad y el riesgo asociado con la interrupción de los servicios. A continuación, se detallan las acciones a seguir en caso de que un equipo o servidor crítico deje de funcionar.

4.1. Un equipo deja de funcionar. Puede tratarse de un servidor físico en las instalaciones de Innovatech Consulting o en la nube.

En el caso de que un equipo o servidor, ya sea físico o en la nube, deje de funcionar, se deben llevar a cabo las siguientes acciones de contingencia:

- **Restauración de un servidor físico en las instalaciones de Innovatech Consulting:**
    - Si el servidor afectado se encuentra en el RACK dentro de las instalaciones de Innovatech Consulting, se procederá a restaurar una de las copias de seguridad existentes en un servidor de respaldo.
    - Se deben realizar pruebas exhaustivas para asegurar que las aplicaciones críticas y los datos estén disponibles y funcionen correctamente. Esto incluye verificar la conectividad, acceso y permisos correspondientes a las diferentes carpetas de usuarios y aplicativos.
- **Restauración de un servidor en la nube (Microsoft Azure):**
    - Si el servidor afectado se encuentra alojado en la nube, se contactará de inmediato con el proveedor de servicios en la nube (Microsoft Azure) para iniciar la restauración del servidor utilizando la última copia de seguridad disponible.
    - Se llevarán a cabo las pruebas necesarias para confirmar que el servidor restaurado opera correctamente y que todos los servicios y datos están accesibles según lo esperado.

Estas acciones tienen como objetivo principal restablecer la funcionalidad de los servidores afectados y asegurar que las operaciones críticas de Innovatech Consulting puedan continuar sin interrupciones significativas.

4.2. El RACK queda inutilizado

En caso de que el RACK que alberga los servidores y equipos críticos de Innovatech Consulting quede inutilizado, se deben llevar a cabo las siguientes acciones de contingencia para restaurar los servicios esenciales:

- **Traslado y reinstalación de los servidores:**
    - Si es posible, los servidores serán trasladados a un nuevo RACK dentro de las mismas instalaciones de Innovatech Consulting. Una

vez reubicados, se procederá a reconectar y reiniciar los equipos para restaurar el acceso a los sistemas y servicios críticos.

- Se debe realizar una revisión exhaustiva para asegurar que todos los sistemas estén operativos y que los datos y aplicaciones sean accesibles según lo previsto.

- **Escenario de daño severo en el RACK:**
  - Si el daño al RACK es tal que los servidores no pueden ser reutilizados en sus ubicaciones originales, se procederá a la restauración de los sistemas utilizando la infraestructura en la nube de Microsoft Azure, según lo detallado en el apartado 4.1.
  - Este proceso implicará el uso de las copias de seguridad almacenadas en la nube para reinstaurar los servicios en servidores virtuales. Se deben llevar a cabo pruebas de conectividad y operatividad para asegurar que todos los servicios estén funcionando correctamente.
- **Coordinación con proveedores:**
  - Se contactará de inmediato con los proveedores de equipos y servicios para iniciar el reemplazo y reinstalación de los equipos del RACK dañados. La prioridad será restablecer el entorno físico lo antes posible para permitir una migración de vuelta a las instalaciones de Innovatech Consulting, si es necesario.

Estas medidas están diseñadas para garantizar la continuidad de los servicios en caso de que el RACK, una parte esencial de la infraestructura física de Innovatech Consulting, quede inutilizado. La capacidad de trasladar operaciones a un entorno alternativo en la nube asegura que los procesos de negocio críticos no se vean interrumpidos durante un tiempo prolongado.

4.3. El Edificio queda inutilizado

En el caso de que el edificio que alberga las oficinas de Innovatech Consulting quede inutilizado, es crucial garantizar la continuidad de los procesos de negocio, teniendo en cuenta que toda la plantilla de trabajadores opera en modalidad de teletrabajo. A continuación, se detallan las acciones de contingencia que se deben seguir:

- **Uso de Infraestructura en la Nube:**

- Dado que los servidores críticos y la mayoría de los sistemas de Innovatech Consulting están alojados en la nube a través de Microsoft Azure, la pérdida del acceso físico al edificio no interrumpirá significativamente las operaciones. Los empleados podrán seguir accediendo a los sistemas y aplicaciones críticas desde cualquier ubicación con acceso a internet.

- **Comunicación con el Personal:**
  - Se debe comunicar de inmediato al personal la situación a través de los canales de comunicación establecidos (correo electrónico, mensajería instantánea, etc.) para informarles sobre la inutilización del edificio y las medidas temporales que se implementarán.
  - Instruir al personal para que continúe sus operaciones desde sus ubicaciones actuales de teletrabajo, asegurando que tengan acceso a todos los recursos necesarios para mantener la continuidad de las actividades.
- **Reposición de Equipos Físicos:**
  - Para aquellos empleados que puedan necesitar acceso a equipos o recursos que estaban ubicados en el edificio, se debe coordinar la provisión de equipos alternativos o acceso a los recursos desde ubicaciones seguras.
  - Si es necesario, se considerará el envío de equipos de reemplazo o la configuración de acceso remoto a recursos que estaban exclusivamente disponibles en el edificio.
- **Recuperación de Servicios Presenciales:**
  - En caso de que sea necesario restablecer la capacidad de trabajar en un entorno físico, Innovatech Consulting evaluará la opción de alquilar oficinas temporales o utilizar espacios de coworking seguros y adecuadamente equipados, hasta que el edificio original esté nuevamente operativo.
  - Durante este tiempo, se garantizará que todos los servicios críticos estén accesibles de forma remota, minimizando la dependencia de una infraestructura física específica.

Estas acciones aseguran que, incluso si el edificio de Innovatech Consulting queda inutilizado, los procesos de negocio puedan continuar sin interrupción

significativa gracias al teletrabajo y la infraestructura en la nube. La prioridad es mantener la operatividad del personal y la accesibilidad a los recursos necesarios, sin que la pérdida del edificio afecte gravemente las operaciones.

4.4. Contingencias de Recursos Críticos No Tecnológicos

En este apartado se abordan contingencias que afectan a recursos críticos no tecnológicos, pero esenciales para la continuidad del negocio, como la falta de acceso a personal clave, proveedores críticos, o servicios esenciales que no estén directamente relacionados con la tecnología.

4.4.1. Falta de Acceso a Personal Clave

- **Identificación del Personal Clave:**
  - El BCP debe incluir una lista actualizada de personal clave cuya ausencia podría impactar significativamente las operaciones. Esto incluye roles críticos en la gestión, tecnología, y operaciones diarias.
- **Plan de Sucesión y Delegación:**
  - Implementar un plan de sucesión para garantizar que, en caso de que el personal clave no esté disponible, otros empleados capacitados puedan asumir temporalmente sus responsabilidades.
  - Asegurar que existan protocolos claros para la delegación de funciones en situaciones de emergencia.

4.4.2. Interrupción de Servicios de Proveedores Críticos

- **Identificación de Proveedores Críticos:**
  - Mantener un inventario actualizado de proveedores críticos, incluyendo servicios en la nube, telecomunicaciones, y suministros esenciales.
- **Acuerdos de Servicio Alternativos:**
  - Desarrollar y mantener acuerdos con proveedores alternativos que puedan asumir las funciones de los proveedores críticos en caso de interrupción.
- **Monitoreo y Comunicación:**

- Establecer mecanismos de monitoreo para detectar posibles interrupciones en los servicios de los proveedores críticos, y asegurar una comunicación fluida para resolver contingencias de manera rápida.

4.4.3. Falta de Acceso a Servicios Esenciales

- **Servicios Esenciales Identificados:**
  - Estos incluyen electricidad, acceso a internet, y otros servicios vitales que, aunque no directamente relacionados con la tecnología, son fundamentales para la operación diaria.
- **Plan de Respaldo para Servicios Esenciales:**
  - Implementar soluciones de respaldo, como generadores para cortes de electricidad, o contratos con múltiples proveedores de internet para asegurar la conectividad.
- **Procedimientos de Emergencia:**
  - Definir procedimientos claros para actuar en caso de interrupción de estos servicios, incluyendo comunicación con empleados y alternativas temporales para mantener las operaciones.

5. ACCIONES DE RECUPERACIÓN

Las acciones de recuperación tienen como objetivo restablecer completamente los servicios y operaciones a su estado normal después de la ejecución de las acciones de contingencia. Estas acciones están diseñadas para asegurar que Innovatech Consulting no solo recupere su funcionalidad crítica, sino que también restablezca todas sus operaciones de forma eficiente y eficaz. A continuación, se detallan las acciones de recuperación correspondientes a los diferentes escenarios de contingencia:

5.1. Recuperación de Equipos Críticos

- **5.1.1. Recuperación de Servidores Físicos y Virtuales:**
  - **Verificación de la Integridad de los Datos:** Tras la restauración de los servidores, se deben realizar verificaciones exhaustivas para asegurar que todos los datos recuperados estén íntegros y actualizados.

- **Reconfiguración de Servidores:** Ajuste y reconfiguración de servidores físicos o virtuales para alinearlos con los parámetros operativos estándar de Innovatech Consulting.
- **Validación de Operaciones:** Ejecución de pruebas operativas para garantizar que los servidores restaurados funcionan correctamente y soportan todas las aplicaciones y servicios críticos.

- **5.1.2. Sustitución de Equipos Afectados:**
  - **Adquisición y Configuración de Nuevos Equipos:** Proceder con la compra de nuevos equipos para reemplazar los dañados, seguidos de su configuración para asegurar que cumplan con los requisitos de Innovatech Consulting.
  - **Migración de Datos y Aplicaciones:** Transferencia de datos y aplicaciones al nuevo hardware, garantizando que no haya pérdida de información y que los servicios se reanuden de manera efectiva.

5.2. Restauración de Infraestructura Física

- **5.2.1. Reubicación de la Infraestructura Física:**
  - **Transporte y Configuración de Equipos:** En el caso de que se haya llevado a cabo una reubicación temporal de servidores u otros equipos, se deberán devolver a sus ubicaciones originales una vez restaurada la infraestructura física.
  - **Reconexión de Servicios:** Reestablecimiento de todas las conexiones de red, electricidad y otros servicios esenciales para asegurar que los equipos operen en su capacidad máxima.
- **5.2.2. Rehabilitación del RACK y Áreas Críticas:**
  - **Inspección y Reparación del RACK:** Realizar una inspección detallada del RACK afectado y proceder con las reparaciones necesarias para devolverlo a su estado funcional completo.
  - **Reinstalación de Equipos:** Reubicar todos los equipos en el RACK reparado y llevar a cabo las pruebas necesarias para garantizar que todos los sistemas estén operativos.

5.3. Restauración del Edificio y Espacios de Trabajo

- **5.3.1. Rehabilitación de las Oficinas (si aplica):**
    - **Evaluación de Daños:** Inspección completa del edificio o espacio afectado para identificar los daños sufridos y determinar las reparaciones necesarias.
    - **Plan de Reinstalación:** Desarrollar un plan detallado para la reinstalación de personal y equipos en el edificio, asegurando un entorno de trabajo seguro y funcional.
- **5.3.2. Alternativas de Trabajo Remoto:**
    - **Continuación del Teletrabajo:** Mantener la modalidad de teletrabajo hasta que las oficinas sean completamente seguras y operativas.
    - **Reincorporación Gradual:** Planificar la reincorporación gradual del personal a las oficinas, asegurando que las áreas críticas estén prioritariamente disponibles para los empleados clave.

5.4. Restablecimiento de la Normalidad Operativa

- **5.4.1. Validación Completa de Servicios:**
    - **Pruebas Integrales:** Realizar pruebas exhaustivas de todos los sistemas y servicios para confirmar que la operación ha sido completamente restaurada.
    - **Revisión de Procesos:** Evaluar y ajustar cualquier proceso que haya sido alterado durante la contingencia para asegurar que se alinea con las políticas operativas estándar.
- **5.4.2. Documentación y Lecciones Aprendidas:**
    - **Registro de Acciones de Recuperación:** Documentar todas las acciones realizadas durante el proceso de recuperación, incluyendo tiempos de respuesta, soluciones implementadas y cualquier desafío encontrado.
    - **Revisión del BCP:** Con base en la experiencia adquirida durante la contingencia, revisar y actualizar el Plan de Continuidad de Negocio para mejorar la respuesta ante futuros incidentes.

6. DATOS DE CONTACTO

Puesto	*Nombre*	*Teléfono*	*Correo electrónico*
Dirección de INNOVATECH CONSULTING	JMG	111 111 111	jmg@innovatechconsulting.com
	JAQ	111 111 111	jaq@innovatechconsulting.com
Responsable SIG	Noemí M.	111 111 111	nm@innovatechconsulting.com
Responsable Dto. Tecnologías Información	AT	111 111 111	at@innovatechconsulting.com
Soporte AZURE	El responsable del Departamento de Tecnologías de la Información contactará con AZURE a través de la plataforma “portal.azure.com”.		

7. MANTENIMIENTO Y PRUEBAS DEL PLAN

El Plan de Continuidad de Negocio (BCP) de Innovatech Consulting debe ser un documento vivo, sujeto a revisiones y actualizaciones regulares para asegurar su efectividad continua. El mantenimiento adecuado del plan, así como la realización de pruebas periódicas, son esenciales para garantizar que la organización esté preparada para enfrentar cualquier eventualidad que pueda interrumpir las operaciones críticas. A continuación, se describen las prácticas de mantenimiento y el plan de pruebas anual:

7.1. Mantenimiento del Plan

- **7.1.1. Revisión Anual del BCP:**
    - El BCP será revisado al menos una vez al año para asegurarse de que sigue siendo relevante y efectivo. Esta revisión debe considerar cambios en la estructura organizacional, actualizaciones tecnológicas, nuevas amenazas y vulnerabilidades, así como cualquier lección aprendida de incidentes anteriores o ejercicios de simulación.
    - La revisión será coordinada por el responsable del SIG en colaboración con el Responsable del Departamento de Tecnologías de la Información, y cualquier cambio propuesto será sometido al Comité del SIG para su aprobación.

- **7.1.2. Actualización Continua:**
    - Además de la revisión anual, el BCP será actualizado cada vez que se produzcan cambios significativos en la infraestructura tecnológica, en la estructura organizativa, o en las operaciones de Innovatech Consulting.
    - Todos los cambios y actualizaciones deben ser documentados y comunicados a todas las partes relevantes para asegurar la preparación continua.
- **7.1.3. Distribución y Acceso:**
    - Una copia actualizada del BCP se almacenará en un repositorio online seguro, accesible a todos los empleados a través de la plataforma NormaPro. Esto garantiza que todos los empleados tengan acceso a la versión más reciente del plan en caso de emergencia.

7.2. Plan de Pruebas Anual

- **7.2.1. Pruebas de Simulacro:**
    - Innovatech Consulting llevará a cabo simulacros anuales que cubran al menos uno de los escenarios de desastre identificados. Estos simulacros son esenciales para probar la eficacia del BCP y la capacidad de respuesta del personal involucrado.
    - Durante un ciclo de tres años, todos los escenarios de desastre identificados (fallo de servidor, inutilización del RACK, inutilización del edificio, etc.) deben ser puestos a prueba para garantizar que el BCP cubra de manera efectiva todas las posibles contingencias.
- **7.2.2. Evaluación y Documentación de Pruebas:**
    - Después de cada simulacro, se llevará a cabo una evaluación exhaustiva para identificar cualquier debilidad o área de mejora en el BCP. Se deben documentar todos los hallazgos, incluyendo cualquier incidencia o problema detectado durante el ejercicio.
    - Un informe específico debe ser elaborado por el Responsable del Departamento de Tecnologías de la Información y revisado por el Comité del SIG. Cualquier ajuste o mejora identificada debe ser incorporada en la siguiente actualización del BCP.

- **7.2.3. Comprobaciones Periódicas:**
    - Además de los simulacros, se realizarán revisiones técnicas cada seis meses para verificar la integridad y disponibilidad de los datos críticos. Estas revisiones incluirán:
        - La restauración de la última copia de seguridad de las bases de datos.
        - Comprobaciones de acceso desde dispositivos cliente a servidores y servicios restringidos por usuario.
        - Validación de las configuraciones de seguridad de los sistemas y redes críticas.
- **7.2.4. Seguimiento de Incidencias:**
    - Cualquier incidencia detectada durante las pruebas y comprobaciones debe ser registrada y seguida de cerca hasta su completa resolución. El seguimiento debe incluir la identificación de la causa raíz, la implementación de soluciones correctivas y la validación de la efectividad de dichas soluciones.

8. PLAN DE PRUEBAS ANUAL

El Plan de Pruebas Anual de Innovatech Consulting es una parte integral del Plan de Continuidad de Negocio (BCP). Las pruebas periódicas son esenciales para garantizar que el plan sea eficaz y que el personal esté preparado para responder adecuadamente en caso de una emergencia. A continuación, se detallan las actividades y cronograma del plan de pruebas anual:

8.1. Simulacros de Escenarios de Desastre

- **8.1.1. Ciclo de Pruebas Trienal:**
    - Durante un ciclo de tres años, Innovatech Consulting se compromete a probar todos los escenarios de desastre identificados en el BCP. Estos escenarios incluyen la falla de un servidor, la inutilización del RACK, la inutilización del edificio, y otros eventos potenciales que puedan interrumpir los procesos críticos de negocio.
    - Cada año se seleccionará al menos uno de estos escenarios para ser puesto a prueba, asegurando así que cada escenario sea evaluado al menos una vez durante el ciclo de tres años.

- **8.1.2. Metodología de Simulacros:**
    - Los simulacros se realizarán en condiciones controladas para evaluar la efectividad de las acciones de contingencia y recuperación establecidas en el BCP.
    - Se involucrará a todo el personal relevante, quienes deberán seguir los procedimientos especificados en el plan sin previo aviso para simular condiciones reales de emergencia.
    - Los resultados de cada simulacro se documentarán, evaluando el desempeño del equipo, la adecuación de los procedimientos y cualquier área de mejora identificada.

8.2. Revisión Semestral de Sistemas y Datos

- **8.2.1. Validación de Copias de Seguridad:**
    - Cada seis meses, se llevará a cabo una restauración de la última copia de seguridad de las bases de datos críticas para asegurar que los datos pueden ser recuperados de manera efectiva en caso de desastre.
    - Se realizarán comprobaciones adicionales para validar la integridad y consistencia de los datos restaurados.
- **8.2.2. Comprobación de Accesos:**
    - Se realizarán pruebas periódicas de acceso desde dispositivos cliente a los servidores y servicios críticos. Estas pruebas incluirán la validación de configuraciones de permisos y la accesibilidad de usuarios a los recursos necesarios.
- **8.2.3. Revisión de Configuraciones de Seguridad:**
    - Durante estas revisiones, se comprobarán las configuraciones de seguridad de los sistemas y redes críticos, incluyendo la gestión de identidades, autenticación y control de accesos.
    - Cualquier vulnerabilidad o inconsistencia identificada será documentada y corregida inmediatamente.

8.3. Documentación y Seguimiento de Pruebas

- **8.3.1. Registro de Resultados:**

- Los resultados de todas las pruebas, incluidas las pruebas de simulacro y las revisiones semestrales, se documentarán en informes detallados. Estos informes incluirán descripciones de las pruebas realizadas, los resultados obtenidos, cualquier incidencia o falla detectada, y las acciones correctivas recomendadas.

- **8.3.2. Informe de Incidencias:**
  - Si durante una prueba se identifica una incidencia, se elaborará un informe específico que detalle la naturaleza del problema, las posibles causas, y las medidas adoptadas para corregirlo.
  - El responsable del Departamento de Tecnologías de la Información será el encargado de asegurar que todas las incidencias se gestionen y resuelvan antes de la siguiente prueba programada.
- **8.3.3. Mejora Continua:**
  - Los resultados de las pruebas y revisiones se utilizarán para actualizar y mejorar continuamente el BCP. Cualquier lección aprendida o mejora identificada será incorporada en la siguiente revisión del plan.
  - El Comité del SIG revisará todos los informes y aprobará cualquier cambio significativo en los procedimientos o configuraciones.

9. Comunicación en Situaciones de Crisis

9.1. Estrategia de Comunicación

Durante una crisis, la gestión efectiva de la comunicación es esencial para minimizar el impacto en la operación y mantener la confianza de todas las partes interesadas. Innovatech Consulting ha establecido un protocolo claro para manejar tanto las comunicaciones internas como externas, asegurando que la información sea oportuna, coherente y precisa.

Responsables de Comunicación:

- **Responsable Principal:** Director de Comunicación.
- **Apoyo:** Departamento de Recursos Humanos y Departamento de Tecnologías de la Información.

Canales de Comunicación:

- **Internos:** Correos electrónicos, plataforma de mensajería corporativa (Microsoft Teams), llamadas de conferencia.
- **Externos:** Comunicados de prensa, correos electrónicos a clientes y proveedores, actualizaciones en la página web corporativa.

El Director de Comunicación coordinará todas las comunicaciones, asegurándose de que los mensajes sean consistentes y que se transmitan rápidamente a todas las partes afectadas.

9.2. Protocolo de Comunicación Interna

Procedimiento de Notificación Interna:

1. **Detección de la Crisis:** Tan pronto como se identifique una crisis, el Director de Comunicación será notificado inmediatamente por el Comité de Gestión de Crisis.
2. **Notificación a la Alta Dirección:** El Director de Comunicación informará de inmediato a los miembros de la alta dirección, incluyendo al CEO, COO y otros directivos clave.
3. **Comunicación al Personal:** Una vez informada la alta dirección, se emitirá una comunicación a todo el personal a través de correo electrónico y la plataforma de mensajería corporativa, proporcionando detalles sobre la situación, las medidas que se están tomando y las acciones esperadas de los empleados.
4. **Actualizaciones Continuas:** Durante la crisis, se enviarán actualizaciones regulares para mantener a los empleados informados sobre los desarrollos y las decisiones que se vayan tomando.

Herramientas de Comunicación:

- **Correo Electrónico Corporativo:** Para comunicaciones formales y detalladas.
- **Microsoft Teams:** Para comunicaciones rápidas y coordinación en tiempo real.
- **Llamadas de Conferencia:** Para reuniones urgentes con la alta dirección y equipos operativos.

9.3. Comunicación con las Partes Externas

Procedimiento de Notificación Externa:

1. **Identificación de Afectados:** El Director de Comunicación, en coordinación con el Departamento de Ventas y el Departamento de TI, identificará a los clientes, proveedores, y otras partes interesadas que pueden verse afectados por la crisis.
2. **Elaboración de Mensajes:** Se prepararán mensajes específicos para cada grupo de partes interesadas. Estos mensajes incluirán un resumen de la situación, las acciones que se están tomando para mitigar el impacto, y cualquier otra información relevante.
3. **Distribución de Comunicados:**
    - **Clientes y Proveedores:** A través de correos electrónicos personalizados y llamadas directas si es necesario.
    - **Medios de Comunicación:** Se emitirá un comunicado de prensa si la situación lo requiere, y se actualizará la página web corporativa con la información pertinente.
    - **Redes Sociales:** En casos donde la crisis pueda afectar la reputación pública de Innovatech Consulting, se utilizarán las cuentas oficiales de redes sociales para gestionar la comunicación con el público en general.

Directrices de Comunicación:

- **Coherencia:** Asegurarse de que todos los mensajes sean coherentes en contenido y tono.
- **Transparencia:** Proveer información clara y honesta, evitando la especulación o la falta de datos.
- **Rapidez:** Emitir comunicaciones lo antes posible para evitar la difusión de rumores o información incorrecta.

10. Gestión de la Documentación del BCP

10.1. Control de Documentos

El proceso de control de la documentación del Plan de Continuidad de Negocio (BCP) en Innovatech Consulting está diseñado para garantizar que toda la documentación relevante esté siempre actualizada, accesible para las personas autorizadas y protegida contra accesos no autorizados. Este control se lleva a cabo a través de un sistema de gestión documental que asegura el registro de cada versión del BCP y su distribución controlada.

Elementos Clave del Control de Documentos:

- **Versionado:** Cada documento dentro del BCP tiene un número de versión que facilita el seguimiento de los cambios y actualizaciones.
- **Aprobación:** Antes de que cualquier documento se considere final y oficial, debe ser revisado y aprobado por el Comité de Seguridad de la Información.
- **Distribución Controlada:** La distribución del BCP y sus documentos relacionados se realiza únicamente a través de canales seguros y a personas autorizadas.

10.2. Revisión y Actualización de la Documentación

El BCP es un documento dinámico que debe revisarse y actualizarse regularmente para reflejar cambios en la organización, la tecnología o el entorno de amenazas. Innovatech Consulting ha establecido un ciclo de revisión formal para asegurar que el BCP se mantenga relevante y efectivo.

Ciclo de Revisión:

- **Frecuencia:** El BCP se revisa de manera anual o cada vez que se produce un cambio significativo en los procesos de negocio, en la estructura organizativa, o en las tecnologías empleadas.
- **Responsables de la Revisión:** La revisión es coordinada por el Responsable del Sistema de Gestión de la Información (SIG) en colaboración con el Responsable del Departamento de Tecnologías de la Información.
- **Proceso de Aprobación:** Los cambios propuestos en el BCP deben ser aprobados por la Alta Dirección de Innovatech Consulting antes de su implementación. Esta aprobación garantiza que los cambios reflejen la dirección estratégica y los riesgos actuales de la organización.

10.3. Almacenamiento y Acceso a la Documentación

Para garantizar la seguridad y disponibilidad de la documentación del BCP, Innovatech Consulting ha establecido políticas claras sobre el almacenamiento y acceso a estos documentos.

Almacenamiento:

- **Repositorio Principal:** Las versiones actuales del BCP se almacenan en un repositorio seguro en la plataforma NormaPro, accesible a través de la red interna de Innovatech Consulting.
- **Respaldo:** Se mantienen copias de respaldo de la documentación del BCP en un servidor seguro en la nube, específicamente en los servicios de Microsoft Azure, para garantizar la disponibilidad durante una crisis.

Acceso:

- **Acceso Normal:** Durante las operaciones normales, el acceso al BCP está restringido a las personas autorizadas, que incluyen la Alta Dirección, el Comité de Seguridad de la Información, y los responsables de la implementación del BCP.
- **Acceso durante Crisis:** En caso de activación del BCP, se proporcionará acceso inmediato a todas las partes involucradas, utilizando las credenciales de emergencia y los protocolos de seguridad establecidos.
- **Protección contra Accesos No Autorizados:** El acceso a los documentos está protegido mediante autenticación multifactor (MFA) y controles de permisos basados en roles, lo que garantiza que solo el personal autorizado pueda ver o modificar los documentos del BCP.

11. Análisis de Impacto en el Negocio (BIA).

11.1. Objetivo del BIA.

El Análisis de Impacto en el Negocio (BIA) es un proceso fundamental dentro del Plan de Continuidad de Negocio (BCP) que tiene como objetivo identificar y evaluar los efectos potenciales de una interrupción significativa en los procesos críticos de negocio. El BIA proporciona una comprensión clara de las prioridades de recuperación, permitiendo a Innovatech Consulting asignar recursos de manera eficiente y desarrollar estrategias efectivas para mitigar el impacto de tales interrupciones.

11.2. Identificación de Procesos Críticos.

La identificación de procesos críticos es el primer paso en el BIA, donde se evalúan todas las actividades de negocio para determinar cuáles son esenciales para la continuidad operativa. Estos procesos se identifican en función de su importancia para la organización y su dependencia de otros procesos, sistemas de TI, y recursos humanos. Se emplean herramientas como el análisis de impacto en el negocio y la evaluación de riesgos para priorizar estos procesos.

La prioridad se asigna basándose en criterios como la pérdida financiera potencial, la interrupción del servicio al cliente, y las implicaciones legales o regulatorias.

11.3. Evaluación de Impacto.

Una vez identificados los procesos críticos, se realiza una evaluación del impacto para determinar las consecuencias de su interrupción. Esta evaluación considera varios aspectos, incluyendo:

- **Impacto Financiero**: Pérdidas económicas directas e indirectas que podrían resultar de la interrupción.
- **Impacto Legal y Regulatorio**: Consecuencias legales y sanciones regulatorias por incumplimientos que podrían derivarse de la interrupción.
- **Impacto Operativo**: Efectos sobre la operación diaria de Innovatech Consulting, incluyendo la capacidad de cumplir con los compromisos de servicio.
- **Impacto en la Reputación**: Daños potenciales a la imagen y confianza del público en la organización.

Esta evaluación permite a Innovatech Consulting determinar los tiempos máximos de interrupción aceptables y definir los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO) para cada proceso crítico.

11.4. Resultados del BIA.

Los resultados del BIA identifican los procesos más críticos para Innovatech Consulting, así como las dependencias clave que sustentan estos procesos. Estos resultados sirven como base para el desarrollo de estrategias de continuidad y recuperación, asegurando que los recursos se asignen adecuadamente para proteger las actividades esenciales de la organización. Los procesos identificados se categorizan según su prioridad, y se desarrollan planes de contingencia específicos para cada uno, alineados con los tiempos de recuperación requeridos y las capacidades de la organización.

12. Gestión de Crisis.

12.1. Definición de Crisis.

En el contexto de Innovatech Consulting, una crisis se define como cualquier evento o serie de eventos que tienen el potencial de interrumpir

significativamente las operaciones normales de la empresa, afectando su capacidad para cumplir con sus obligaciones y objetivos críticos. Esto incluye, pero no se limita a, desastres naturales, fallos tecnológicos, violaciones de seguridad, o cualquier otra situación que amenace la continuidad del negocio, la seguridad de la información, o la reputación de la organización.

12.2. Comité de Gestión de Crisis.

El Comité de Gestión de Crisis es el grupo responsable de dirigir y coordinar la respuesta de Innovatech Consulting ante una crisis. La composición del comité incluye:

- **Director General**: Responsable de la toma de decisiones estratégicas.
- **Responsable del Sistema de Gestión de la Información (SIG)**: Asegura que se mantenga la seguridad de la información durante la crisis.
- **Responsable del Departamento de Tecnologías de la Información (TI)**: Gestiona los aspectos técnicos y garantiza la continuidad de los servicios tecnológicos.
- **Responsable de Comunicación**: Maneja las comunicaciones internas y externas durante la crisis.
- **Otros Miembros Clave**: Representantes de las áreas operativas críticas según la naturaleza de la crisis.

Las funciones del comité incluyen la evaluación de la situación, la toma de decisiones rápidas y bien fundamentadas, y la coordinación de todas las acciones necesarias para mitigar el impacto de la crisis.

12.3. Escalación y Toma de Decisiones.

El proceso de escalación de incidentes se inicia cuando un evento es identificado como potencialmente disruptivo para las operaciones normales. Este proceso sigue una serie de pasos estructurados:

1. **Detección y Evaluación Inicial**: El personal operativo detecta el incidente y realiza una evaluación inicial para determinar su gravedad.
2. **Notificación al Comité de Gestión de Crisis**: Si el incidente es evaluado como serio, se notifica de inmediato al Comité de Gestión de Crisis.

3. **Escalación Formal**: El comité evalúa el incidente y decide si debe ser escalado al nivel de crisis. En este punto, se activa el Plan de Continuidad de Negocio (BCP) si es necesario.
4. **Toma de Decisiones**: Las decisiones clave durante la gestión de la crisis son tomadas colectivamente por el comité, basado en la información disponible, el impacto previsto, y las mejores prácticas para la gestión de crisis.

12.4. Herramientas y Recursos para la Gestión de Crisis.

Innovatech Consulting dispone de una serie de herramientas y recursos diseñados para facilitar la gestión efectiva de crisis, incluyendo:

- **Sistemas de Comunicación de Emergencia**: Plataformas de mensajería instantánea, sistemas de notificación masiva y conferencias en línea para mantener la comunicación fluida entre los miembros del comité y el personal.
- **Documentación de Planes de Continuidad**: Acceso rápido a la versión más actualizada del BCP y otros documentos relevantes a través del repositorio en línea NormaPro.
- **Infraestructura Tecnológica Resiliente**: Uso de servicios en la nube (como Azure) para asegurar que los sistemas críticos permanezcan operativos durante la crisis.
- **Protocolos de Escalación**: Procedimientos claramente definidos para la escalación y respuesta ante incidentes.
- **Recursos Externos**: Contacto preestablecido con proveedores y servicios de soporte técnico para asistencia inmediata en caso de necesidad.

13. Recuperación Ante Desastres (DRP).

13.1. Introducción al DRP.

El Plan de Recuperación ante Desastres (DRP) es una parte integral del Plan de Continuidad de Negocio (BCP) de Innovatech Consulting, centrado específicamente en la restauración de sistemas de TI críticos y en la recuperación de operaciones tras la ocurrencia de un desastre significativo. Mientras que el BCP se ocupa de la continuidad general del negocio, el DRP se enfoca en la recuperación técnica, asegurando que los sistemas de información

y tecnológicos puedan ser restablecidos rápidamente para soportar las operaciones críticas.

13.2. Estrategias de Recuperación..

Las estrategias de recuperación definidas en el DRP de Innovatech Consulting se basan en la identificación de recursos esenciales y en la implementación de soluciones que aseguren la mínima interrupción de los servicios. Entre las estrategias específicas se incluyen:

- **Redundancia de Sistemas**: Implementación de sistemas de respaldo y redundancia en la infraestructura de TI, tanto en las instalaciones físicas como en la nube, para asegurar la disponibilidad continua de los servicios críticos.
- **Copia de Seguridad y Restauración**: Procedimientos automatizados para la realización de copias de seguridad periódicas, tanto en local como en la nube, con un enfoque en la capacidad de restaurar datos y sistemas con rapidez.
- **Ubicaciones Alternativas**: Preparación de sitios de recuperación alternativos que pueden ser activados en caso de que las instalaciones principales queden inutilizadas.

13.3. Prioridades de Recuperación.

La priorización de la recuperación de sistemas y servicios está basada en su criticidad para la continuidad del negocio. Innovatech Consulting ha definido las siguientes prioridades:

1. **Sistemas de Gestión de la Información (SGSI)**: Restauración inmediata del SGSI para asegurar la protección de los datos sensibles y el cumplimiento de las normativas de seguridad.
2. **Plataforma de Servicios en la Nube (Azure)**: Reestablecimiento de la conectividad y operatividad de los servicios en la nube, que soportan la mayoría de las operaciones de Innovatech Consulting.
3. **Sistemas de Comunicación**: Restablecimiento de las herramientas de comunicación interna y externa para asegurar una coordinación efectiva durante y después de la recuperación.

4. **Sistemas Operativos Críticos**: Restauración de los servidores y sistemas operativos que sustentan las operaciones esenciales del negocio.

13.4. Procedimientos de Recuperación.

El DRP de Innovatech Consulting detalla un conjunto de procedimientos a seguir durante la recuperación, con responsabilidades claramente asignadas y los recursos necesarios identificados. Los pasos clave incluyen:

1. **Evaluación Inicial del Daño**: Inmediatamente después de un desastre, se realiza una evaluación del daño para determinar el alcance de la interrupción y planificar la recuperación.
2. **Activación de Sitios de Respaldo**: Si las instalaciones principales son inutilizables, se activa un sitio de respaldo predefinido, asegurando la continuidad de las operaciones desde una ubicación alternativa.
3. **Restauración de Copias de Seguridad**: Utilización de copias de seguridad recientes para restaurar los datos y sistemas críticos, priorizando aquellos que son esenciales para las operaciones del negocio.
4. **Validación de la Recuperación**: Una vez restaurados los sistemas, se llevan a cabo pruebas de validación para asegurar que todos los sistemas funcionen correctamente y que se cumplan los requisitos de seguridad.
5. **Informe de Recuperación**: Elaboración de un informe detallado que documente el proceso de recuperación, las lecciones aprendidas y las áreas de mejora para futuros incidentes.

15. Evaluación y Mejora Continua.

15.1. Auditorías del BCP.

El Plan de Continuidad de Negocio (BCP) de Innovatech Consulting está sujeto a un proceso riguroso de auditorías periódicas para asegurar su efectividad y adecuación a las necesidades cambiantes de la organización. Estas auditorías se realizan con la siguiente frecuencia y metodología:

- **Frecuencia**: Se llevarán a cabo auditorías internas cada seis meses, complementadas por auditorías externas anuales. Estas revisiones son fundamentales para identificar posibles deficiencias en el plan y asegurar que esté alineado con los estándares de la ISO 27001:2022.

- **Métodos de Auditoría**: Las auditorías incluyen la revisión documental del BCP, entrevistas con el personal clave involucrado en la gestión de crisis, y simulaciones de escenarios de desastre para evaluar la respuesta del plan en situaciones reales. Además, se revisarán los registros de pruebas y ejercicios previos para comprobar la implementación efectiva de las lecciones aprendidas.

15.2. Evaluación Post-Incidencia.

Después de cada incidente o simulacro significativo, Innovatech Consulting realiza una evaluación exhaustiva para identificar áreas de mejora en el BCP. Este proceso incluye:

- **Revisión de la Respuesta**: Se revisa la eficacia de la respuesta a incidentes, evaluando si se siguieron correctamente los procedimientos establecidos y si se lograron los objetivos de recuperación en los tiempos previstos.
- **Análisis de Desempeño**: Se realiza un análisis detallado del desempeño del equipo de gestión de crisis y de los sistemas técnicos, identificando cualquier fallo o desafío que haya surgido durante la respuesta.
- **Identificación de Mejoras**: Basándose en el análisis, se identifican mejoras específicas que podrían optimizar la respuesta en futuros incidentes, incluyendo ajustes en los procedimientos, mejoras en la comunicación, y actualizaciones tecnológicas.

15.3. Mejora Continua.

La mejora continua es un pilar fundamental en la gestión del BCP de Innovatech Consulting, asegurando que el plan evolucione en respuesta a los cambios en el entorno empresarial y tecnológico. Los mecanismos clave para esta mejora incluyen:

- **Revisión Regular del BCP**: Además de las auditorías, el BCP se revisa de manera regular para asegurar que siga siendo relevante y efectivo. Estas revisiones tienen lugar cada vez que hay un cambio significativo en la organización, como la adopción de nuevas tecnologías, cambios en la estructura organizativa, o actualizaciones en la normativa.
- **Feedback de las Partes Interesadas**: Se recopila de manera continua feedback de los empleados, clientes, y proveedores sobre la eficacia del

BCP, utilizando encuestas y reuniones de retroalimentación para identificar áreas de mejora.

- **Actualización del Plan**: Con base en las auditorías, evaluaciones post-incidencia, y feedback recibido, el BCP se actualiza regularmente. Estas actualizaciones son aprobadas por la alta dirección y comunicadas a todo el personal relevante para asegurar que todos estén al tanto de los cambios.
- **Capacitación y Formación Continua**: Se implementan programas de formación continua para el personal, asegurando que estén capacitados en las últimas actualizaciones del BCP y preparados para responder de manera efectiva en caso de crisis.

16. Plan de Capacitación y Sensibilización.

16.1. Objetivo de la Capacitación.

El objetivo del Plan de Capacitación y Sensibilización en Innovatech Consulting es asegurar que todos los empleados comprendan plenamente su rol y responsabilidades dentro del Plan de Continuidad de Negocio (BCP). La capacitación es esencial para:

- **Fomentar la Consciencia**: Garantizar que todo el personal esté consciente de los riesgos que pueden afectar la continuidad del negocio y de la importancia de estar preparado para responder de manera efectiva.
- **Habilitar la Respuesta Eficaz**: Equipar a los empleados con los conocimientos y habilidades necesarios para ejecutar sus responsabilidades dentro del BCP en caso de una interrupción o desastre.
- **Promover la Participación Activa**: Involucrar a todos los niveles de la organización en la gestión de la continuidad del negocio, asegurando que cada empleado, independientemente de su rol, sepa cómo puede contribuir a mantener la operación continua de la empresa.

16.2. Programa de Capacitación.

Innovatech Consulting ha desarrollado un programa integral de capacitación y sensibilización que incluye los siguientes componentes:

- **Simulacros Anuales**: Se llevan a cabo simulacros anuales de diferentes escenarios de interrupción para evaluar la preparación del personal y la

efectividad del BCP. Estos simulacros permiten a los empleados practicar sus roles y responsabilidades en un entorno controlado.

- **Talleres Prácticos**: Se organizan talleres periódicos que cubren aspectos específicos del BCP, como la recuperación de datos, la comunicación en crisis, y la gestión de desastres tecnológicos. Estos talleres están diseñados para proporcionar formación práctica y resolver dudas en tiempo real.
- **Cursos Específicos**: Se ofrecen cursos específicos sobre continuidad del negocio, seguridad de la información, y gestión de crisis, dirigidos tanto a nuevos empleados como a personal clave que desempeña roles críticos en el BCP. Estos cursos son obligatorios y se renuevan anualmente.
- **Sesiones de Sensibilización**: Para mantener la conciencia del BCP alta en toda la organización, se realizan sesiones de sensibilización periódicas, que incluyen charlas, boletines informativos y campañas internas que refuerzan la importancia de la continuidad del negocio.

16.3. Evaluación de la Eficacia de la Capacitación.

Para asegurar que las actividades de capacitación y sensibilización sean efectivas, Innovatech Consulting emplea las siguientes metodologías de evaluación:

- **Encuestas de Retroalimentación**: Después de cada sesión de capacitación o simulacro, se distribuyen encuestas para recopilar la opinión de los participantes sobre la claridad, relevancia y utilidad de la formación recibida. Esta retroalimentación se utiliza para ajustar y mejorar futuros programas.
- **Evaluaciones Post-Capacitación**: Se realizan pruebas y evaluaciones post-capacitación para medir la retención de conocimientos y la capacidad del personal para aplicar lo aprendido en situaciones reales. Los resultados de estas evaluaciones determinan si se requieren sesiones de refuerzo o capacitación adicional.
- **Monitoreo del Desempeño en Simulacros**: Durante los simulacros, se supervisa y evalúa el desempeño del personal en tiempo real, lo que permite identificar cualquier área de debilidad o falta de preparación. Los hallazgos se documentan y se incluyen en los informes de simulacro para informar futuras capacitaciones.

- **Revisión de Indicadores de Desempeño**: Se establecen indicadores clave de desempeño (KPI) para medir la efectividad general del programa de capacitación, tales como la tasa de asistencia, la tasa de éxito en evaluaciones, y la mejora en el tiempo de respuesta durante simulacros. Estos KPI son revisados regularmente por el Comité de Continuidad del Negocio para asegurar que el programa de capacitación cumpla con los objetivos establecidos.

Anexo al BCP: Integración de Azure en el Plan de Continuidad de Negocio (BCP) de Innovatech Consulting.

Índice

1. Introducción.

En el contexto de la transformación digital de Innovatech Consulting, Microsoft Azure juega un papel fundamental en la operación continua de nuestros servicios críticos. La integración de Azure en nuestro Plan de Continuidad de Negocio (BCP) garantiza que las operaciones puedan ser restauradas de manera rápida y eficiente en caso de un incidente o desastre que afecte nuestros sistemas. Este anexo detalla las estrategias, procedimientos y mecanismos específicos utilizados para asegurar la continuidad de los servicios críticos en Azure.

2. Servicios Críticos en Azure.

Microsoft Azure alberga varios servicios críticos para Innovatech Consulting, los cuales incluyen:

- **Servidores Virtuales (VMs)**: Utilizados para alojar aplicaciones empresariales esenciales.
- **Azure SQL Database**: Base de datos central para nuestras operaciones de negocio.
- **Azure Storage**: Almacenamiento de datos importantes, incluidas copias de seguridad y archivos esenciales.
- **Azure Active Directory (AAD)**: Servicio de gestión de identidades y accesos para los empleados.

Estos servicios son cruciales para la operativa diaria y, por tanto, se han implementado medidas específicas para garantizar su disponibilidad y recuperación en situaciones de crisis.

3. Estrategias de Recuperación en Azure.

Para garantizar la continuidad de los servicios alojados en Azure, Innovatech Consulting ha implementado las siguientes estrategias:

- **Azure Site Recovery (ASR)**: Este servicio permite la replicación de máquinas virtuales y servicios críticos hacia una región secundaria de Azure. En caso de una interrupción en la región primaria, los servicios pueden ser restaurados rápidamente desde la región secundaria.
- **Azure Backup**: Utilizado para realizar copias de seguridad automatizadas y programadas de bases de datos, servidores virtuales y otros datos críticos. Las copias de seguridad están almacenadas en varias

ubicaciones geográficas, asegurando la disponibilidad en caso de desastre.

- **Alta Disponibilidad (HA)**: Se han configurado soluciones de alta disponibilidad para bases de datos y aplicaciones críticas, permitiendo el failover automático en caso de fallos.

4. Pruebas y Validación.

La efectividad de las estrategias de recuperación en Azure es validada a través de pruebas periódicas. A continuación, se documentan las pruebas realizadas:

- **Pruebas de recuperación con Azure Site Recovery**: Realizadas trimestralmente para asegurar que las réplicas están actualizadas y pueden ser activadas en la región secundaria en un plazo aceptable.
- **Validación de copias de seguridad**: Verificación mensual de las copias de seguridad realizadas por Azure Backup, incluyendo la restauración de datos de prueba para confirmar su integridad.
- **Simulacros de desastre**: Anualmente, se realiza un simulacro completo de recuperación de desastres utilizando las soluciones de Azure, evaluando el tiempo de recuperación y la eficacia de los procedimientos.

5. Monitorización y actualización.

Para garantizar la efectividad continua de los servicios críticos en Azure, Innovatech Consulting utiliza las siguientes herramientas y procesos de monitorización:

- **Azure monitor**: Monitoriza en tiempo real el rendimiento y la disponibilidad de los servicios críticos, enviando alertas en caso de anomalías o interrupciones.
- **Revisiones periódicas**: Cada trimestre, el equipo de Tecnologías de la Información ha de revisar la configuración de recuperación de desastres, realizando ajustes según sea necesario para adaptarse a cambios en el entorno o en los requisitos del negocio.

6. Documentación y comunicación.

Durante una situación de crisis que afecte los servicios de Azure, se seguirán los siguientes procedimientos de comunicación:

- **Comunicación Interna**: El Departamento de Tecnologías de la Información notificará a la alta dirección y a los equipos operativos clave a través de correo electrónico y herramientas de mensajería instantánea. Las actualizaciones se proporcionarán a intervalos regulares hasta que se restaure la normalidad.
- **Comunicación con Clientes y Proveedores**: En caso de una interrupción significativa, se enviarán notificaciones a los clientes y proveedores mediante correos electrónicos predefinidos. Estas comunicaciones se gestionarán de manera centralizada por el equipo de comunicación de crisis.

7. Conclusión.

La integración de Microsoft Azure en el Plan de Continuidad de Negocio de Innovatech Consulting refuerza nuestra capacidad para responder a incidentes y desastres, asegurando la continuidad operativa de nuestros servicios críticos. Mediante el uso de herramientas avanzadas de Azure y la implementación de estrategias robustas de recuperación, Innovatech Consulting se posiciona para enfrentar con éxito los desafíos de un entorno digital cada vez más complejo y exigente.

ANEXO II: POLITICA DE SEGURIDAD DE LA INFORMACIÓN

	Nombre	Función	Fecha	Firma
Elaborado	Noemí M.	Responsable SIG	12/06/2024	
Revisado	JMG	Responsable SIG	12/06/2024	
Aprobado	JMG	Dirección	12/06/2024	

MODIFICACIONES VERSIÓN ANTERIOR:

Versión 01: Edición inicial.

Anexo II: Política de Seguridad de la Información de Innovatech Consulting.

1. Introducción.

Innovatech Consulting considera la información como un activo fundamental que debe ser protegido para garantizar la continuidad de las operaciones, cumplir con las normativas legales y mantener la confianza de nuestros clientes, socios y empleados. La presente Política de Seguridad de la Información establece las directrices y principios que rigen la protección de la información en todas sus formas, con el fin de prevenir su pérdida, alteración, acceso no autorizado o destrucción.

2. Objetivo.

El objetivo de esta política es establecer un marco para la gestión de la seguridad de la información que permita proteger la confidencialidad, integridad y disponibilidad de los datos. Además, busca asegurar que todos los empleados, contratistas y socios comerciales entiendan y cumplan con sus responsabilidades en cuanto a la seguridad de la información, alineándose con los requisitos de la norma ISO 27001:2022.

3. Alcance.

Esta política se aplica a todos los sistemas de información, redes, aplicaciones, procesos, empleados, contratistas y terceros que acceden, procesan, almacenan o transmiten información de Innovatech Consulting. El alcance incluye, pero no se limita a, información en formato digital, físico, comunicaciones electrónicas, datos en tránsito, en reposo y cualquier otro medio que pueda contener información relevante para la empresa.

4. Principios de Seguridad.

Innovatech Consulting se compromete a mantener los siguientes principios de seguridad en toda la organización:

- **Confidencialidad**: Asegurar que la información esté accesible únicamente a las personas autorizadas y que esté protegida contra accesos no autorizados.
- **Integridad**: Garantizar la exactitud y completitud de la información y los métodos de procesamiento, previniendo cualquier alteración no autorizada.

- **Disponibilidad**: Asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea necesario.

5. Roles y responsabilidades.

La responsabilidad de proteger la información recae sobre todos los miembros de Innovatech Consulting, desde la alta dirección hasta cada uno de los empleados, contratistas y terceros asociados. Las responsabilidades clave incluyen:

- **Alta Dirección**: Proveer liderazgo y recursos necesarios para la implementación y mantenimiento del SGSI, así como aprobar la Política de Seguridad de la Información.
- **Responsable del SGSI**: Coordinar la implementación de la política, monitorear su cumplimiento y gestionar incidentes de seguridad.
- **Responsables de departamentos**: Asegurar que los controles de seguridad se implementen efectivamente en sus respectivas áreas.
- **Empleados y contratistas**: Cumplir con las directrices establecidas, reportar cualquier incidente de seguridad y participar en las actividades de formación y concienciación.
- **Terceros y proveedores**: Cumplir con los requisitos de seguridad establecidos en los contratos y acuerdos de nivel de servicio (SLA).

6. Directrices de Seguridad.

Innovatech Consulting establece las siguientes directrices para la protección de la información:

- **Gestión de Acceso**: Implementar controles de acceso basados en el principio de privilegios mínimos, asegurando que solo el personal autorizado pueda acceder a la información crítica.
- **Clasificación y Manejo de la Información**: Establecer un sistema de clasificación de la información basado en su sensibilidad, con directrices claras sobre cómo debe ser manejada, almacenada y transmitida.

- **Gestión de Incidentes**: Todos los incidentes de seguridad de la información deben ser reportados y gestionados de manera oportuna para minimizar su impacto. Se implementará un proceso formal de respuesta a incidentes que incluirá la identificación, contención, erradicación, recuperación y lecciones aprendidas.
- **Protección física y ambiental**: Asegurar que los activos de información estén protegidos contra riesgos físicos y ambientales, incluyendo incendios, inundaciones, robos y otros desastres naturales o provocados.
- **Gestión de copias de seguridad**: Realizar copias de seguridad periódicas de la información crítica, almacenarlas en lugares seguros y verificar regularmente su integridad para garantizar que puedan ser restauradas en caso de desastre.
- **Control de proveedores**: Asegurar que los proveedores que manejan información de Innovatech Consulting cumplan con los estándares de seguridad establecidos por la empresa y que los riesgos asociados a terceros sean gestionados adecuadamente.
- **Seguridad en la Nube**: Implementar controles específicos para la protección de la información almacenada y procesada en la nube, asegurando que los servicios en la nube utilizados por Innovatech Consulting cumplan con los estándares de seguridad requeridos.

7. Cumplimiento y auditoría.

El cumplimiento de esta política es obligatorio para todos los miembros de Innovatech Consulting. Se realizarán auditorías periódicas para evaluar la eficacia del SGSI y el cumplimiento de la política. Cualquier incumplimiento de esta política puede dar lugar a sanciones disciplinarias, que pueden incluir la terminación del contrato laboral o contractual.

8. Formación y concienciación.

Innovatech Consulting proporcionará formación y programas de concienciación en seguridad de la información para todos los empleados y contratistas. Estos programas incluirán cursos, talleres y simulaciones de incidentes para garantizar que todos los

participantes comprendan sus roles y responsabilidades en la protección de la información.

9. Revisión y mejora continua.

Esta política será revisada al menos anualmente o en respuesta a cambios significativos en el entorno de la empresa o en las amenazas de seguridad. Innovatech Consulting se compromete a la mejora continua de su SGSI, adaptándose a las nuevas amenazas y cumpliendo con las mejores prácticas internacionales.

10. Aprobación y difusión.

Esta Política de Seguridad de la Información ha sido aprobada por la alta dirección de Innovatech Consulting y es efectiva a partir de su fecha de emisión. Será difundida a todos los empleados, contratistas y terceros relevantes, y estará disponible para su consulta en los canales internos designados.

ANEXO III: COMPLIANCE REPORT.

Microsoft Defender for Cloud

ISO 27001:2013 Compliance Report

8/20/2024 5:04:29 PM UTC

Table of contents

Executive summary

Introduction

Microsoft Defender for Cloud executes a set of automated assessments on your Cloud environment which can help provide evidence relevant to specific controls in a compliance framework or standard. This report summarizes the current status of those assessments on your environment, as they map to the associated controls. This report does not represent a complete compliance report for the standard, nor does it ensure compliance.

Compliance with ISO 27001:2013 controls

Your environment is compliant with 203 of 207 supported ISO 27001:2013 controls.

Coverage

Subscriptions: 1

resources: 2014

Subscription Name	Subscription ID
Microsoft Azure (institutodeinnovacion): #1042019	b53a4594-2da0-4884-9fa0-0e84bffae4f6

ISO 27001:2013 sections summary

The following is a summary status for each of the sections of the ISO 27001:2013. For each section, you will find the overall number of passing and failing controls, based on automated assessments run by Defender for Cloud.

A failing control indicates that at least one Defender for Cloud assessment associated with this control failed. A passing control indicates that all the Defender for Cloud assessments associated with this control passed. Note that status is shown only for supported controls, i.e. controls that have relevant Defender for Cloud assessments associated with them.

Area	Failed controls	Passed controls	
A.5. Information Security Policies	0	2	
A.6. Organization of Information Security	0	7	
A.7. Human Resources Security	0	6	
A.8. Asset Management	0	10	
A.9. Access Control	3	11	
A.10. Cryptography	0	2	
A.11. Physical And Environmental Security	0	15	
A.12. Operations Security	1	13	
A.13. Communications Security	0	7	
A.14. System Acquisition, Development And Maintenance	0	13	

A.15. Supplier Relationships	0	5	
A.16. Information Security Incident Management	0	7	
A.17. Information Security Aspects Of Business Continuity Management	0	4	
A.18. Compliance	0	8	
C.4. Context of the organization	0	4	
C.5. Leadership	0	16	
C.6. Planning	0	23	
C.7. Support	0	20	
C.8. Operation	0	3	
C.9. Performance Evaluation	0	23	
C.10. Improvement	0	4	

ISO 27001:2013 controls status

The following is a summary status for each supported control of the ISO 27001:2013. For each control, you will find the overall number of passing, failing and skipped assessment associated with that control.

A failing assessment indicates a Defender for Cloud assessment that failed on at least one resource in your environment. A passing Defender for Cloud assessment indicates an assessment that passed on all resources. A skipped assessment indicates an assessment that was not run, whether because this assessment type is disabled or because there are no relevant resources in your environment.

Note that status is shown only for supported controls, i.e. controls that have relevant Defender for Cloud assessments associated with them.

A.5. Information Security Policies

Control	Failed assessments	Passed assessments	Skipped assessments	
A.5.1.1. Policies for information security	0	0	41	
A.5.1.2. Review of the policies for information security	0	0	28	

A.6. Organization of Information Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.6.1.1. Information security roles and responsibilities	0	0	72	

A.6.1.2. Segregation of Duties	0	1	4	
A.6.1.3. Contact with authorities	0	0	2	
A.6.1.4. Contact with special interest groups	0	0	6	
A.6.1.5. Information security in project management	0	0	25	
A.6.2.1. Mobile device policy	0	0	13	
A.6.2.2. Teleworking	0	0	16	

A.7. Human Resources Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.7.1.1. Screening	0	0	3	
A.7.1.2. Terms and conditions of employment	0	0	24	
A.7.2.1. Management responsibilities	0	0	26	
A.7.2.2. Information security awareness, education and training	0	0	14	
A.7.2.3. Disciplinary process	0	0	2	
A.7.3.1. Termination or change of employment responsibilities	0	0	8	

A.8. Asset Management

Control	Failed assessments	Passed assessments	Skipped assessments	
A.8.1.1. Inventory of assets	0	0	2	
A.8.1.2. Ownership of assets	0	0	7	
A.8.1.3. Acceptable use of assets	0	0	2	
A.8.1.4. Return of assets	0	0	8	
A.8.2.1. Classification of information	0	1	4	
A.8.2.2. Labelling of information	0	0	4	
A.8.2.3. Handling of assets	0	0	26	
A.8.3.1. Management of removable media	0	0	6	
A.8.3.2. Disposal of media	0	0	2	
A.8.3.3. Physical media transfer	0	0	2	

A.9. Access Control

Control	Failed assessments	Passed assessments	Skipped assessments	
A.9.1.1. Access control policy	0	0	4	

A.9.1.2. Access to networks and network services	0	5	24	
A.9.2.1. User registration and de-registration	0	0	27	
A.9.2.2. User access provisioning	0	0	19	
A.9.2.3. Management of privileged access rights	1	5	27	
A.9.2.4. Management of secret authentication information of users	1	4	16	
A.9.2.5. Review of user access rights	1	3	13	
A.9.2.6. Removal or adjustment of access rights	0	2	15	
A.9.3.1. Use of secret authentication information	0	0	15	
A.9.4.1. Information access restriction	0	0	11	
A.9.4.2. Secure log-on procedures	0	2	15	
A.9.4.3. Password management system	0	7	15	
A.9.4.4. Use of privileged utility programs	0	0	9	
A.9.4.5. Access control to program source code	0	0	10	

A.10. Cryptography

Control	Failed assessments	Passed assessments	Skipped assessments	
A.10.1.1. Policy on the use of cryptographic controls	0	10	7	
A.10.1.2. Key Management	0	0	15	

A.11. Physical And Environmental Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.11.1.1. Physical security perimeter	0	0	8	
A.11.1.2. Physical entry controls	0	0	9	
A.11.1.3. Securing offices, rooms and facilities	0	0	5	
A.11.1.4. Protecting against external and environmental threats	0	0	9	
A.11.1.5. Working in secure areas	0	0	3	
A.11.1.6. Delivering and loading areas	0	0	5	
A.11.2.1. Equipment sitting and protection	0	0	1	
A.11.2.2. Supporting utilities	0	0	3	
A.11.2.3. Cabling security	0	0	4	
A.11.2.4. Equipment maintenance	0	0	9	

A.11.2.5. Removal of assets	0	0	6	
A.11.2.6. Security of equipment and assets off-premises	0	0	10	
A.11.2.7. Secure disposal or re-use of equipment	0	0	5	
A.11.2.8. Unattended user equipment	0	0	2	
A.11.2.9. Clear desk and clear screen policy	0	0	3	

A.12. Operations Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.12.1.1. Documented operating procedures	0	0	30	
A.12.1.2. Change management	0	0	27	
A.12.1.3. Capacity management	0	0	2	
A.12.1.4. Separation of development, testing and operational environments	0	0	10	
A.12.2.1. Controls against malware	0	0	11	
A.12.3.1. Information backup	0	0	13	
A.12.4.1. Event Logging	0	4	49	

A.12.4.2. Protection of log information	0	0	8	
A.12.4.3. Administrator and operator logs	0	4	25	
A.12.4.4. Clock Synchronization	0	4	4	
A.12.5.1. Installation of software on operational systems	0	1	18	
A.12.6.1. Management of technical vulnerabilities	1	3	11	
A.12.6.2. Restrictions on software installation	0	1	18	
A.12.7.1. Information systems audit controls	0	0	1	

A.13. Communications Security

Control	Failed assessments	Passed assessments	Skipped assessments	
A.13.1.1. Network controls	0	0	40	
A.13.1.2. Security of network services	0	0	16	
A.13.1.3. Segregation of networks	0	0	17	
A.13.2.1. Information transfer policies and procedures	0	2	30	
A.13.2.2. Agreements on information transfer	0	0	11	

A.13.2.3. Electronic messaging	0	0	10	
A.13.2.4. Confidentiality or non-disclosure agreements	0	0	14	

A.14. System Acquisition, Development And Maintenance

Control	Failed assessments	Passed assessments	Skipped assessments	
A.14.1.1. Information security requirements analysis and specification	0	0	24	
A.14.1.2. Securing application services on public networks	0	0	32	
A.14.1.3. Protecting application services transactions	0	0	29	
A.14.2.1. Secure development policy	0	0	7	
A.14.2.2. System change control procedures	0	0	25	
A.14.2.3. Technical review of applications after operating platform changes	0	0	18	
A.14.2.4. Restrictions on changes to software packages	0	0	24	
A.14.2.5. Secure system engineering principles	0	0	5	
A.14.2.6. Secure development environment	0	0	10	

A.14.2.7. Outsourced development	0	0	28	
A.14.2.8. System security testing	0	0	8	
A.14.2.9. System acceptance testing	0	0	14	
A.14.3.1. Protection of test data	0	0	11	

A.15. Supplier Relationships

Control	Failed assessments	Passed assessments	Skipped assessments	
A.15.1.1. Information security policy for supplier relationships	0	0	6	
A.15.1.2. Addressing security within supplier agreement	0	0	24	
A.15.1.3. Information and communication technology supply chain	0	0	4	
A.15.2.1. Monitoring and review of supplier services	0	0	4	
A.15.2.2. Managing changes to supplier services	0	0	15	

A.16. Information Security Incident Management

Control	Failed assessments	Passed assessments	Skipped assessments	

A.16.1.1. Responsibilities and procedures	0	0	7	
A.16.1.2. Reporting information security events	0	0	14	
A.16.1.3. Reporting information security weaknesses	0	0	4	
A.16.1.4. Assessment of and decision on information security events	0	0	23	
A.16.1.5. Response to information security incidents	0	0	12	
A.16.1.6. Learning from information security incidents	0	0	13	
A.16.1.7. Collection of evidence	0	0	7	

A.17. Information Security Aspects Of Business Continuity Management

Control	Failed assessments	Passed assessments	Skipped assessments	
A.17.1.1. Planning information security continuity	0	0	11	
A.17.1.2. Implementing information security continuity	0	0	18	
A.17.1.3. Verify, review and evaluate information security continuity	0	0	3	
A.17.2.1. Availability of information processing facilities	0	0	17	

A.18. Compliance

Control	Failed assessments	Passed assessments	Skipped assessments	
A.18.1.1. Identification applicable legislation and contractual requirements	0	0	29	
A.18.1.2. Intellectual property rights	0	0	2	
A.18.1.3. Protection of records	0	0	15	
A.18.1.4. Privacy and protection of personally identifiable information	0	0	6	
A.18.1.5. Regulation of cryptographic controls	0	0	2	
A.18.2.1. Independent review of information security	0	0	2	
A.18.2.2. Compliance with security policies and standards	0	0	35	
A.18.2.3. Technical compliance review	0	0	5	

C.4. Context of the organization

Control	Failed assessments	Passed assessments	Skipped assessments	
C.4.3.a. Determining the scope of the information security management system	0	0	3	

C.4.3.b. Determining the scope of the information security management system	0	0	3	
C.4.3.c. Determining the scope of the information security management system	0	0	18	
C.4.4. Information security management system	0	0	5	

C.5. Leadership

Control	Failed assessments	Passed assessments	Skipped assessments	
C.5.1.a. Leadership and commitment	0	0	6	
C.5.1.b. Leadership and commitment	0	0	27	
C.5.1.c. Leadership and commitment	0	0	10	
C.5.1.d. Leadership and commitment	0	0	1	
C.5.1.e. Leadership and commitment	0	0	3	
C.5.1.f. Leadership and commitment	0	0	9	
C.5.1.g. Leadership and commitment	0	0	3	
C.5.1.h. Leadership and commitment	0	0	1	
C.5.2.a. Policy	0	0	4	

C.5.2.b. Policy	0	0	4	
C.5.2.c. Policy	0	0	22	
C.5.2.d. Policy	0	0	22	
C.5.2.e. Policy	0	0	4	
C.5.2.f. Policy	0	0	4	
C.5.2.g. Policy	0	0	1	
C.5.3.b. Organizational roles, responsibilities and authorities	0	0	2	

C.6. Planning

Control	Failed assessments	Passed assessments	Skipped assessments	
C.6.1.1.a. General	0	0	3	
C.6.1.1.b. General	0	0	3	
C.6.1.1.c. General	0	0	3	
C.6.1.1.d. General	0	0	3	
C.6.1.1.e.1. General	0	0	3	
C.6.1.1.e.2. General	0	0	3	
C.6.1.2.a.1. Information security risk assessment	0	0	2	
C.6.1.2.a.2. Information security risk assessment	0	0	2	

C.6.1.2.b. Information security risk assessment	0	0	1	
C.6.1.2.c.1. Information security risk assessment	0	0	2	
C.6.1.2.c.2. Information security risk assessment	0	0	2	
C.6.1.2.d.1. Information security risk assessment	0	0	2	
C.6.1.2.d.2. Information security risk assessment	0	0	2	
C.6.1.2.d.3. Information security risk assessment	0	0	2	
C.6.1.2.e.1. Information security risk assessment	0	0	2	
C.6.1.2.e.2. Information security risk assessment	0	0	2	
C.6.1.3.a. Information security risk treatment	0	0	1	
C.6.1.3.b. Information security risk treatment	0	0	1	
C.6.1.3.c. Information security risk treatment	0	0	1	
C.6.1.3.d. Information security risk treatment	0	0	1	
C.6.1.3.e. Information security risk treatment	0	0	1	
C.6.1.3.f. Information security risk treatment	0	0	1	
C.6.2.e. Information security objectives and planning to achieve them	0	0	2	

C.7. Support

Control	Failed assessments	Passed assessments	Skipped assessments	
C.7.1. Resources	0	0	7	
C.7.2.a. Competence	0	0	3	
C.7.2.b. Competence	0	0	1	
C.7.2.c. Competence	0	0	1	
C.7.2.d. Competence	0	0	1	
C.7.3.a. Awareness	0	0	3	
C.7.3.b. Awareness	0	0	3	
C.7.3.c. Awareness	0	0	3	
C.7.4.a. Communication	0	0	4	
C.7.4.b. Communication	0	0	4	
C.7.4.c. Communication	0	0	4	
C.7.4.d. Communication	0	0	4	
C.7.4.e. Communication	0	0	4	
C.7.5.2.c. Creating and updating	0	0	1	
C.7.5.3.a. Control of documented information	0	0	1	
C.7.5.3.b. Control of documented information	0	0	3	

C.7.5.3.c. Control of documented information	0	0	1	
C.7.5.3.d. Control of documented information	0	0	3	
C.7.5.3.e. Control of documented information	0	0	3	
C.7.5.3.f. Control of documented information	0	0	7	

C.8. Operation

Control	Failed assessments	Passed assessments	Skipped assessments	
C.8.1. Operational planning and control	0	0	21	
C.8.2. Information security risk assessment	0	0	3	
C.8.3. Information security risk treatment	0	0	4	

C.9. Performance Evaluation

Control	Failed assessments	Passed assessments	Skipped assessments	
C.9.1.a. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.b. Monitoring, measurement, analysis and evaluation	0	0	3	

C.9.1.c. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.d. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.e. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.1.f. Monitoring, measurement, analysis and evaluation	0	0	3	
C.9.2.a.1. Internal audit	0	0	1	
C.9.2.a.2. Internal audit	0	0	1	
C.9.2.b. Internal audit	0	0	1	
C.9.2.c. Internal audit	0	0	2	
C.9.2.d. Internal audit	0	0	1	
C.9.2.e. Internal audit	0	0	5	
C.9.2.f. Internal audit	0	0	1	
C.9.2.g. Internal audit	0	0	3	
C.9.3.a. Management review	0	0	5	
C.9.3.b. Management review	0	0	4	
C.9.3.c.1. Management review	0	0	6	
C.9.3.c.2. Management review	0	0	4	

C.9.3.c.3. Management review	0	0	4	
C.9.3.c.4. Management review	0	0	4	
C.9.3.d. Management review	0	0	3	
C.9.3.e. Management review	0	0	3	
C.9.3.f. Management review	0	0	3	

C.10. Improvement

Control	Failed assessments	Passed assessments	Skipped assessments	
C.10.1.d. Nonconformity and corrective action	0	0	1	
C.10.1.e. Nonconformity and corrective action	0	0	1	
C.10.1.f. Nonconformity and corrective action	0	0	3	
C.10.1.g. Nonconformity and corrective action	0	0	3	

ANEXO IV: PLAN DE ACCIÓN FORMATIVA.

1. Introducción.
2. Objetivos de la formación.
3. Contenidos de la Formación.
4. Metodología.
5. Evaluación y seguimiento.

Anexo 1 de la acción formativa: Detalles del plan de formación en seguridad de la información.

1. Objetivo del plan de formación.

2. Duración de la formación.

4. Metodología.

5. Contenidos de la formación.

6. Materiales de Apoyo

7. Indicadores de Éxito

Anexo 2 de la acción formativa: Plan de seguimiento y evaluación del sistema de gestión de seguridad de la información (SGSI).

1. Objetivo del Plan de Seguimiento y Evaluación.

2. Ámbito de aplicación.

3. Metodología de seguimiento.

    3.1 Auditorías internas (bimestrales).

    3.2 Evaluaciones de riesgos (trimestrales).

    3.3 Revisión de incidentes y No Conformidades (mensual).

    3.4 Indicadores de Desempeño (KPIs).

4. Plan de mejora continua.

    4.1 Análisis de resultados.

    4.2 Implementación de Acciones Correctivas

    4.3 Retroalimentación de empleados.

5. Calendario de revisión.

6. Responsabilidades

ANEXO 3 de la acción formativa: Manual de buenas prácticas en seguridad de la información.

1. Introducción.
2. Objetivo.
3. Principios fundamentales de la seguridad de la información.
4. Buenas prácticas generales.
    - 4.1 Protección de contraseñas.
    - 4.2 Gestión de dispositivos.
    - 4.3 Uso del correo electrónico.
    - 4.4 Navegación segura.
    - 4.5 Almacenamiento y manejo de datos.
5. Buenas prácticas específicas por áreas.
    - 5.1 Gestión de accesos.
    - 5.2 Gestión de incidentes.
    - 5.3 Protección de la información en entornos físicos.
6. Buenas prácticas para la protección de la información en teletrabajo.
7. Cumplimiento con las Políticas de Seguridad de la Información.
8. Formación Continua.

ANEXO 4 de la acción formativa: Guía de identificación de amenazas.

1. Introducción.
2. Objetivo.
3. Definición de Amenaza.
4. Clasificación de las Amenazas.
    - 4.1 Amenazas Naturales.
    - 4.2 Amenazas de origen humano (accidentales).
    - 4.3 Amenazas de origen humano (intencionadas).
    - 4.4 Amenazas tecnológicas.
    - 4.5 Amenazas regulatorias y legales.
5. Proceso de Identificación de Amenazas

1. Introducción.

El desarrollo de una cultura de seguridad de la información en una organización es esencial para garantizar la protección de los activos informáticos y la confidencialidad, integridad y disponibilidad de la información. En Innovatech Consulting, como parte del cumplimiento de la norma ISO 27001, es fundamental que todo el personal tenga un conocimiento básico de las políticas, procedimientos y mejores prácticas en materia de seguridad de la información.

Esta formación ha sido diseñada para los 13 empleados de Innovatech Consulting, en el marco del plan de acción de seguridad, y responde a la necesidad de mitigar riesgos identificados en el SGSI. El objetivo es capacitar al personal para que comprendan sus responsabilidades en la protección de la información y sepan cómo actuar en situaciones que puedan comprometer la seguridad de los sistemas.

2. Objetivos de la formación.

a) Comprender los conceptos clave en seguridad de la información.

b) Familiarizarse con las políticas y procedimientos del Sistema de Gestión de la Seguridad de la Información (SGSI) implementado según ISO 27001.

c) Conocer las principales amenazas y vulnerabilidades a las que se enfrenta la empresa.

d) Saber cómo reaccionar ante incidentes de seguridad de la información.

e) Promover buenas prácticas para la protección de la información en el entorno laboral.

3. Contenidos de la Formación.

a. Conceptos fundamentales en Seguridad de la Información.

- **Confidencialidad**: Asegurar que la información solo esté disponible para aquellos que tienen acceso autorizado.
- **Integridad**: Garantizar la exactitud y confiabilidad de la información y los métodos de procesamiento.

- **Disponibilidad**: Asegurar que los usuarios autorizados tengan acceso a la información cuando la necesiten.

b. Políticas y procedimientos de seguridad en Innovatech Consulting.

- **Política de Seguridad de la información**: Explicación de la política global de seguridad adoptada en Innovatech, alineada con la ISO 27001.
- **Clasificación de la Información**: Cómo se clasifican los documentos y la importancia de aplicar controles adecuados a cada tipo de información.
- **Uso de dispositivos móviles y trabajo remoto**: Normas de seguridad para trabajar fuera de la oficina y uso de dispositivos móviles.
- **Control de Acceso**: Políticas para gestionar las credenciales y asegurar el acceso adecuado a la información y a los sistemas.
- **Política de contraseñas**: Recomendaciones sobre el uso seguro de contraseñas y sistemas de autenticación.

c. Amenazas comunes a la seguridad de la información.

- **Malware**: Tipos (virus, troyanos, ransomware) y cómo protegerse.
- **Phishing**: Identificación de correos electrónicos fraudulentos y otros intentos de suplantación de identidad.
- **Ingeniería Social**: Estrategias utilizadas por los atacantes para obtener información sensible mediante el engaño.
- **Pérdida de Datos**: Situaciones en las que la información crítica puede perderse o ser robada.

d. Reacción ante incidentes de seguridad.

- **Reportar incidentes**: Cómo y cuándo reportar un incidente de seguridad, como la pérdida de un dispositivo o la detección de un correo sospechoso.
- **Protocolo de actuación**: Explicación del proceso a seguir en caso de detectar un incidente de seguridad de la información.
- **Consecuencias de no cumplir con los procedimientos**: Impacto en la empresa y posibles sanciones legales y contractuales.

d. Buenas prácticas de seguridad en el entorno laboral.

- **Protección física de equipos**: Cómo asegurar el entorno físico donde se manejan datos sensibles.
- **Uso seguro de internet y redes**: cómo evitar la exposición innecesaria a riesgos en internet.
- **Gestión segura de la información**: almacenamiento adecuado de datos y documentos, uso de herramientas de encriptación.
- **Respaldo regular de información**: importancia de los backups y cómo hacerlos de forma efectiva.

4. Metodología.

La formación será impartida en dos sesiones de 2 horas cada una, con un enfoque participativo y práctico. Se incluirán presentaciones con ejemplos reales, ejercicios de identificación de amenazas, simulaciones de incidentes y una evaluación final.

5. Evaluación y seguimiento.

Cada empleado deberá completar una evaluación al final del curso, con el objetivo de medir la comprensión de los conceptos tratados. Se realizarán también auditorías internas periódicas para verificar el cumplimiento de los empleados con las políticas y procedimientos del SGSI.

Anexo 1 de la acción formativa: Detalles del plan de formación en seguridad de la información.

1. Objetivo del plan de formación.

El objetivo del plan de formación es dotar a los empleados de Innovatech Consulting de los conocimientos necesarios en materia de seguridad de la información para garantizar la correcta implementación y mantenimiento del Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo con la norma ISO 27001. Se busca fortalecer las competencias del personal para mitigar los riesgos asociados al uso de los sistemas de información y promover una cultura de seguridad a todos los niveles de la organización.

2. Duración de la formación.

La formación constará de dos sesiones con una duración total de **4 horas**, distribuidas en **2 sesiones de 2 horas cada una**.

Fechas propuestas:

- Primera sesión: 8 de marzo 2024 (2 horas).
- Segunda sesión: 3 de mayo 2024 (2 horas).

3. Público objetivo.

La formación está destinada a los **13 empleados** de Innovatech Consulting, quienes tienen roles con acceso a la información crítica de la empresa y a los sistemas informáticos. Se incluyen tanto personal técnico como no técnico, dado que la protección de la información es responsabilidad de todos los miembros de la organización.

4. Metodología.

La formación seguirá una metodología teórico-práctica, con los siguientes componentes:

- **Presentaciones teóricas**: Explicación de los conceptos fundamentales de seguridad de la información, políticas y normativas aplicadas en Innovatech Consulting.
- **Casos prácticos**: Ejercicios de simulación de incidentes y actividades interactivas para la identificación de amenazas y vulnerabilidades.

- **Evaluación final**: Evaluaciones individuales para medir la comprensión de los conceptos abordados en las sesiones.

5. Contenidos de la formación.

La formación se estructurará en módulos que cubren los temas esenciales para los empleados de Innovatech Consulting:

Primera Sesión (2 horas):

1. **Conceptos Básicos de Seguridad de la Información (30 min).**
    - Definición y objetivos de la seguridad de la información.
    - Confidencialidad, integridad y disponibilidad de la información.
2. **Políticas de Seguridad y Procedimientos (40 min).**
    - Política de seguridad de Innovatech Consulting.
    - Clasificación y protección de la información.
    - Políticas de contraseñas, dispositivos móviles y teletrabajo.
3. **Amenazas Comunes y Cómo Protegerse (50 min).**
    - Tipos de malware (virus, troyanos, ransomware).
    - Phishing y técnicas de ingeniería social.
    - Seguridad en el uso de redes y dispositivos.

Segunda Sesión (2 horas).

4. **Gestión de Incidentes de Seguridad (40 min).**
    - Cómo identificar y reportar incidentes de seguridad.
    - Protocolo interno para el manejo de incidentes.
    - Ejemplo práctico de simulación de un incidente.
5. **Buenas Prácticas de Seguridad en el Entorno Laboral (50 min).**
    - Uso seguro de la red corporativa y protección física de equipos.
    - Gestión adecuada de la información (almacenamiento y eliminación).

- Políticas de backup y recuperación de datos.

6. **Evaluación Final y Discusión (30 min).**
   - Evaluación teórica/práctica para comprobar el conocimiento adquirido.
   - Discusión de dudas y cierre de la formación.

6. Materiales de Apoyo.

Se proporcionará a los empleados los siguientes materiales de apoyo para reforzar los conocimientos impartidos durante la formación:

1. **Manual de Buenas Prácticas en Seguridad de la Información**: Documento que resume las políticas clave y procedimientos de Innovatech Consulting.
2. **Guía de Identificación de Amenazas**: Material didáctico con ejemplos de ataques comunes y cómo reconocerlos.
3. **Presentaciones y Recursos Adicionales**: Las presentaciones utilizadas durante la formación estarán disponibles en formato digital para consulta posterior.
4. **Evaluaciones**: Exámenes y cuestionarios para verificar el conocimiento adquirido.

7. Indicadores de Éxito.

Para medir el impacto de la formación, se establecerán los siguientes indicadores:

1. **Tasa de asistencia**: Número de empleados que completan ambas sesiones.
2. **Resultado de las evaluaciones**: Nivel de comprensión demostrado en la evaluación final (objetivo ≥ 80% de respuestas correctas).
3. **Mejora en el reporte de incidentes**: Aumento en la detección y reporte de posibles amenazas o incidentes de seguridad tras la formación.
4. **Seguimiento post-formación**: Auditorías internas para verificar la correcta implementación de las políticas de seguridad de la información por parte de los empleados.

8. Responsable de la formación.

El responsable de la impartición de la formación será el **Departamento de Seguridad de la Información** de Innovatech Consulting, con la colaboración de auditores de seguridad externos, si se considera necesario.

Anexo 2 de la acción formativa: Plan de seguimiento y evaluación del sistema de gestión de seguridad de la información (SGSI).

1. Objetivo del Plan de Seguimiento y Evaluación.

El objetivo de este plan es garantizar que el Sistema de Gestión de Seguridad de la Información (SGSI) de Innovatech Consulting, basado en la norma ISO 27001, se mantenga efectivo y alineado con los objetivos estratégicos de la organización. El plan de seguimiento y evaluación tiene como finalidad medir el cumplimiento de los controles, identificar áreas de mejora y asegurar la sostenibilidad de las buenas prácticas en seguridad de la información a lo largo del tiempo.

2. Ámbito de aplicación.

Este plan cubre todas las áreas y procesos involucrados en la implementación y mantenimiento del SGSI de Innovatech Consulting, incluyendo:

- **Activos de Información**: Bases de datos, servidores, dispositivos móviles, y toda la infraestructura que soporte la información crítica de la empresa.
- **Personal**: Todos los empleados de Innovatech Consulting con acceso a la información confidencial o recursos críticos.
- **Procesos Clave**: Políticas de seguridad, gestión de incidentes, acceso a la información, auditorías y revisiones periódicas del SGSI.

3. Metodología de seguimiento.

El seguimiento del SGSI se realizará mediante una combinación de herramientas y enfoques, que incluyen:

3.1 Auditorías internas (bimestrales).

Se llevará a cabo una auditoría interna cada dos meses para evaluar la implementación de los controles de seguridad establecidos en la norma ISO 27001. Estas auditorías incluirán:

- Revisión de la documentación de políticas y procedimientos.
- Verificación del cumplimiento en las áreas de acceso a la información y gestión de incidentes.

- Comprobación de la actualización y protección de los activos de información.

Responsable: Departamento de Seguridad de la Información.

3.2 Evaluaciones de riesgos (trimestrales).

Cada tres meses, se realizará una evaluación de riesgos actualizada que revisará:

- Nuevas amenazas potenciales identificadas en el entorno de la organización.
- Cambios en la infraestructura tecnológica que puedan impactar en la seguridad.
- Vulnerabilidades detectadas en las auditorías o en el reporte de incidentes.

Responsable: Comité de Riesgos de Innovatech Consulting.

3.3 Revisión de incidentes y No Conformidades (mensual).

Mensualmente, se revisará el registro de incidentes de seguridad y cualquier no conformidad detectada en la implementación del SGSI, con el objetivo de:

- Analizar las causas raíz de los incidentes.
- Proponer acciones correctivas para evitar la repetición de los incidentes.
- Actualizar las políticas de seguridad en caso de ser necesario.

Responsable: Equipo de Respuesta a Incidentes de Seguridad.

3.4 Indicadores de Desempeño (KPIs).

Se establecerán indicadores clave de desempeño (KPIs) para monitorizar la efectividad de las medidas implementadas. Algunos de estos KPIs incluirán:

- **Tasa de incidentes de seguridad resueltos**: % de incidentes resueltos en un tiempo determinado.
- **Cumplimiento de políticas de acceso**: % de empleados que siguen los procedimientos de acceso a la información.
- **Resultados de auditorías internas**: Número de no conformidades detectadas en cada auditoría.
- **Tasa de éxito en evaluaciones de riesgos**: Porcentaje de mitigación de riesgos identificados en las evaluaciones trimestrales.

Responsable: Dirección de Innovatech Consulting con soporte del Departamento de Seguridad.

4. Plan de mejora continua.

El seguimiento y la evaluación continuos permitirán identificar áreas donde el SGSI puede ser optimizado. Para asegurar la mejora continua, se implementarán los siguientes procesos:

4.1 Análisis de resultados.

Después de cada auditoría interna, revisión de incidentes o evaluación de riesgos, se analizarán los resultados para determinar si las políticas y controles actuales son efectivos. Se evaluará si los riesgos están controlados y si las medidas preventivas son suficientes.

4.2 Implementación de Acciones Correctivas

En caso de identificar fallos en los controles o no conformidades, se definirán acciones correctivas concretas, que serán implementadas por los equipos responsables de cada área. Se realizará un seguimiento de la implementación para asegurar que las medidas tomadas resuelvan las deficiencias identificadas.

4.3 Retroalimentación de empleados.

La participación de los empleados será fundamental para la mejora continua. Se realizará una encuesta semestral para recoger la opinión de los empleados sobre la efectividad del SGSI y su comprensión de las políticas de seguridad. Esta retroalimentación permitirá ajustar las formaciones y los procedimientos si es necesario.

5. Calendario de revisión.

El plan de seguimiento se desarrollará siguiendo un calendario estructurado de actividades durante el año. A continuación, se presenta el cronograma:

- **Enero**: Auditoría interna de SGSI + Revisión de incidentes.
- **Febrero**: Evaluación trimestral de riesgos.
- **Marzo**: Auditoría interna de SGSI + Revisión de incidentes.
- **Abril**: Evaluación trimestral de riesgos.

- **Mayo**: Auditoría interna de SGSI + Revisión de incidentes.
- **Junio**: Evaluación trimestral de riesgos.
- **Julio - Diciembre**: Repetición del ciclo de actividades.

6. Responsabilidades

A continuación, se detallan las responsabilidades de los diferentes actores involucrados en el seguimiento y evaluación del SGSI:

- **Departamento de Seguridad de la Información**: Responsable de la implementación de auditorías internas, revisión de incidentes y cumplimiento de políticas de seguridad.
- **Comité de Riesgos**: Encargado de realizar las evaluaciones trimestrales de riesgos y reportar nuevas amenazas.
- **Equipo de Respuesta a Incidentes de Seguridad**: Responsable de la resolución de incidentes y la propuesta de acciones correctivas.
- **Dirección de Innovatech Consulting**: Responsable de revisar los resultados de los KPIs y asegurar que se cumplan los objetivos de seguridad de la información.

ANEXO 3 de la acción formativa: Manual de buenas prácticas en seguridad de la información.

1. Introducción.

El presente manual de buenas prácticas en seguridad de la información está diseñado para proporcionar a los empleados de Innovatech Consulting las pautas necesarias para garantizar la protección y seguridad de la información de la empresa, clientes y otros actores involucrados. Su implementación es clave para cumplir con los requisitos de la norma ISO 27001, y es una herramienta esencial para mitigar riesgos relacionados con la seguridad de la información.

2. Objetivo

El objetivo de este manual es concienciar a todos los empleados sobre la importancia de la seguridad de la información, definir procedimientos y comportamientos recomendados para prevenir incidentes de seguridad, y asegurar la integridad, confidencialidad y disponibilidad de la información gestionada por la empresa.

3. Principios fundamentales de la seguridad de la información.

La seguridad de la información en Innovatech Consulting se basa en tres pilares esenciales:

- **Confidencialidad**: Garantizar que la información sea accesible únicamente por personas autorizadas.
- **Integridad**: Asegurar que la información sea precisa y completa, y que no se modifique de manera no autorizada.
- **Disponibilidad**: Asegurar que la información y los sistemas estén disponibles cuando se necesiten.

4. Buenas prácticas generales.

4.1 Protección de contraseñas.

- Utiliza contraseñas seguras que incluyan letras mayúsculas, minúsculas, números y caracteres especiales. La longitud mínima recomendada es de 12 caracteres.

- Nunca compartas tus contraseñas, ni las escribas en lugares accesibles para otros.
- Cambia las contraseñas con regularidad, y nunca utilices la misma contraseña para múltiples cuentas.
- Habilita la autenticación multifactor (MFA) siempre que sea posible.

4.2 Gestión de dispositivos.

- Mantén tus dispositivos (ordenadores, móviles, tablets) siempre protegidos con contraseñas o PIN.
- Bloquea tu equipo si te alejas de tu puesto de trabajo, incluso por breves periodos de tiempo.
- Utiliza software antivirus y mantén todos los programas y sistemas operativos actualizados.
- No conectes dispositivos USB desconocidos a tu equipo. Usa únicamente medios de almacenamiento de fuentes confiables.

4.3 Uso del correo electrónico.

- No abras correos ni descargues archivos adjuntos de remitentes desconocidos o sospechosos.
- No compartas información sensible por correo electrónico a menos que sea estrictamente necesario y siempre mediante canales cifrados.
- Verifica los enlaces en los correos electrónicos antes de hacer clic, y si tienes dudas, comunícate con el remitente a través de un canal independiente.

4.4 Navegación segura.

- Evita acceder a sitios web que no cuenten con protocolos de seguridad (como HTTPS).
- No ingreses información personal o confidencial en sitios web no verificados.
- Usa conexiones seguras (VPN) cuando trabajes de forma remota y evita el uso de redes Wi-Fi públicas para acceder a información sensible.

4.5 Almacenamiento y manejo de datos.

- Asegúrate de almacenar los datos en lugares seguros, preferiblemente en servidores corporativos o soluciones de almacenamiento en la nube aprobadas.
- No utilices servicios de almacenamiento o compartición de archivos no autorizados por la empresa.
- Elimina correctamente la información que ya no sea necesaria, siguiendo los procedimientos de borrado seguro de la empresa.

5. Buenas prácticas específicas por áreas.

5.1 Gestión de accesos.

- Solicita y utiliza únicamente los permisos de acceso necesarios para desempeñar tu función. Evita acceder a sistemas o áreas de información que no sean pertinentes para tu trabajo.
- Revisa periódicamente tus permisos de acceso y notifica si detectas accesos innecesarios o no autorizados.
- Asegúrate de cerrar las sesiones de usuario cuando termines de usar un sistema o al final del día.

5.2 Gestión de incidentes.

- Reporta inmediatamente cualquier incidente de seguridad, como el acceso no autorizado a información, pérdida de dispositivos o correos electrónicos sospechosos, al equipo de seguridad de Innovatech Consulting.
- Colabora en la mitigación de los incidentes siguiendo las indicaciones de los equipos de TI y seguridad.

5.3 Protección de la información en entornos físicos.

- Mantén tu entorno de trabajo limpio y seguro: guarda documentos sensibles en cajones o armarios cerrados, y no dejes información confidencial al alcance de terceros.
- Utiliza medidas de seguridad físicas (como tarjetas de acceso o claves) para acceder a áreas restringidas de la empresa.

- No dejes documentos impresos sin supervisión en impresoras, y destruye adecuadamente los documentos que ya no sean necesarios.

6. Buenas prácticas para la protección de la información en teletrabajo.

- Utiliza solo equipos autorizados y configurados por el departamento de TI de la empresa para el trabajo remoto.
- Siempre conecta a la red corporativa mediante VPN.
- Mantén las videollamadas y conferencias en entornos privados para evitar que terceros puedan escuchar información sensible.
- Evita almacenar información confidencial localmente en tu equipo. Usa servicios de almacenamiento en la nube autorizados por la empresa.

7. Cumplimiento con las Políticas de Seguridad de la Información.

Todos los empleados de Innovatech Consulting deben familiarizarse y cumplir con las políticas de seguridad de la información de la empresa. El incumplimiento de estas políticas puede resultar en sanciones y comprometer la seguridad de la organización.

8. Formación Continua.

Innovatech Consulting proporcionará formación periódica sobre seguridad de la información para mantener a los empleados actualizados sobre las nuevas amenazas y mejores prácticas. Es importante que todos los empleados asistan y participen activamente en estas formaciones.

Firma de Compromiso.

A continuación, todos los empleados deberán firmar este documento para confirmar que han leído, comprendido y se comprometen a seguir las buenas prácticas en seguridad de la información.

Empleado:_____

Fecha: _____

ANEXO 4 de la acción formativa: Guía de identificación de amenazas.

1. Introducción.

La identificación de amenazas es un proceso fundamental dentro de la gestión de riesgos de la seguridad de la información. Este documento tiene como objetivo proporcionar una guía estructurada para identificar, documentar y clasificar las amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información gestionada por Innovatech Consulting.

La identificación de amenazas es un paso clave dentro del ciclo de gestión de riesgos y está alineada con los requisitos de la norma ISO 27001. Esta guía servirá como referencia para los equipos de seguridad y otros empleados, asegurando una comprensión clara de los posibles riesgos y cómo abordarlos.

2. Objetivo.

El objetivo de esta guía es proporcionar un marco sistemático para identificar amenazas que puedan impactar los activos de información de Innovatech Consulting. Esto permitirá:

- Establecer un inventario de amenazas potenciales.
- Evaluar la probabilidad de ocurrencia y el impacto asociado.
- Priorizar las acciones correctivas o preventivas para mitigar dichas amenazas.
- Proporcionar una base sólida para la gestión de riesgos continua.

3. Definición de Amenaza.

Una amenaza es cualquier circunstancia o evento que puede explotar una vulnerabilidad de los sistemas de información, comprometiendo la confidencialidad, integridad o disponibilidad de los datos. Las amenazas pueden ser de diferentes tipos: naturales, accidentales o intencionadas, y pueden originarse tanto en el entorno interno como en el externo de la organización.

4. Clasificación de las Amenazas.

Las amenazas se pueden clasificar en diferentes categorías según su origen, naturaleza y objetivo. A continuación, se detallan las principales categorías que Innovatech Consulting debe tener en cuenta:

4.1 Amenazas Naturales.

- **Inundaciones**: Daños en instalaciones y equipos.
- **Incendios**: Pérdida de datos e interrupciones en las operaciones.
- **Fenómenos meteorológicos extremos**: Daños en infraestructuras y sistemas de comunicaciones.
- **Terremotos**: Interrupciones graves en la operativa y destrucción de activos físicos.

4.2 Amenazas de origen humano (accidentales).

- **Errores humanos**: Modificación o eliminación accidental de datos, errores de configuración de sistemas, etc.
- **Fallas en el suministro eléctrico**: Pérdida de acceso a los sistemas críticos, corrupción de datos, daños a hardware.
- **Fallas de software**: Errores en aplicaciones críticas o fallos en actualizaciones de software.

4.3 Amenazas de origen humano (intencionadas).

- **Acceso no autorizado (intrusiones)**: Acceso deliberado por parte de un atacante a información confidencial.
- **Ataques de malware**: Virus, gusanos, ransomware y otros códigos maliciosos que buscan dañar o comprometer la información.
- **Phishing**: Intentos de obtener información sensible como credenciales de acceso a través de técnicas de ingeniería social.
- **Robo de equipos**: Sustracción de dispositivos que contienen información crítica o confidencial.
- **Sabotaje o espionaje**: Intentos deliberados de dañar o acceder a los sistemas o datos corporativos con fines maliciosos.

4.4 Amenazas tecnológicas.

- **Fallos en sistemas o hardware**: Caída de servidores, pérdida de datos por fallos de hardware, o mal funcionamiento de redes.
- **Obsolescencia tecnológica**: Equipos o sistemas que no se actualizan adecuadamente, dejando vulnerabilidades abiertas.
- **Interrupciones en las telecomunicaciones**: Pérdida de acceso a Internet o fallas en las comunicaciones internas.

4.5 Amenazas regulatorias y legales.

- **No cumplimiento normativo**: Incumplimiento de leyes como la protección de datos (ej. GDPR) o regulaciones específicas del sector.
- **Violación de propiedad intelectual**: Uso inadecuado o no autorizado de software patentado o licencias de terceros.
- **Pérdida de registros legales**: Pérdida o corrupción de información sensible con implicaciones legales o financieras.

5. Proceso de Identificación de Amenazas.

El proceso de identificación de amenazas debe ser continuo y debe involucrar a todas las áreas relevantes de la empresa. A continuación, se describe un proceso estándar de identificación de amenazas:

5.1 Revisión de Activos.

El primer paso es identificar y clasificar todos los activos de información, incluidos hardware, software, datos, sistemas de comunicaciones y personal. Se debe tener en cuenta el valor de cada activo y su relevancia para las operaciones.

5.2 Análisis de vulnerabilidades.

Es importante identificar las vulnerabilidades asociadas a los activos, es decir, las debilidades que podrían ser explotadas por una amenaza. Estas vulnerabilidades pueden estar relacionadas con:

- Configuraciones incorrectas.
- Falta de actualizaciones o parches de seguridad.

- Capacitación inadecuada del personal.
- Ausencia de políticas de seguridad.

5.3 Identificación de posibles amenazas.

Con base en el análisis de activos y vulnerabilidades, se procede a identificar las posibles amenazas que podrían aprovechar esas debilidades. Este paso puede implicar:

- Revisión de incidentes pasados.
- Estudio de informes de amenazas actuales en el sector (ciberataques, desastres naturales).
- Consultas con expertos en seguridad de la información.

5.4 Priorización de amenazas.

Una vez identificadas, las amenazas se deben clasificar y priorizar en función de:

- **Probabilidad de ocurrencia**: Qué tan probable es que una amenaza se materialice.
- **Impacto potencial**: Qué tan graves serían las consecuencias para la empresa si una amenaza se materializa.

Las amenazas con mayor probabilidad de ocurrencia y mayor impacto deben ser priorizadas para la implementación de controles de seguridad.

6. Herramientas para la identificación de amenazas.

Para facilitar el proceso de identificación de amenazas, se recomienda el uso de las siguientes herramientas:

- **Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas)**: Para identificar amenazas tanto internas como externas.
- **Análisis de impacto en el negocio (BIA)**: Para evaluar cómo las amenazas pueden afectar las operaciones.
- **Cuestionarios de evaluación de riesgos**: Para identificar y documentar amenazas específicas a partir de la revisión de procesos y entrevistas con personal clave.

7. Ejemplos de amenazas específicas en Innovatech Consulting.

1. **Amenaza: Phishing.**
    - **Descripción**: Un atacante intenta engañar a un empleado para que revele credenciales a través de un correo electrónico falso.
    - **Impacto**: Acceso no autorizado a sistemas críticos y posible robo de datos.
    - **Medidas preventivas**: Capacitación regular en reconocimiento de ataques de phishing, implementación de filtros de correo.
2. **Amenaza: Incendio en las oficinas.**
    - **Descripción**: Un incendio destruye equipos críticos en las instalaciones.
    - **Impacto**: Pérdida de datos y de infraestructura clave.
    - **Medidas preventivas**: Sistemas de respaldo fuera de sitio, políticas de recuperación ante desastres.
3. **Amenaza: Ataque de ransomware.**
    - **Descripción**: Un malware bloquea el acceso a los sistemas de Innovatech hasta que se pague un rescate.
    - **Impacto**: Pérdida de datos y posibles pérdidas financieras.
    - **Medidas preventivas**: Copias de seguridad periódicas, control de acceso estricto, software antivirus actualizado.