Escuela Politécnica Superior de Jaén

Máster Universitario en Seguridad Informática

UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior (Jaén)

Trabajo Fin de Máster

PLANIFICACIÓN Y DISEÑO DE UN SERVICIO SEGURO EN LA NUBE

Alumno/a: **Varela López, Blas**

Tutor/a: Prof. D. José Ramón Balsas Almagro
Dpto.: Informática

Noviembre, 2023

Universidad de Jaén
Escuela Politécnica Superior de Jaén
Departamento de Informática

Don José Ramón Balsas Almagro, tutor del Trabajo Fin de Máster titulado: Planificación y diseño de un servicio seguro en la nube, que presenta Blas Varela López, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, noviembre de 2023

El alumno: Los tutores:

Blas Varela López José Ramón Balsas Almagro

Índice

1. Introducción....11
1.1. Motivación....11
1.2. Objetivo....11
1.3. Metodología aplicada....11
2. Servicio a desplegar....13
2.1. Descripción del servicio....13
2.2. Roles....14
2.3. Tecnologías iniciales del servicio....15
3. Aspectos de seguridad....16
3.1. Legislación aplicable....16
3.1.1. Protección de datos proactiva....16
3.1.2. Determinar el tipo y volumen de los datos....16
3.1.3. Registro de actividades de tratamiento....17
3.1.4. Consentimiento y deber de informar....18
3.1.5. Brechas de seguridad....19
3.2. Análisis de riesgos....19
3.2.1. Identificación de activos....20
3.2.2. Factores agravantes....23
3.2.3. Riesgo potencial....24
3.3. Requisitos de seguridad....27
4. Proveedor de servicios en la nube....30
4.1. Azure Virtual Network....30
4.2. Private Endpoint....30
4.3. Azure Virtual Machine Scale Sets....30
4.4. Azure Files....31
4.5. Azure Database for MySQL como servidor flexible....31
4.6. Azure Key Vault....33
4.7. Azure VPN Gateway....35
4.8. Azure Application Gateway....35
4.8.1. Balanceador de carga....36
4.8.2. Web Application Firewall....36
4.9. Azure Monitor....37
4.10. Microsoft Defender for Cloud....38
4.11. Microsoft Sentinel....39
5. Medidas de seguridad....40

5.1. Vulnerabilidades....40
5.2. Contraseñas....41
5.3. Comunicación con el servidor....41
5.4. Permisos de archivos....42
5.5. Seguridad en la base de datos....42
5.6. Medidas en el panel de administración de WordPress....43
5.7. Medidas en htaccess....43
5.8. Medidas en wp-config....44
5.9. Firewall....44
5.10. Seguridad por ocultación....46
5.11. Monitorización....46
5.12. Seguridad en las redes....47
5.13. Seguridad en los datos....47
5.14. Requisitos cubiertos....48
6. Arquitectura del sistema....49
6.1. Descripción de los componentes....49
6.2. Flujos de trabajo....57
7. Análisis de costes....59
7.1. Análisis de costes en producción....59
7.2. Análisis de costes del sistema de pruebas....59
8. Despliegue del sistema....61
8.1. Creación del Grupo de recursos y la red virtual....61
8.2. Creación de una dirección IP pública....65
8.3. Creación del Application Gateway....66
8.4. Creación de una cuenta de almacenamiento....70
8.5. Creación de recursos compartidos mediante NFS....72
8.6. Configuración de un punto de conexión privado....73
8.7. Creación de la base de datos....75
8.8. Creación del conjunto de máquinas virtuales....80
8.9. Configuración SSL en Application Gateway....87
8.10. Creación de un VPN Gateway....93
8.11. Configuración de reglas en Application Gateway....100
8.12. Configuración de la copia de seguridad de WordPress....104
8.13. Configuración y ejemplo de uso de WPSchoolPress....107
8.14. Configuración de IThemes Security....112
8.15. Configuración de WP Activity Log....115

8.16. Configuración de Microsoft Sentinel....118
9. Evaluación de la seguridad....123
9.1. Evaluación de restauración del sistema....123
9.2. Evaluación de seguridad de las contraseñas....126
9.3. Evaluación de privilegios mínimos....128
9.4. Evaluación de vulnerabilidades....129
9.5. Evaluación de logs....137
9.6. Subsanación de errores....143
9.6.1. Subsanación de errores de cabeceras HTTP....143
9.6.2. Subsanación de seguridad de las contraseñas....147
10. Conclusiones....149
Bibliografía....152
Apéndice I: Material complementario....157

Índice de figuras

Ilustración 1: Panel de WPSchoolPress 15
Ilustración 2: Activos esenciales 21
Ilustración 3: Activos de soporte I 22
Ilustración 4: Activos de soporte II 22
Ilustración 5: Activos de soporte III 23
Ilustración 6: Factores agravantes 24
Ilustración 7: Riesgo potencial 24
Ilustración 8: Niveles de criticidad [5] 25
Ilustración 9: Riesgo en activos de soporte 26
Ilustración 10: Pasos en la autenticación con Azure Key Vault [13] 34
Ilustración 11: Arquitectura de Application Gateway 36
Ilustración 12: Componentes de Azure Monitor 38
Ilustración 13: Funcionalidades de Microsoft Sentinel 39
Ilustración 14: Arquitectura propuesta 49
Ilustración 15: Panel de configuración de Application Gateway 50
Ilustración 16: Panel de configuración del conjunto de máquinas virtuales 52
Ilustración 17: Panel de configuración de discos del conjunto de máquinas virtuales 53
Ilustración 18: Panel de configuración de redes del conjunto de máquinas virtuales 53
Ilustración 19: Panel de configuración de opciones avanzadas del conjunto de máquinas virtuales 54
Ilustración 20: Panel de configuración de MySQL Flexible Server 55
Ilustración 21: Panel de configuración de redes del servidor flexible 56
Ilustración 22: Panel de configuración de seguridad del servidor flexible 56
Ilustración 23: Panel de configuración del VPN Gateway 57
Ilustración 24: Creación de un grupo de recursos 61
Ilustración 25: Datos básicos de la red virtual 62
Ilustración 26: Seguridad de la red virtual 62
Ilustración 27: Direcciones de la red virtual 63
Ilustración 28: Creación de la subred del Application Gateway 63
Ilustración 29: Creación de la subred del *back-end* 64
Ilustración 30: Red virtual y subredes creadas 64
Ilustración 31: Resumen red virtual 65
Ilustración 32: Datos básicos de la dirección IP 65
Ilustración 33: Preferencias de Dirección IP 66
Ilustración 34: Datos básicos del *Application Gateway* 67
Ilustración 35: Creación de reglas WAF 67
Ilustración 36: Dirección pública del *Application Gateway* 68
Ilustración 37: Creación de un grupo *back-end* 68
Ilustración 38: Configuración *back-end* en *Application Gateway* 68
Ilustración 39: Agente de escucha para HTTP 69
Ilustración 40: Regla de enrutamiento al *back-end* para HTTP 69
Ilustración 41: Creación de configuración de *back-end* 70
Ilustración 42: Resumen de configuraciones en Application Gateway 70
Ilustración 43: Datos básicos de una cuenta de almacenamiento 71
Ilustración 44: Redes de la cuenta de almacenamiento 71
Ilustración 45: Recuperación de los datos la cuenta de almacenamiento 72

Ilustración 46: Cifrados de archivos en la cuenta de almacenamiento....72
Ilustración 47: Recursos compartidos de archivos....73
Ilustración 48: Creación de un recurso compartido....73
Ilustración 49: Datos básicos de un punto de conexión privado....74
Ilustración 50: JSON de la cuenta de almacenamiento....74
Ilustración 51: Selección del subrecurso para el punto privado....74
Ilustración 52: Red virtual del punto de conexión privado....75
Ilustración 53: Creación de una zona DNS privada....75
Ilustración 54: Datos básicos de la base de datos....76
Ilustración 55: Configuración del proceso y almacenamiento....76
Ilustración 56: Credenciales de la base de datos....77
Ilustración 57: Creación de un punto de conexión privado....77
Ilustración 58: Configuración de red de la base de datos....78
Ilustración 59: Copias de seguridad en MySQL flexible server....78
Ilustración 60: Creación de la base de datos de Wordpress....79
Ilustración 61: Opciones de conexión de la base de datos....79
Ilustración 62: Conexión a la base de datos....79
Ilustración 63: Creación del usuario de la base de datos....79
Ilustración 64: Privilegios del usuario para la base de datos....79
Ilustración 65: Datos básicos de VMSS....80
Ilustración 66: Configuración Azure Spot....81
Ilustración 67: Configuración de disco de VMSS....81
Ilustración 68: Configuración de red de VMSS....82
Ilustración 69: Configuración de la interfaz de red para VMSS....82
Ilustración 70: Configuración escalado de VMSS....83
Ilustración 71: Opciones avanzadas en VMSS....83
Ilustración 72: Consola serie de las máquinas....84
Ilustración 73: Conexión a la máquina mediante SSH....85
Ilustración 74: Montaje del recurso compartido....85
Ilustración 75: Acceso a la web....85
Ilustración 76: Configuración de la cuenta de administración en Wordpress....86
Ilustración 77: Instalación de Wordpress terminada....86
Ilustración 78: Panel de administración de Wordpress....87
Ilustración 79: Generación de un certificado raíz....87
Ilustración 80: Generación de una solicitud de firma....88
Ilustración 81: Generación de un certificado firmado....88
Ilustración 82: Configuración agente de escucha HTTPS....89
Ilustración 83: Generación de un certificado pfx....89
Ilustración 84: Regla de enrutamiento HTTPS....90
Ilustración 85: Regla de enrutamiento HTTPS a *back-end*....90
Ilustración 86: Agente de escucha redirigido a puerto 443....90
Ilustración 87: Almacén de certificados en el servidor....91
Ilustración 88: Activación SSL en Apache....91
Ilustración 89: Configuración del *back-end* para HTTPS....92
Ilustración 90: Nombre del host en configuración de *back-end*....92
Ilustración 91: Estado del *back-end*....92
Ilustración 92: Acceso mediante HTTPS....93
Ilustración 93: Información del certificado....93

Ilustración 94: Subred de VPN Gateway 94
Ilustración 95: Datos básicos de VPN Gateway....95
Ilustración 96: Creación de certificado raíz en PowerShell 96
Ilustración 97: Creación de certificado cliente en PowerShell....96
Ilustración 98: Exportación de certificado cliente 97
Ilustración 99: Creación de certificado raíz en PowerShell 97
Ilustración 100: Certificado raíz generado para la VPN 98
Ilustración 101: Configuración punto a sitio 98
Ilustración 102: Direcciones y certificado del VPN....98
Ilustración 103: Descarga del cliente VPN....99
Ilustración 104: Cliente VPN....99
Ilustración 105: VPN instalado....99
Ilustración 106: Uso de Azure VPN 100
Ilustración 107: Conexión VPN realizada 100
Ilustración 108: Conexión SSH mediante IP privada 100
Ilustración 109: Reglas de Application Gateway....101
Ilustración 110: Regla personalizada en Application Gateway....101
Ilustración 111: Condiciones de regla personalizada....102
Ilustración 112: Regla personalizada habilitada....103
Ilustración 113: Modo prevención activado....103
Ilustración 114: Bloqueo del tráfico desde Application Gateway 103
Ilustración 115: Límite de conexiones desde una dirección 104
Ilustración 116: Plugin para copias de seguridad....104
Ilustración 117: Configuración del plugin de copias de seguridad....105
Ilustración 118: Configuración de exclusiones en la copia de seguridad 106
Ilustración 119: Creación copia de seguridad de WordPress....106
Ilustración 120: Copia de seguridad creada....107
Ilustración 121: Copias de seguridad en Dropbox 107
Ilustración 122: Plugin WPSchoolPress....107
Ilustración 123: Importación de demo en WPSchoolPress 108
Ilustración 124: Panel de WPSchoolPress....108
Ilustración 125: Lista de alumnos 108
Ilustración 126: Datos del alumno 108
Ilustración 127: Información de la cuenta de alumno....109
Ilustración 128: Información de la cuenta de profesor 109
Ilustración 129: Información de la clase....109
Ilustración 130: Información de la asignatura 109
Ilustración 131: Información de la asistencia a clase 110
Ilustración 132: Información de examen....110
Ilustración 133: Notas de examen 110
Ilustración 134: Información de evento 111
Ilustración 135: Calendario del instituto 111
Ilustración 136: Información de la asistencia para el alumno 112
Ilustración 137: Plugin de IThemes Security....112
Ilustración 138: Selección rol de seguridad de IThemes Security 113
Ilustración 139: Política de contraseñas 113
Ilustración 140: Exploración de vulnerabilidades con IThemes Security 114
Ilustración 141: Resumen de vulnerabilidad con IThemes Security 114

Ilustración 142: Activación del segundo factor de autenticación 114
Ilustración 143: Vinculando dispositivo de doble factor de autenticación 115
Ilustración 144: Dispositivo de doble factor de autenticación vinculado 115
Ilustración 145: Segundo factor de autenticación requerido 115
Ilustración 146: Instalación de WP Activity Log 116
Ilustración 147: Cantidad de información de WP Activity Log 116
Ilustración 148: Páginas por defecto WP Activity Log 117
Ilustración 149: Tipo de retención de registros en WP Activity Log 117
Ilustración 150: Registros de WP Activity Log 117
Ilustración 151: Información de los registros de WP Activity Log 118
Ilustración 152: Creación de un área de trabajo de Log Analytics 119
Ilustración 153: Configuración de diagnóstico de Application Gateway 119
Ilustración 154: Selección de logs en configuración de diagnóstico 120
Ilustración 155: Selección de área de trabajo en Microsoft Sentinel 120
Ilustración 156: Centro de contenido en Microsoft Sentinel 121
Ilustración 157: Conector en Microsoft Sentinel 121
Ilustración 158: Reglas en Microsoft Sentinel 121
Ilustración 159: Resumen del conector de datos 122
Ilustración 160: Regla en Microsoft Sentinel 122
Ilustración 161: Máquina simulación de restauración 123
Ilustración 162: Copias de seguridad cargadas 124
Ilustración 163: Restauración de las copias de seguridad 124
Ilustración 164: Proceso de restauración de copias de seguridad 125
Ilustración 165: Plugins restaurados correctamente 125
Ilustración 166: Logs restaurados correctamente 125
Ilustración 167: Alumnos restaurados correctamente 126
Ilustración 168: Ejecución de Hashcat 127
Ilustración 169: Resultado de Hashcat 127
Ilustración 170: Intento de acceso a la lista de alumnos 128
Ilustración 171: Intento de acceso a lista de clases 129
Ilustración 172: Intento de acceso a recurso restringido 129
Ilustración 173: Intento de acceso al panel de administración 129
Ilustración 174: Zed Attack Proxy [42] 130
Ilustración 175: Configuración de un proxy en Firefox 131
Ilustración 176: Navegador interceptado por OWASP ZAP 131
Ilustración 177: Dynamic SSL Certificates en ZAP 132
Ilustración 178: Creación de un certificado raíz desde ZAP 132
Ilustración 179: Gestor de certificados en Firefox 133
Ilustración 180: Certificado importado en Firefox 133
Ilustración 181: Web interceptada por OWASP ZAP 134
Ilustración 182: Nueva regla personalizada en el WAF 135
Ilustración 183: Nuevo Escaneo en OWASP ZAP 136
Ilustración 184: Seguimiento del escaneo de OWASP ZAP 136
Ilustración 185: Alertas generadas por OWASP ZAP 137
Ilustración 186: Incidentes generados en Microsoft Sentinel 137
Ilustración 187: Incidentes generados con la regla personalizada 138
Ilustración 188: Información sobre el incidente en Microsoft Sentinel 138
Ilustración 189: Logs generados desde *Application Gateway* 139

Ilustración 190: Ejemplo de log generado por Application Gateway primera parte.....139
Ilustración 191: Ejemplo de log generado por Application Gateway segunda parte.....140
Ilustración 192: Logs de acceso en WordPress.....140
Ilustración 193: Ejemplo de log generado por WP Activity Log.....141
Ilustración 194: Ejemplo de eventos de IThemes Security.....142
Ilustración 195: Ejemplo de log en IThemes Security primera parte.....142
Ilustración 196: Ejemplo de log en IThemes Security segunda parte.....143
Ilustración 197: Reescrituras en Application Gateway.....143
Ilustración 198: Nuevo conjunto de reescritura en Application Gateway.....144
Ilustración 199: Reglas de reescritura en Application Gateway.....144
Ilustración 200: Ejemplo de regla de cabecera HTTP.....145
Ilustración 201: Lista de reglas de cabeceras HTTP.....146
Ilustración 202: Alertas tras los cambios en las cabeceras.....146
Ilustración 203: Plugin Password bcrypt.....147
Ilustración 204: Cálculo de fuerza bruta para MD5.....147
Ilustración 205: Cálculo de fuerza bruta para bcrypt.....148

Índice de tablas

Tabla 1: Información sobre el uso de datos de los alumnos 18
Tabla 2: Información sobre el uso de datos de los padres.....19
Tabla 3: Riesgos para los datos 26
Tabla 4: Riesgos para los servicios 26
Tabla 5: Requisitos de seguridad 29
Tabla 6: Requisitos cubiertos 48
Tabla 7: Análisis de costes mensual en producción 59
Tabla 8: Análisis de costes anual en producción 59
Tabla 9: Análisis de costes mensual en pruebas.....60
Tabla 10: Análisis de costes anual en pruebas.....60

1. Introducción

1.1. Motivación

Los servicios proporcionados por proveedores en la nube se están convirtiendo en una de las principales opciones para las organizaciones a la hora de desplegar sus servicios en Internet debido a la gran flexibilidad y a la reducción de costes que proporciona el uso de estos proveedores.

Con el aumento de las amenazas a los servicios web [1], es importante que las organizaciones protejan sus sistemas, lo que lleva a un estudio de los elementos aportados por los proveedores para llevar a cabo esta labor, además de los que ya se contemplarían, aunque el despliegue fuera local.

1.2. Objetivo

El propósito del trabajo es planificar y realizar el despliegue de un servicio utilizando la infraestructura proporcionada por algún proveedor en la nube, siguiendo para ello medidas de seguridad propuestas tras analizar los diferentes aspectos de seguridad del servicio y las herramientas proporcionadas por el proveedor en la nube, tras lo cual se evaluará la seguridad del despliegue realizado.

Los objetivos principales que se persiguen con lo anterior son los siguientes:

- Adquirir competencias que impliquen el desarrollo seguro de servicios en la nube.
- Analizar aspectos legales y de seguridad de un sistema en la nube.
- Estudiar, integrar y utilizar las tecnologías proporcionadas por el proveedor en la nube y por otros terceros que ayuden a la construcción de un sistema seguro.

1.3. Metodología aplicada

Los pasos a seguir para la realización del proyecto son los siguientes:

- Definir las características básicas del servicio a desplegar.
- Estudiar los aspectos de seguridad para el diseño del sistema.

- Estudiar y seleccionar un proveedor en la nube y servicios del mismo para la explotación del servicio propuesto.
- Determinar medidas de seguridad para la construcción del sistema.
- Diseñar la arquitectura del sistema.
- Analizar los costes de explotación del sistema propuesto.
- Desarrollo de un entorno de experimentación con el diseño propuesto.
- Evaluar la seguridad del sistema desplegado.

2. Servicio a desplegar

En este apartado se describe brevemente el servicio sobre el cual se realizará el estudio y despliegue.

2.1. Descripción del servicio

El servicio consistirá en un sistema de gestión para institutos. Constará de unos 1000 alumnos y unos 90 profesores, con lo que el sistema tendrá que ser capaz de soportar, al menos, este número de peticiones en horario lectivo. También se tendrá que tener en cuenta a los padres, puesto que estos podrán acceder al sistema, por lo tanto, si se produjera un pico de usuarios, con todos los disponibles, el sistema tendría que aguantar una carga de 2090 usuarios concurrentes.

El sistema de gestión constará de un panel que permitirá realizar diferentes acciones de gestión dependiendo del rol del usuario.

El sistema permitirá crear clases y asignaturas asignadas, añadir unos horarios a las clases y llevar un registro de asistencia de los alumnos y profesores, permitiendo a estos últimos añadir un motivo de ausencia de un alumno.

También permitirá añadir notas de asignaturas y exámenes de los estudiantes, pudiendo adjuntar un comentario a las mismas.

Se incluirá un calendario que permitirá observar los horarios de las clases, exámenes y otros eventos del instituto. Además, permitirá enviar notificaciones por correo, tanto a usuarios concretos como a grupos de usuarios.

Se podrá llevar una gestión de diferentes formas de transporte que el instituto oferta, como autobús público o privado del colegio, incluyendo las rutas y los detalles del conductor.

El profesor podrá llevar una gestión de la asistencia de los alumnos, pudiendo además añadir comentarios en caso de falta o modificarla si el alumno la justifica. Podrá mostrar las fechas de las clases y los exámenes, además de compartir las calificaciones a los alumnos mediante el sistema. En caso de querer contactar con

alumnos o padres o de avisar a todos los alumnos podrá hacerlo mediante envió de correos.

Los alumnos podrán hacer un seguimiento de los horarios de las asignaturas, las fechas de los exámenes, los eventos del colegio y el transporte disponible. Podrán registrar su asistencia a las clases y comprobar sus calificaciones, además de recibir diferentes avisos del profesor por correo.

El sistema permitirá a los padres hacer un seguimiento de sus hijos, pudiendo comprobar los horarios, sus asistencias y las calificaciones. Podrán recibir avisos por parte del profesor y comprobar las formas de transporte disponibles.

2.2. Roles

Dependiendo del rol el usuario podrá realizar diferentes acciones en el panel, los roles serán los siguientes:

- Administrador: Podrá añadir, editar o eliminar la información del colegio y de usuarios de los demás roles. Sera el encargado de crear las clases, las asignaturas, los horarios y los exámenes, añadir los eventos al calendario y crear los usuarios para los profesores, estudiantes y padres.
- Profesor: Podrá editar los miembros de las clases, ver información de todas las clases y asignaturas y ver los exámenes de sus asignaturas y clases. También podrá modificar las asistencias de sus clases y realizar notificaciones mediante correo a estudiantes, padres y otros profesores, además de asignar notas a los estudiantes de sus asignaturas y exámenes.
- Estudiante: Podrá ver información de los profesores, las clases, los estudiantes de sus clases, las asignaturas de sus clases, sus notas, el calendario de asistencia de sus clases, exámenes y eventos, información del transporte y registrar su asistencia a una clase.
- Padre: Podrá ver información de los profesores y diferente información de sus hijos, como clases, asignaturas, asistencia, exámenes, notas, horarios y asistencia.

2.3. Tecnologías iniciales del servicio

Se utilizará WordPress para crear el sitio web y el plugin *WPSchoolPress*[1] para construir el sistema de gestión, se ha seleccionado este plugin debido a su sencillez tanto en su instalación como en su uso, aportando las funcionalidades necesarias para el sistema, además es uno de los más utilizados con lo que se pueden encontrar varios tutoriales y documentación.

El plugin proporcionará un panel para realizar las acciones propuestas anteriormente, incluyendo una separación de las mismas dependiendo de los roles.

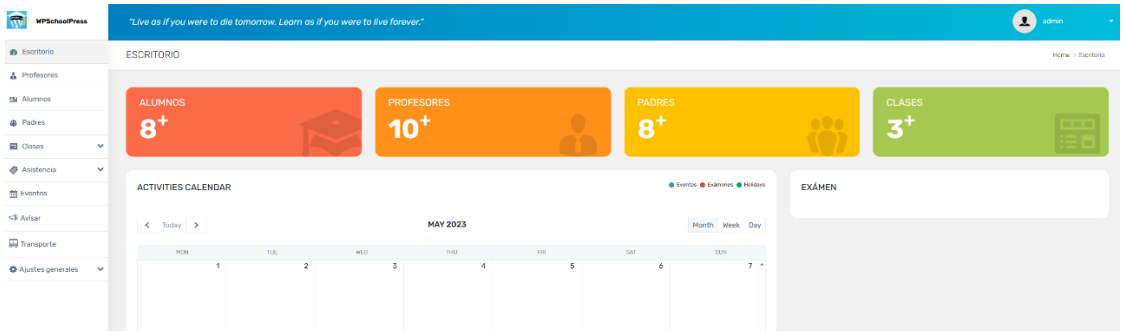


Ilustración 1: Panel de WPSchoolPress

[1] https://wpschoolpress.com/

3. Aspectos de seguridad

En esta sección se estudiarán los diferentes aspectos de seguridad que tendrán que tenerse en cuenta en el diseño del sistema.

3.1. Legislación aplicable

Deberá seguirse el Reglamento General de Protección de Datos (RGPD), el cual regula el tratamiento de la información de carácter personal en el territorio europeo. [2]

Para realizar su implantación se seguirán una serie de pasos descritos en las siguientes secciones. [3]

3.1.1. Protección de datos proactiva

Se debe ser proactivo en la protección de los datos, demostrando que se cumple con los diferentes principios que ayudan a la misma:

- Licitud, transparencia y lealtad al tratamiento de los datos.
- Limitación de la finalidad del tratamiento.
- Utilizar sólo los datos necesarios.
- Limitar la conservación de los datos.
- Asegurar la integridad y confidencialidad de los datos.

Para ello se seguirán una serie de requisitos de seguridad que serán descritos en las siguientes secciones.

3.1.2. Determinar el tipo y volumen de los datos

Se deben determinar qué tipos de datos se van a tratar y en qué volumen para poder saber las obligaciones a cumplir.

Se establecen dos categorías de datos personales:

- Datos personales básicos: Suponen un riesgo menor, se tratan, por ejemplo, de datos identificativos, académicos, laborales etc.

- Datos de categorías especiales: Se tratan de datos sensibles cuyo tratamiento conlleva un mayor riesgo, por ejemplo, datos relativos a salud, opiniones políticas, etc.

En el caso del sistema propuesto se manejarán los siguientes datos:

- Nombre y apellidos.
- Fecha de nacimiento.
- Dirección.
- Género.
- Calificaciones.
- Teléfono.
- Educación.
- Profesión.

Los datos que se tratarán, por lo tanto, entrarán en la categoría de datos personales básicos.

3.1.3. Registro de actividades de tratamiento

Se trata de un documento que registra la información relativa al tratamiento de datos que se van a realizar.

Este registro es obligatorio para empresas con más de 250 empleados o si se manejan datos de categorías especiales o a gran escala.

Su contenido para el sistema es el siguiente:

- Identidad del responsable:
- Finalidad: Contribuir de manera complementaria al desarrollo educativo.
- Categorías de interesados y de datos: Datos personales básicos.
- Destinatarios: Los datos podrán ser comunicados a empresas prestadoras de servicios en el centro o el Ministerio competente en materia de educación o a instituciones de la Unión Europea.
- Transferencias internacionales: No está prevista.
- Medidas de seguridad:

- Plazos de conservación de los datos:

3.1.4. Consentimiento y deber de informar

Para adaptar este reglamento se tendrá que obtener el consentimiento expreso de profesores, alumnos y padres para el tratamiento de sus datos personales. En el caso de los alumnos menores de catorce años el consentimiento tendrá que ser dado por los padres o los tutores.

Al tratarse de un centro educativo no se necesita un consentimiento directo, puesto que el tratamiento de los datos está justificado en el ejercicio de la función educativa. No obstante, se debe informar de forma clara cuando se recojan los datos de la matrícula, tanto de los usos que se puedan dar a estos en el centro, como de su uso en la plataforma de gestión. [4]

Por lo tanto, al recoger los datos en la matriculación del alumno, se tendrá que añadir una tabla como la siguiente para informar del uso de los datos en la plataforma:

Información sobre la protección de datos	
Responsable	Dirección de los centros y servicios educativos dependientes de la Consejería de Educación y Deporte (en caso de tratarse de un centro público).
Finalidad	Contribuir de manera complementaria al desarrollo educativo.
Base jurídica	Art. 6.1 e) del Reglamento (UE) 2016/679.
Destinatarios	Los datos podrán ser comunicados a empresas prestadoras de servicios en el centro o al Ministerio competente en materia de educación o a instituciones de la Unión Europea.
Transferencias internacionales	No está prevista la transferencia a terceros países.
Derechos	Derecho de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición, conforme a la norma vigente en materia de protección de datos.
Más información	Disponible en https://aepd.es/

Tabla 1: Información sobre el uso de datos de los alumnos

Si fuera preciso utilizar los datos para una finalidad diferente a la función educativa o la informada en el momento de la matrícula, se tendría que obtener un nuevo consentimiento expreso para esa finalidad.

Por lo tanto, con lo anterior, se tendría el consentimiento del usuario al completar este la matriculación y se habría informado del mismo.

En el caso de los padres, para poder utilizar la plataforma, tendrán que firmar un documento similar donde se les informará sobre el uso de sus datos en la plataforma.

Información sobre la protección de datos	
Responsable	Dirección de los centros y servicios educativos dependientes de la Consejería de Educación y Deporte (en caso de tratarse de un centro público).
Finalidad	Realizar un seguimiento del desarrollo educativo de su hijo.
Base jurídica	Art. 6.1 e) del Reglamento (UE) 2016/679.
Destinatarios	Los datos podrán ser comunicados a empresas prestadoras de servicios en el centro o al Ministerio competente en materia de educación o a instituciones de la Unión Europea.
Transferencias internacionales	No está prevista la transferencia a terceros países.
Derechos	Derecho de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición, conforme a la norma vigente en materia de protección de datos.
Más información	Disponible en https://aepd.es/

Tabla 2: Información sobre el uso de datos de los padres

3.1.5. Brechas de seguridad

Se debe informar a los usuarios de la plataforma en caso de que se produzca una brecha de seguridad en menos de 72 horas desde que se detectó.

Se informará mediante una notificación enviada por correo electrónico a los usuarios.

3.2. Análisis de riesgos

Este análisis determinara los posibles riesgos para la protección de los datos y servicios de la organización, así como la valoración de la probabilidad de que estos sucedan y el daño que causarían si se materializaran.

El proceso dará como resultado una información, determinando los peligros a los que se expone la organización. Esta información responderá fundamentalmente a las cuestiones:

- ¿Qué hay que proteger?
- ¿De qué o quién nos tenemos que proteger y por qué?
- ¿Cómo nos tenemos que proteger?

Se utilizará la Metodología de Análisis y Gestión de Riesgos de los Sistema de Información (MAGERIT v.3) para la realización del análisis. Para seguir esta metodología se hará uso de la herramienta PILAR[2] en su versión micro.

Esta metodología, al igual que la mayoría, trabaja sobre los siguientes elementos:

- Activos: Los elementos de la organización que deben protegerse, como los datos y servicios.
- Amenazas: Situaciones de la que deben protegerse los activos.
- Vulnerabilidades: Los aspectos que facilitan la materialización de las amenazas.

Estos tres elementos dan como resultado el riesgo en una organización. Mediante su análisis, intenta tratarse de manera que se consiga un equilibrio en el que no se gaste más para tratar un riesgo de lo que costaría recuperarse de la situación.

3.2.1. Identificación de activos

En primer lugar, se identificarán los activos implicados en el sistema de información, tanto los esenciales, que queremos proteger, como los de soporte.

Los activos esenciales incluyen la información y los servicios que queremos proteger, cada uno de los mismos se valorará en las distintas dimensiones, estas son:

- Confidencialidad: El daño que causaría que el activo fuera conocido por quien no debe.
- Integridad: El daño que causaría que el activo estuviera dañado o corrupto.
- Disponibilidad: El daño que causaría no poder hacer uso del activo.

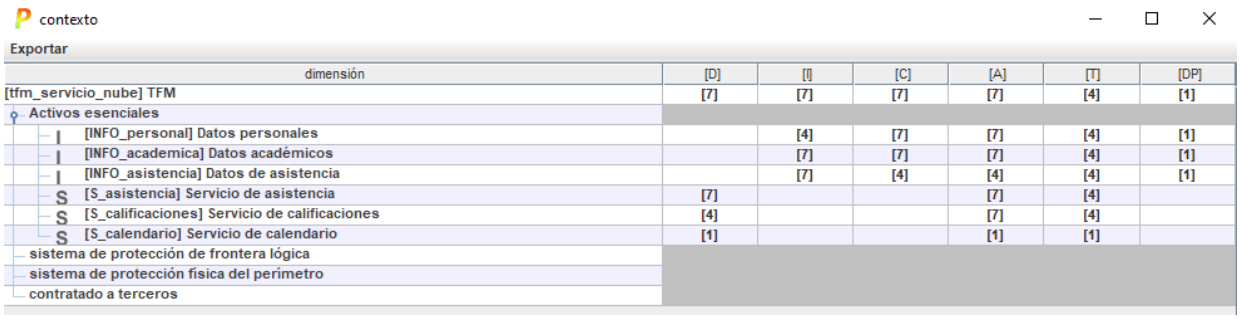
[2] https://pilar.ccn-cert.cni.es

- Autenticidad: El daño que causaría no saber quién ha hecho uso del activo.
- Trazabilidad: El daño que causaría no realizar un seguimiento de quien ha accedido al activo y que ha hecho con él.

La valoración de los activos se realiza con una escala de 0 a 10. En algunos casos un activo no podrá valorarse en alguna dimensión, por ejemplo, la confidencialidad suele ser típica de datos y por lo tanto no se valoraría en los servicios.

También existe un campo de datos personales (DP) en caso de utilizar la herramienta para hacer el seguimiento de los controles de privacidad y del reglamento.

Los activos esenciales del sistema y su valoración pueden verse en la ilustración inferior.



dimensión	[D]	[I]	[C]	[A]	[T]	[DP]
[tfm_servicio_nube] TFM	[7]	[7]	[7]	[7]	[4]	[1]
Activos esenciales						
[INFO_personal] Datos personales		[4]	[7]	[7]	[4]	[1]
[INFO_academica] Datos académicos		[7]	[7]	[7]	[4]	[1]
[INFO_asistencia] Datos de asistencia		[7]	[4]	[4]	[4]	[1]
[S_asistencia] Servicio de asistencia	[7]			[7]	[4]	
[S_calificaciones] Servicio de calificaciones	[4]			[7]	[4]	
[S_calendario] Servicio de calendario	[1]			[1]	[1]	
sistema de protección de frontera lógica						
sistema de protección física del perímetro						
contratado a terceros						

Ilustración 2: Activos esenciales

Como puede observarse, se han decidido los siguientes activos esenciales:

- Datos personales: Los diferentes datos almacenados de alumnos, profesores y padres.
- Datos académicos: Los datos de calificaciones de los alumnos.
- Datos de asistencia: Los datos de asistencia a clase de los alumnos.
- Servicio de asistencia: Permite a los alumnos registrar la asistencia a clase.
- Servicio de calificaciones: Permite a los alumnos consultar sus calificaciones y a los profesores publicarlas.
- Servicio de calendario: Permite ver las clases y eventos del instituto.

En las siguientes ilustraciones pueden verse los activos de soporte seleccionados.

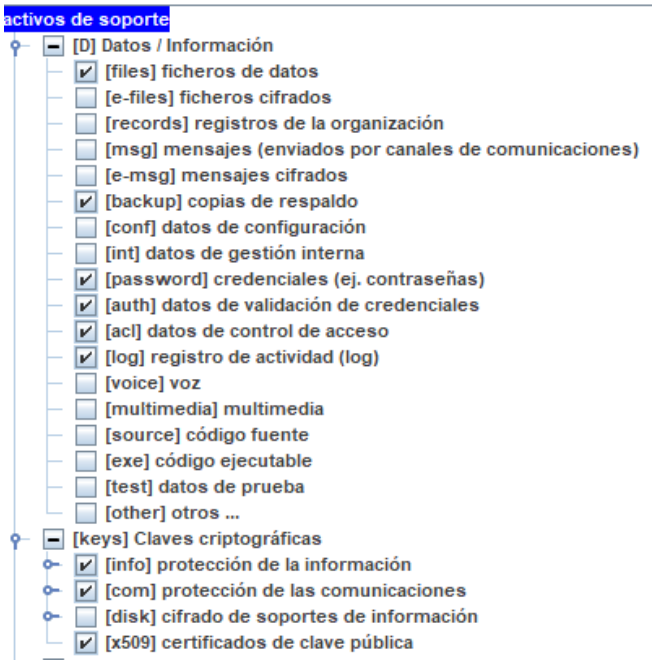


Ilustración 3: Activos de soporte I

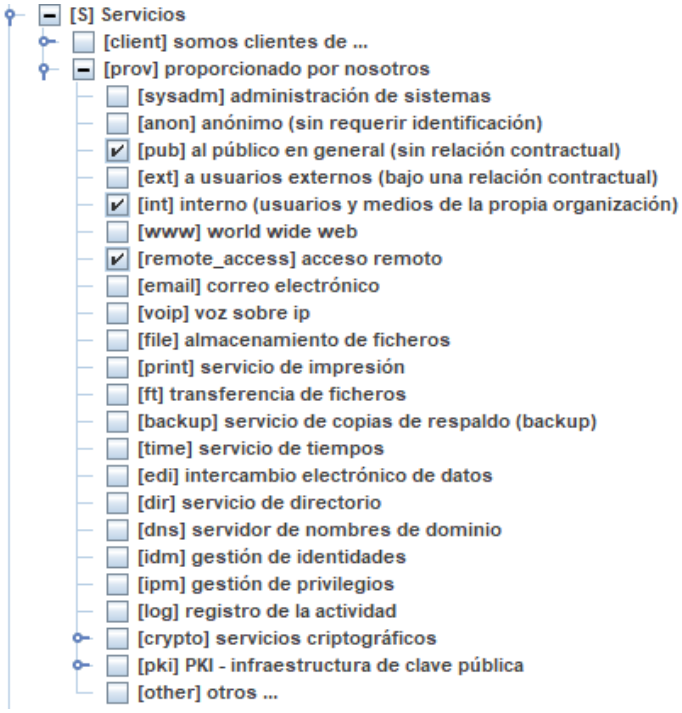


Ilustración 4: Activos de soporte II

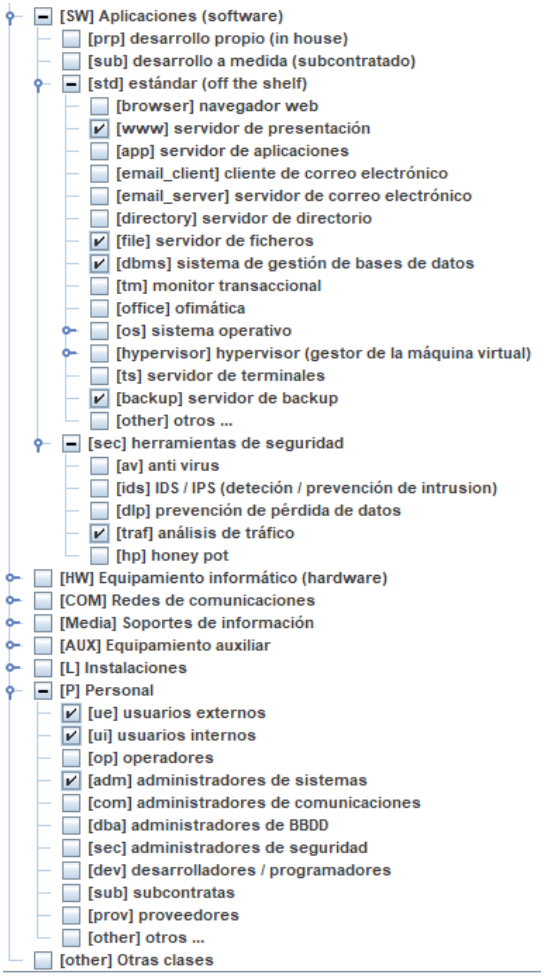


Ilustración 5: Activos de soporte III

3.2.2. Factores agravantes

Se añaden algunos factores que podrían aumentar o reducir el riesgo en el sistema, como posibles motivaciones o beneficios del atacante.

En este caso se identificará al atacante como público general (reducirá el riesgo), identificaremos atacantes que tendrían ánimo de causar daño y moderadamente interesados (modificar la asistencia), así como objetivos poco atractivos (aunque podrían querer modificar la asistencia, podría ser poco atractivo por la dificultad de llegar a realizarlo).

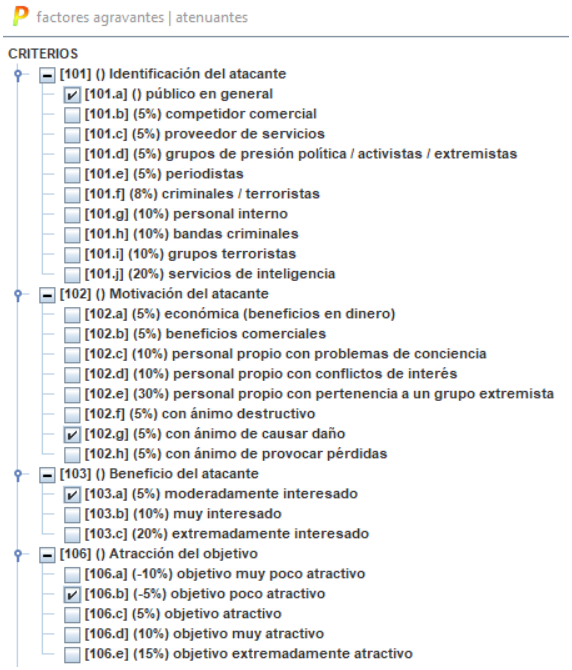
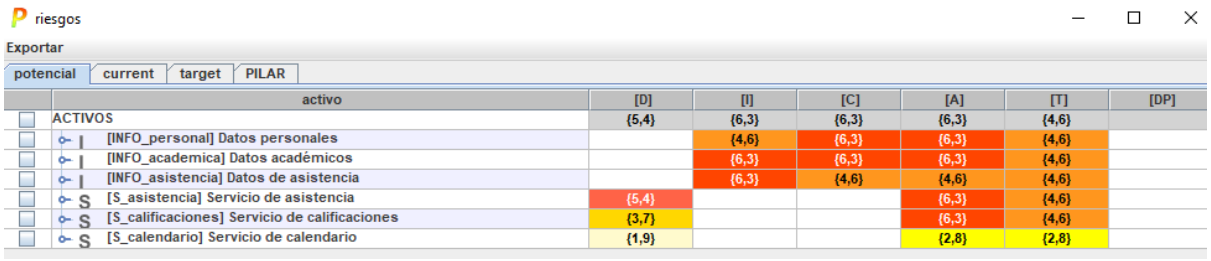


Ilustración 6: Factores agravantes

3.2.3. Riesgo potencial

La herramienta nos muestra una estimación de riesgo para los diferentes activos en sus dimensiones con un valor de 0.0 a 10.



activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{5,4}	{6,3}	{6,3}	{6,3}	{4,6}	
[INFO_personal] Datos personales		{4,6}	{6,3}	{6,3}	{4,6}	
[INFO_academica] Datos académicos		{6,3}	{6,3}	{6,3}	{4,6}	
[INFO_asistencia] Datos de asistencia		{6,3}	{4,6}	{4,6}	{4,6}	
[S_asistencia] Servicio de asistencia	{5,4}			{6,3}	{4,6}	
[S_calificaciones] Servicio de calificaciones	{3,7}			{6,3}	{4,6}	
[S_calendario] Servicio de calendario	{1,9}			{2,8}	{2,8}	

Ilustración 7: Riesgo potencial

Los niveles de criticidad de los valores serían los mostrados en la ilustración inferior.

Ilustración 8: Niveles de criticidad [5]

Por lo tanto, de esta manera puede observarse en qué activos tendríamos los mayores riesgos y en qué dimensiones. Para el caso de los datos, el riesgo sería el siguiente.

Activo	Integridad	Confidencialidad	Autenticidad	Trazabilidad
Datos personales	El riesgo, según la escala, sería muy alto, puesto que tendrían que mantenerse los datos de alumnos, profesores y padres, sin modificarse.	El riesgo sería crítico, puesto que solo el propietario de los datos debería conocerlos.	El riesgo sería crítico, puesto que solo el usuario debería poder acceder a los datos.	El riesgo es muy alto, puesto que se tiene que realizar un seguimiento de quien ha visto los datos de un alumno.
Datos académicos	El riesgo sería muy crítico, puesto que las calificaciones no deberían poder modificarse.	El riesgo sería crítico, puesto que solo el profesor y el alumno deberían conocer las calificaciones.	El riesgo sería crítico, puesto que solo el alumno y el profesor deberían poder acceder a las calificaciones.	El riesgo es muy alto, puesto que se tiene que realizar un seguimiento de quien ha visto las calificaciones del alumno.
Datos de asistencia	El riesgo sería muy crítico puesto que una modificación de este dato tendría consecuencias en, por ejemplo, las calificaciones de un alumno.	El riesgo sería muy alto, puesto que, a diferencia de lo anterior, aunque solo alumno, profesor y padres deberían conocer este dato, es algo que otros usuarios ya podrían llegar a conocer si son de la misma clase.	El riesgo sería muy alto, puesto que existen más personas que podrían llegar a acceder a estos datos.	El riesgo es muy alto, puesto que se tiene que realizar un seguimiento de quien ha visto la asistencia del alumno.

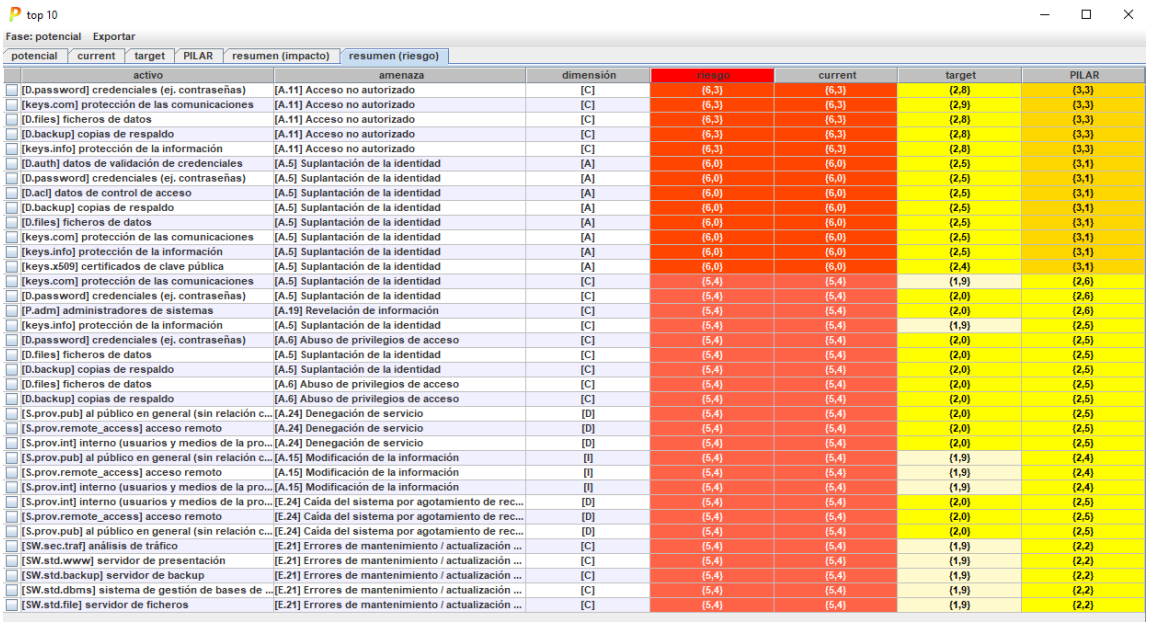
Tabla 3: Riesgos para los datos

Para el caso de los servicios:

Activo	Disponibilidad	Autenticidad	Trazabilidad
Servicio de asistencia	El riesgo es crítico, puesto que el servicio debería estar disponible siempre que se tenga que pasar la asistencia en una clase.	El riesgo es crítico, puesto que solo el alumno debería poder registrar su asistencia.	El riesgo es muy alto, puesto que se debería saber quién ha registrado la asistencia y cuando.
Servicio de calificaciones	El riesgo es medio, puesto que, si el servicio no está disponible, siempre podrían consultarse las calificaciones más tarde.	El riesgo es crítico, puesto que solo el profesor debería poder publicar calificaciones y solo el alumno y los padres deberían poder verlas.	El riesgo es muy alto, puesto que se debería saber quién ha publicado las calificaciones y quien las ha visto.
Servicio de calendario	El riesgo es bajo, puesto que el calendario solo muestra clases y eventos, con lo que no afectaría demasiado si el servicio no se encontrara disponible.	El riesgo es medio, puesto que cualquiera puede utilizar el calendario, aunque solo los administradores deberían poder editarlo.	El riesgo es medio, puesto que se debería hacer un seguimiento de las modificaciones en el calendario.

Tabla 4: Riesgos para los servicios

También puede verse un resumen del riesgo de los activos de soporte, esto incluye el riesgo del activo, en que dimensión se ve más afectado y cuál es la principal amenaza del activo.


top 10

Fase: potencial Exportar

potencial | current | target | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	riesgo	current	target	PILAR
[D.password] credenciales (ej. contraseñas)	[A.11] Acceso no autorizado	[C]	{6,3}	{6,3}	{2,8}	{3,3}
[keys.com] protección de las comunicaciones	[A.11] Acceso no autorizado	[C]	{6,3}	{6,3}	{2,9}	{3,3}
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]	{6,3}	{6,3}	{2,8}	{3,3}
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]	{6,3}	{6,3}	{2,8}	{3,3}
[keys.info] protección de la información	[A.11] Acceso no autorizado	[C]	{6,3}	{6,3}	{2,8}	{3,3}
[D.auth] datos de validación de credenciales	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,5}	{3,1}
[D.password] credenciales (ej. contraseñas)	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,5}	{3,1}
[D.acl] datos de control de acceso	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,5}	{3,1}
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,5}	{3,1}
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,5}	{3,1}
[keys.com] protección de las comunicaciones	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,5}	{3,1}
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,5}	{3,1}
[keys.x509] certificados de clave pública	[A.5] Suplantación de la identidad	[A]	{6,0}	{6,0}	{2,4}	{3,1}
[keys.com] protección de las comunicaciones	[A.5] Suplantación de la identidad	[C]	{5,4}	{5,4}	{1,9}	{2,6}
[D.password] credenciales (ej. contraseñas)	[A.5] Suplantación de la identidad	[C]	{5,4}	{5,4}	{2,0}	{2,6}
[P.adm] administradores de sistemas	[A.19] Revelación de información	[C]	{5,4}	{5,4}	{2,0}	{2,6}
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[C]	{5,4}	{5,4}	{1,9}	{2,5}
[D.password] credenciales (ej. contraseñas)	[A.6] Abuso de privilegios de acceso	[C]	{5,4}	{5,4}	{2,0}	{2,5}
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[C]	{5,4}	{5,4}	{2,0}	{2,5}
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[C]	{5,4}	{5,4}	{2,0}	{2,5}
[D.files] ficheros de datos	[A.6] Abuso de privilegios de acceso	[C]	{5,4}	{5,4}	{2,0}	{2,5}
[D.backup] copias de respaldo	[A.6] Abuso de privilegios de acceso	[C]	{5,4}	{5,4}	{2,0}	{2,5}
[S.prov.pub] al público en general (sin relación c...	[A.24] Denegación de servicio	[D]	{5,4}	{5,4}	{2,0}	{2,5}
[S.prov.remote_access] acceso remoto	[A.24] Denegación de servicio	[D]	{5,4}	{5,4}	{2,0}	{2,5}
[S.prov.int] interno (usuarios y medios de la pro...	[A.24] Denegación de servicio	[D]	{5,4}	{5,4}	{2,0}	{2,5}
[S.prov.pub] al público en general (sin relación c...	[A.15] Modificación de la información	[I]	{5,4}	{5,4}	{1,9}	{2,4}
[S.prov.remote_access] acceso remoto	[A.15] Modificación de la información	[I]	{5,4}	{5,4}	{1,9}	{2,4}
[S.prov.int] interno (usuarios y medios de la pro...	[A.15] Modificación de la información	[I]	{5,4}	{5,4}	{1,9}	{2,4}
[S.prov.int] interno (usuarios y medios de la pro...	[E.24] Caída del sistema por agotamiento de rec...	[D]	{5,4}	{5,4}	{2,0}	{2,5}
[S.prov.remote_access] acceso remoto	[E.24] Caída del sistema por agotamiento de rec...	[D]	{5,4}	{5,4}	{2,0}	{2,5}
[S.prov.pub] al público en general (sin relación c...	[E.24] Caída del sistema por agotamiento de rec...	[D]	{5,4}	{5,4}	{2,0}	{2,5}
[SW.sec.traf] análisis de tráfico	[E.21] Errores de mantenimiento / actualización ...	[C]	{5,4}	{5,4}	{1,9}	{2,2}
[SW.std.www] servidor de presentación	[E.21] Errores de mantenimiento / actualización ...	[C]	{5,4}	{5,4}	{1,9}	{2,2}
[SW.std.backup] servidor de backup	[E.21] Errores de mantenimiento / actualización ...	[C]	{5,4}	{5,4}	{1,9}	{2,2}
[SW.std.dbms] sistema de gestión de bases de ...	[E.21] Errores de mantenimiento / actualización ...	[C]	{5,4}	{5,4}	{1,9}	{2,2}
[SW.std.file] servidor de ficheros	[E.21] Errores de mantenimiento / actualización ...	[C]	{5,4}	{5,4}	{1,9}	{2,2}

Ilustración 9: Riesgo en activos de soporte

Las amenazas que intentarán mitigarse con los requisitos propuestos en la siguiente sección serán las siguientes:

- A.5: Suplantación de identidad.
- A.6: Abuso de privilegios de acceso.
- A.11: Acceso no autorizado.
- A.15: Modificación de la información.
- A.19: Revelación de información.
- E.21: Errores de mantenimiento / actualización.
- E.24: Caída del sistema por agotamiento de recursos.

3.3. Requisitos de seguridad

Se utilizará el estándar de verificación de seguridad de aplicaciones de OWASP (ASVS), para establecer una serie de requisitos de seguridad para el sistema propuesto, intentando cubrir los riesgos vistos en la sección anterior. [6]

Este estándar proporciona a los desarrolladores o propietarios una forma sencilla de evaluar el grado de confianza de las aplicaciones, los controles de seguridad que deben implantarse y la lista de requisitos para verificar la seguridad, que además puede utilizarse en un contrato.

La lista donde se recogen los requisitos que se han seleccionado para este caso muestra el identificador, la descripción del requisito, los niveles ASVS y su *Common Weakness Enumeration* (CWE), una lista con diferentes tipos de vulnerabilidades software y hardware. En la lista también se especificarán las amenazas que el requisito podría ayudar a mitigar o cubrir.

Los niveles de verificación de seguridad que se definen en el estándar son los siguientes:

- Nivel 1 para bajos niveles de garantía, se puede comprobar mediante *pentesting*.
- Nivel 2 para aplicaciones que contienen datos confidenciales, es el nivel recomendado.
- Nivel 3 para aplicaciones críticas que realizan transacciones de alto valor.

El sistema propuesto se encontraría por lo tanto en el nivel 2 al contener datos confidenciales.

El CWE, por su parte, indica el código de la debilidad común que el requisito especificado intenta cubrir.

Identificador	Descripción	Niveles	CWE	Amenazas
1.9.1	Verifique que la aplicación cifra las comunicaciones entre componentes, especialmente cuando estos componentes se encuentran en contenedores, sistemas, sitios o proveedores de nube diferentes.	L2, L3	319	A.11, A.15, A.19
2.1.1	Verifique que las contraseñas de los usuarios tienen al menos 12 caracteres de longitud.	L1, L2, L3	521	A.5, A.11
2.1.5	Verifique que los usuarios pueden cambiar su contraseña.	L1, L2, L3	620	A.5, A.11
2.1.6	Verifique que la funcionalidad de cambio de contraseña requiere la contraseña actual y la nueva del usuario.	L1, L2, L3	620	A.5, A.11
2.1.9	Verifique que no hay reglas de composición de contraseñas que limiten el tipo de caracteres permitidos. No debe haber ningún requisito para mayúsculas o minúsculas o números o caracteres especiales.	L1, L2, L3	521	A.5, A.11
2.4.1	Verifique que las contraseñas se almacenan en una forma tal que resisten ataques sin conexión. Las contraseñas deberán usar hash con salto mediante una derivación de llave de una sola vía aprobada o función de hash de contraseña. Las funciones derivación de llave y hash de contraseña toman una contraseña, un salto y un factor de costo como entrada al generar un hash de contraseña.	L2, L3	916	A.15, A.19
4.1.3	Verifique que existe el principio de privilegios mínimos: los usuarios solo deben poder acceder a funciones, archivos de datos, direcciones URL, controladores, servicios y otros recursos, para los que poseen una autorización especifica. Esto implica protección contra la suplantación y elevación de privilegios.	L1, L2, L3	285	A.5, A.6, A.11, A.15, A.19
4.3.1	Verifique que las interfaces administrativas utilicen autenticación multifactor adecuada para evitar el uso no autorizado.	L1, L2, L3	419	A.11

7.1.4	Verifique que cada evento de registro incluye la información necesaria que permitiría una investigación detallada de la escala de tiempo cuando se produce un evento.	L2, L3	778	A.5, A.6, A.11, A.15, E.21
7.3.1	Verifique que la aplicación registra eventos relevantes para la seguridad, incluidos los eventos de autenticación correctos y con errores, los errores de control de acceso, los errores de deserialización y los errores de validación de entrada.	L2, L3	778	A.5, A.6, A.11, A.15, E.21
8.1.5	Verifique que se realizan copia de seguridad periódicas de datos importantes y que se realizan pruebas de restauración de datos.	L3	19	A.15, E.21
7.1.3	Verifique que la aplicación registra eventos relevantes para la seguridad.	L2, L3	778	A.5, A.6, A.11, A.15, E.21
9.1.1	Verifique que TLS se utilice para toda la conectividad del cliente y que no recurra a comunicaciones inseguras no cifradas.	L1, L2, L3	319	A.11, A.15, A.19
9.2.2	Verifique que las comunicaciones cifradas, como TLS, se utilizan para todas las conexiones entrantes y salientes, incluidos los puertos de administración, monitoreo, la autenticación, la API o las llamadas a servicios web, la base de datos, la nube, el serverless, el mainframe, ya sean externos o de conexiones de asociados. El servidor no debe volver a protocolos inseguros o no cifrados.	L2, L3	319	
11.1.4	Verifique que la aplicación tenga controles anti-automatización para proteger contra llamadas excesivas, como exfiltración masiva de datos, solicitudes de lógica empresarial, carga de archivos o ataques de denegación de servicio.	L1, L2, L3	770	E.24
12.1.1	Verifique que la aplicación no aceptara archivos grandes que puedan llenar el almacenamiento o provocar una denegación de servicio.	L1, L2, L3	400	E.24
14.2.1	Verifique que todos los componentes estén actualizados, preferiblemente utilizando un comprobador de dependencias durante el tiempo de compilación.	L1, L2, L3	1026	E.21

Tabla 5: Requisitos de seguridad

Mediante estos requisitos quedarían cubiertas las amenazas propuestas en el apartado anterior.

4. Proveedor de servicios en la nube

Se utilizará la plataforma de Microsoft Azure para desplegar el servicio propuesto, se ha decidido utilizar esta plataforma para aumentar los conocimientos de la misma, puesto que no ha sido utilizada durante el transcurso del curso, además es una de las que más facilidades ofrece a los estudiantes, aportando la mayor cantidad de crédito gratuito tanto para la cuenta de estudiante como para las cuentas de prueba.

Para conseguir construir un sistema seguro se utilizarán una serie de recursos que esta plataforma proporciona. [7]

4.1. Azure Virtual Network

Se utilizará este recurso para crear una red privada que permitirá a los diferentes recursos comunicarse de forma segura entre sí, exponiendo sólo determinadas partes a Internet y aislando del mismo al resto de la red. [8]

Dentro de las redes privadas se pueden crear subredes donde agrupar los diferentes recursos bajo un mismo grupo de seguridad de red (NSG).

Los grupos de seguridad permiten filtrar el tráfico de red entre los diferentes recursos de la red virtual. Para este propósito, contienen reglas de seguridad que permiten o deniegan el tráfico de red, tanto entrante como saliente, pudiendo especificar un origen o un destino, un puerto y un protocolo.

4.2. Private Endpoint

Se trata de una interfaz de red que utiliza una dirección IP privada, disponible sólo dentro de la red virtual. Permite por lo tanto conectar de forma privada y segura los diferentes servicios utilizados dentro de la red privada, ya sean de Azure o de terceros. [9]

4.3. Azure Virtual Machine Scale Sets

Este recurso permite crear y administrar un grupo de máquinas virtuales, aumentando o disminuyendo el número de instancias de las máquinas dependiendo de la demanda o de forma manual.

Este servicio ofrece alta disponibilidad y resistencia en las aplicaciones al poder distribuir las máquinas entre diferentes zonas de disponibilidad. Mediante el escalado automático también ofrece escalabilidad al sistema al escalar según la demanda de recursos.

4.4. Azure Files

Este servicio ofrece recursos compartidos de archivos en la nube de forma administrada [10], estos se pueden obtener mediante lo siguiente:

- Protocolo de mensajes del servidor (SMB): Es un protocolo de Microsoft implementado en Windows cuyo propósito es el uso compartido de archivos.
- Protocolo *Network File System* (NFS): Es un protocolo de archivos distribuidos que permite a un cliente acceder a archivos de una red como si se tratase de almacenamiento local.
- API REST de Azure Files.

Una vez se monta la ruta de acceso del recurso compartido se pueden abrir y modificar los archivos como si estuvieran en el almacenamiento local, esto permitirá sincronizar varias máquinas para que compartan cierto contenido.

4.5. Azure Database for MySQL como servidor flexible

Se trata de un servicio de base de datos administrado, basado en MySQL, y listo para ser puesto en producción. [11]

La arquitectura flexible permite conseguir una alta disponibilidad y obtener controles de optimización de costos, pudiendo además iniciar o detener el servidor o modificar el nivel de proceso, aumentándolo o disminuyéndolo.

Este tipo de servidor ofrece tres opciones de implementación que influyen en los niveles de proceso:

- Flexible: Para cargas de trabajo que no necesitan la CPU continuamente.
- Uso general: Proporciona un equilibrio entre proceso y memoria con rendimiento de E/S escalable.

- Crítico para la empresa: Cargas de trabajo de alto rendimiento que requieren un procesamiento de transacciones más rápido y en paralelo.

La escalabilidad proporcionada es dinámica, con lo que los recursos utilizados por la base de datos pueden cambiarse en cualquier momento.

Este servicio crea automáticamente copias de seguridad y las almacena con redundancia local o geográfica, según se configure. Las copias de seguridad tienen un periodo de retención tras el cual se eliminan, por defecto son siete días y se puede configurar con un plazo entre 1 y 35 días. Las copias de seguridad son cifradas mediante AES de 256 bits.

Para realizar la conexión a la instancia de la base de datos se pueden utilizar dos opciones.

- Acceso privado: Se implementa en la red privada y solo se comunica mediante las direcciones IP privadas de la misma.
- Acceso público: Se implementa un punto de conexión público, el cual se trata de una DNS. Se debe establecer una lista de direcciones IP permitidas, las cuales podrán realizar la conexión.

El servicio también permite crear réplicas de lectura, el cual copia la base de datos a un servidor de solo lectura al que se podrá acceder para evitar cuellos de botella. Este servidor se actualiza de forma asíncrona mediante la replicación basada en la posición de los archivos *binlog*, una tecnología nativa de MySQL.

La base de datos usa un módulo criptográfico con validación FIPS 140-2, un estándar gubernamental de los Estados Unidos que define los requisitos mínimos de seguridad para los módulos criptográficos. Como se ha visto, se utiliza el cifrado AES de 256 bits, tanto para la base de datos, como para las copias de seguridad y los archivos temporales de las consultas. El servicio también cifra los datos en movimiento de la capa de transporte, admitiendo TLS 1.2 o superior por defecto.

Por último, el servicio integra características de alertas y supervisión de rendimiento. Las métricas generadas tienen una frecuencia de un minuto y 30 días de historial.

4.6. Azure Key Vault

Se trata de un servicio para el almacenamiento y acceso a secretos (claves API, contraseñas, certificados, etc.) de forma segura. Ofrece dos niveles de servicio, por un lado, el nivel estándar, que realiza el cifrado con una clave software, por otro lado, el nivel premium, que incluye claves protegidas mediante módulo de seguridad de hardware (HSM). [12]

Este servicio funciona junto a Azure Active Directory (Azure AD), para autenticar la identidad de cualquier entidad de seguridad que quiera acceder al servicio. Una entidad de seguridad puede representar lo siguiente:

- Un usuario que identifica a un individuo con un perfil en Azure Active Directory.
- Un grupo que identifica a un conjunto de usuarios creados en Azure Active Directory.
- Una entidad de servicio que identifica a una aplicación o servicio.

Para realizar la autorización se sigue el flujo presente en el diagrama al intentar realizar una operación, los pasos son los siguientes:

1. Un usuario o servicio solicita un token de acceso al Key Vault autenticándose mediante Azure AD.
2. Si la autenticación mediante Azure AD tiene éxito se le concede un token OAuth.
3. Se realiza una llamada a la API de Key Vault con el token obtenido.
4. El firewall de Key Vault determina si se cumple alguno de sus criterios, en ese caso permite la llamada.
5. Si se ha permitido la llamada, Key Vault verifica mediante Azure AD el token proporcionado.
6. Key Vault comprueba si la entidad tiene el permiso necesario para realizar la operación solicitada.
7. Se realiza la operación y se devuelve el resultado.

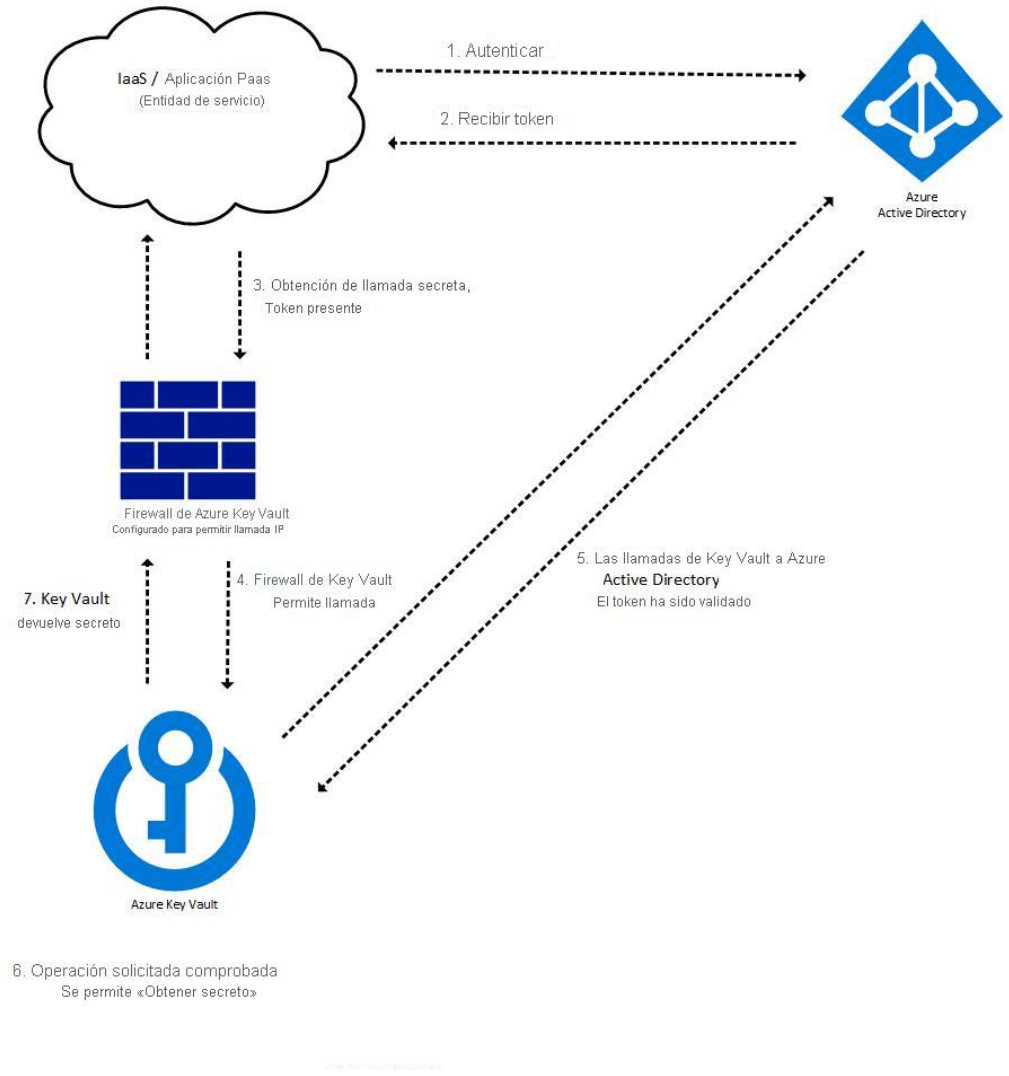


Ilustración 10: Pasos en la autenticación con Azure Key Vault [13]

Las operaciones que se pueden realizar son determinadas mediante el control de acceso basado en roles de Azure (RBAC de Azure), en la interfaz de administración, y mediante las directivas de acceso de RBAC, en la interfaz de datos. Las operaciones que pueden gestionarse en cada interfaz son las siguientes:

- Interfaz de administración: es desde donde se administra Key Vault, se utiliza para crear y eliminar almacenes. También pueden leerse las propiedades del almacén y administrar las directivas de acceso.
- Interfaz de datos: es desde donde se trabaja con los datos almacenados de un almacén de claves. Se pueden agregar, eliminar y modificar los diferentes secretos.

Además del acceso a las interfaces, también se puede controlar el acceso a los secretos concretos mediante RBAC o las directivas de acceso.

El servicio genera una serie de registros acerca de las actividades realizadas en un almacén, incluyendo quién ha accedido a un almacén y cuando lo ha hecho, entre otros datos.

Por último, se incorpora una protección frente a eliminación temporal, permitiendo recuperar almacenes y secretos eliminados. También pueden realizarse copias de seguridad periódicas al actualizar, eliminar o crear secretos en un almacén.

4.7. Azure VPN Gateway

Se trata de un servicio que permite utilizar un tipo un tipo de puerta de enlace de red virtual para enviar tráfico cifrado entre esta red y otra externa u otra propia de la red de Microsoft. Para crear conexiones a esta puerta de enlace se establecen túneles VPN, todos los túneles generados comparten el mismo ancho de banda de puerta de enlace. [14]

Al crear una puerta de enlace Azure configura e implementa dos o más máquinas virtuales con una subred para las mismas. El proceso de creación de las mismas puede llegar a tardar 45 minutos o más, cuando este termina permite configurar las conexiones que pueden ser túneles VPN IPSec o IKE. La conexión puede establecerse de varias formas:

- Entre dos VPN Gateway (de red virtual la red virtual).
- Entre el VPN Gateway y un dispositivo VPN local (de sitio a sitio).
- De punto a sitio, estableciendo la conexión con alguna herramienta con OpenVPN.

4.8. Azure Application Gateway

Este servicio incluye un *Web Application Firewall* (WAF) y un balanceador de carga que opera en capa 7.

El servicio incluye terminación SSL/TLS en la puerta de enlace, con lo que se podrá configurar HTTPS en el mismo, también SSL/TLS de extremo a extremo a los servidores de la red privada.

En el caso de la segunda versión del servicio, admite escalado automático, que cambiará dependiendo de los patrones de la carga del tráfico. También redundancia de zonas para ofrecer mayor resistencia a errores. [15]

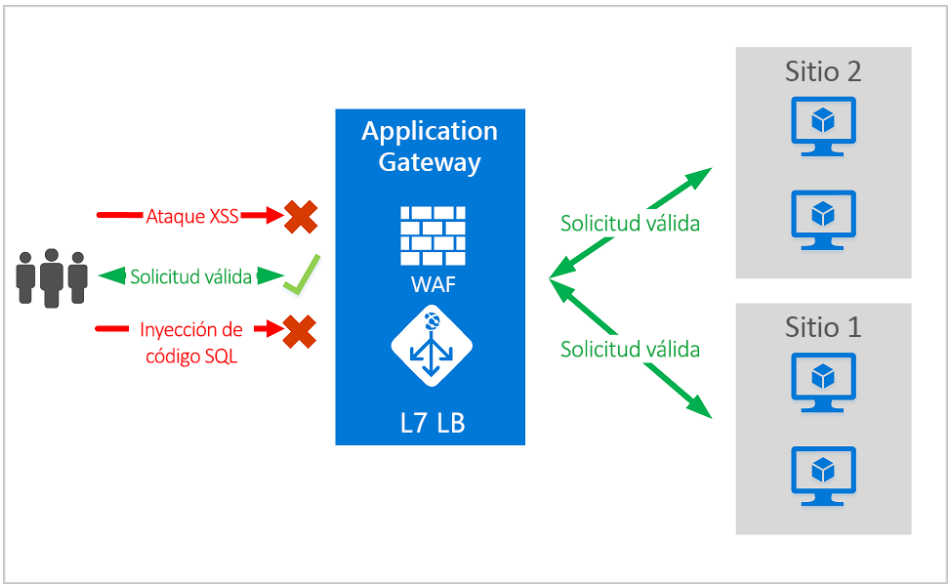


Ilustración 11: Arquitectura de Application Gateway

4.8.1. Balanceador de carga

Al tratarse de un balanceador L7, puede tomar decisiones de enrutamiento basadas en atributos de una solicitud HTTP, por ejemplo, puede redirigir el tráfico a ciertos servidores optimizados para un tipo de recurso dependiendo de la URL proporcionada.

Permite gestionar cookies, de forma que se puede redirigir el tráfico de un usuario al mismo servidor en el que ya había guardado información de una sesión. También se puede realizar redireccionamiento automático de HTTP a HTTPS para asegurar que la conexión siempre va cifrada.

4.8.2. Web Application Firewall

Ofrece protección centralizada de las aplicaciones web contra las vulnerabilidades de seguridad más habituales. Se basa en el conjunto de reglas básicas de OWASP.

El servicio ofrece lo siguiente:

- Protege las aplicaciones web de las vulnerabilidades y los ataques web.
- Permite proteger varias webs al mismo tiempo.
- Permite crear directivas WAF personalizadas.
- Protege de bots mediante un conjunto de reglas de reputación de IP.

También se genera un registro en tiempo real de los ataques a aplicaciones, puede integrarse con Azure Monitor para realizar un seguimiento de las alertas.

El WAF cuenta además con dos modos de ejecución:

- Modo de detección: supervisa y registra las alertas de amenazas, pero no bloquea las solicitudes entrantes.
- Modo de prevención: bloquea las intrusiones y los ataques detectados por las reglas.

4.9. Azure Monitor

Se trata de una solución de supervisión para recopilar, analizar y responder a la telemetría de entornos locales y en la nube. [16]

El servicio recopila y agrega los datos de las diferentes capas y componentes a una plataforma de datos en común. Los datos almacenados se pueden correlacionar y analizar, tras lo cual pueden realizarse análisis y visualizaciones sobre los mismos.

Los datos obtenidos pueden exportarse para ser utilizados por otras herramientas proporcionadas por terceros.

En el diagrama pueden verse los diferentes componentes del sistema:

- Orígenes de los datos: son los tipos de datos que se recogen de cada recurso que es supervisado. Estos, tras recopilarse, se enrutan a la plataforma de datos.
- Plataforma de datos: se compone de almacenes para los datos recopilados, estos son separados según su tipo.

- Consumo de datos: diferentes aplicaciones que utilizan los datos almacenados en la plataforma, proporcionando análisis, visualizaciones, conclusiones y respuestas.

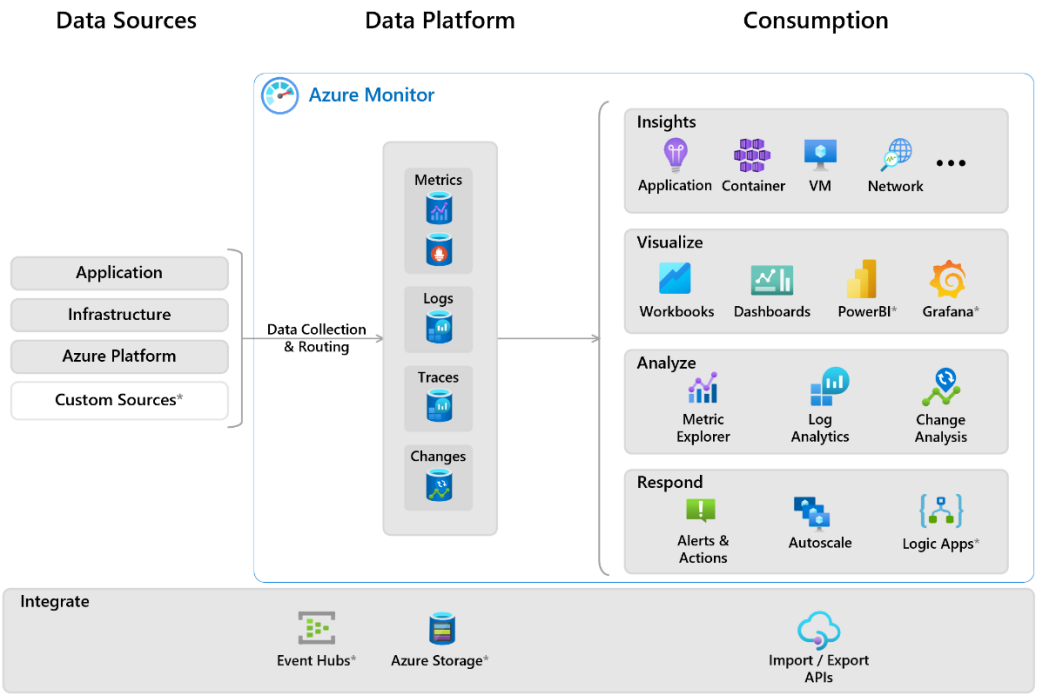


Ilustración 12: Componentes de Azure Monitor

4.10. Microsoft Defender for Cloud

Se trata de una plataforma de protección de aplicaciones en la nube, incluye un conjunto de medidas y buenas prácticas para proteger las aplicaciones en la nube. [17]

Combina funcionalidades de:

- DevSecOps: unifica la administración de seguridad a nivel de código en entornos multinube o con varios pipelines.
- CSPM: permite administrar posturas de seguridad en la nube, mostrando acciones que pueden realizarse para evitar cometer infracciones.
- CWPP: permite proteger las cargas de trabajo en la nube.

4.11. Microsoft Sentinel

Es una solución escalable y nativa de la nube que proporciona administración de eventos de seguridad (SIEM) y respuesta automatizada de orquestación de seguridad (SOAR). [18]

Permite obtener una vista general de la seguridad de la organización al ofrecer una única solución para la detección de ataques, la visibilidad de amenazas, la búsqueda proactiva y la respuesta frente a amenazas.

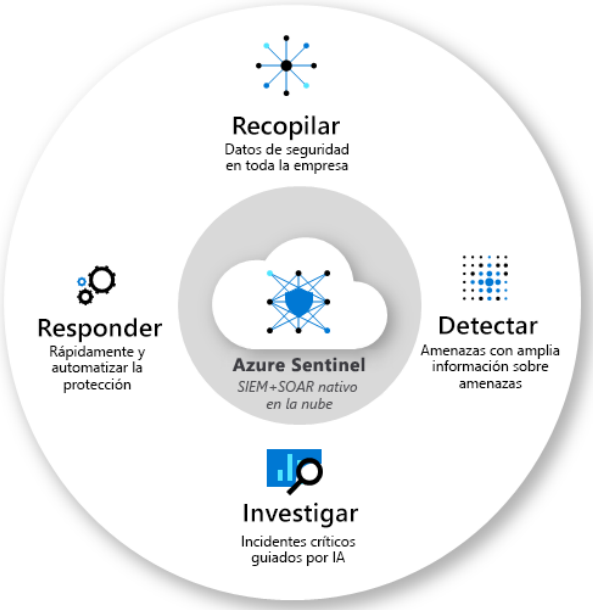


Ilustración 13: Funcionalidades de Microsoft Sentinel

Microsoft Sentinel permite, por lo tanto:

- Recopilar datos de todos los usuarios, dispositivos, aplicaciones e infraestructura en la nube y entornos locales.
- Detectar amenazas minimizando los falsos positivos mediante el análisis e inteligencia sobre amenazas.
- Investigar amenazas con inteligencia artificial.
- Responder a los incidentes con orquestación y automatización de tareas comunes integradas.

5. Medidas de seguridad

En esta sección se estudiarán las diferentes medidas de seguridad que se utilizarán en el sistema.

Se seguirá la guía de buenas prácticas de seguridad propuesta para WordPress. [19]

Estas medidas buscarán cubrir una serie de aspectos de seguridad:

- Limitar el acceso: Esto reducirá el número de puntos de entrada que un atacante podría utilizar para acceder al sistema.
- Contención: El sistema debe estar configurado para minimizar el daño en caso de que este sea comprometido.
- Preparación y conocimiento: Se debe hacer un seguimiento de la instalación de WordPress y mantener una serie de copias de seguridad para recuperar el estado del sistema en caso de que ocurra algún problema.
- Fuentes confiables: Se deben utilizar plugins y temas de fuentes confiables, por ejemplo, del propio repositorio de WordPress.org

También se utilizarán las buenas prácticas para despliegue en Azure propuestas por Microsoft para la arquitectura. [20]

5.1. Vulnerabilidades

Hay que mantener el sistema operativo y el software instalado actualizado para cubrir las diferentes vulnerabilidades que van surgiendo, tanto en el servidor como en las máquinas locales desde donde se realizarán accesos. Esto incluye mantener WordPress actualizado.

Las actualizaciones menores de WordPress, que incluyen parches de seguridad, no suelen producir problemas de compatibilidad, con lo que se puede permitir a WordPress actualizarlas automáticamente, comportamiento que ya viene configurado por defecto. Sin embargo, al actualizar a versiones mayores se podrían producir incompatibilidades con los plugins instalados.

Lo ideal sería tener una versión de desarrollo del servicio de WordPress, esto se puede conseguir haciendo una copia de la carpeta de WordPress y teniendo una máquina a parte solo para pruebas, esta podría estar en Azure o en local gestionada por el administrador, aunque en este caso también tendría que obtenerse la copia de la base de datos. La versión de desarrollo podría mantenerse de forma continua para realizar pruebas o crearla cuando fuera necesario. En esta versión se probarían las actualizaciones de los plugins y las actualizaciones mayores de WordPress para realizar un seguimiento y comprobar que no se producen incompatibilidades, tras lo cual se actualizaría en producción.

5.2. Contraseñas

Es necesario utilizar contraseñas fuertes para evitar ataques por fuerza bruta. Para ello se pueden utilizar generadores automáticos para crear contraseñas seguras. Se forzará el uso de contraseñas fuertes mediante el plugin *iThemes Security*, este plugin además aportará otras herramientas de seguridad que se verán en las siguientes secciones.

En el caso de las cuentas de administración se utilizará un segundo factor de autenticación para el inicio de sesión como medida de seguridad adicional, este también se implementará mediante *iThemes Security*.

El segundo factor de autenticación será una contraseña de un solo uso (TOTP) y el usuario podrá utilizar cualquier aplicación que facilite este sistema, por ejemplo, *Microsoft Authenticator*.

5.3. Comunicación con el servidor

En el caso de acceder a los servidores donde se aloja WordPress, se utilizarán protocolos de comunicación seguros que utilicen cifrado como SSH, SFTP o RDP.

Las conexiones entre el *Application Gateway* y el servidor, y entre el servidor y la base de datos, estarán cifradas.

5.4. Permisos de archivos

Cuando no sea necesario para alguna funcionalidad tener permisos de lectura en archivos de WordPress es mejor restringir los mismos puesto que podría ser potencialmente peligroso.

El propietario de los archivos debería ser la cuenta de usuario del administrador del servidor. Se añadirán permisos de escritura para WordPress en los archivos que este necesite. Los directorios y sus permisos serían los siguientes:

- /: Se trata del directorio raíz de WordPress, los archivos deberían tener permisos de escritura solo para la cuenta de usuario de administrador.
- /wp-admin/: Se trata del área de administración, todos los archivos deberían tener permisos de escritura solo para la cuenta de administración.
- /wp-includes/: Incluye la lógica de aplicación de WordPress, todos los archivos deberían tener permisos de escritura solo para la cuenta de administración.
- /wp-content/: Aquí se encuentra el contenido proporcionado por los usuarios, los archivos por lo tanto tendrán permisos de escritura para la cuenta de administración y para la de WordPress.
- /wp-content/plugins/: Incluye los plugins instalados, los archivos solo tendrán permisos de escritura para la cuenta de administración.

5.5. Seguridad en la base de datos

Para la mayoría de operaciones de WordPress las acciones en la base de datos de SELECT, INSERT, UPDATE y DELETE serán suficientes, por lo tanto, el usuario de la base de datos que será utilizado por WordPress no tendrá permisos para las operaciones de DROP, ALTER y GRANT, estas acciones sólo podrán ser realizadas por las cuentas de administración de la base de datos.

En caso de realizar actualizaciones puede que las acciones anteriores si tengan que ser utilizadas, con lo que se tendrían que modificar los privilegios de la cuenta de WordPress de manera temporal.

Se tendrían 3 cuentas para la base de datos:

- Administrador Azure: Tiene todos los permisos para todas las bases de datos. Es el encargado de mantener la infraestructura en Azure.
- Administrador WordPress: Tiene todos los permisos para la base de datos de WordPress. Es el encargado de mantener el servidor de WordPress.
- WordPress: Es la cuenta utilizada por la aplicación. Tiene los permisos de SELECT, INSERT, UPDATE y DELETE.

Se realizarán copias de seguridad de la base de datos semanalmente, estas estarán cifradas. Para realizar las copias se utilizará el propio servicio de copias de seguridad proporcionado por MySQL Flexible Server.

5.6. Medidas en el panel de administración de WordPress

Puede añadirse una capa de protección extra utilizando un segundo factor de autenticación en las cuentas de administración de WordPress, como se ha visto anteriormente.

Se restringirá el acceso al panel de administración para que solo ciertas direcciones puedan acceder, para ello se utilizará una regla en el firewall de aplicaciones de Azure la cual denegará el tráfico a cualquier ruta que contenga wp-admin si la dirección IP no es una de las esperadas.

5.7. Medidas en htaccess

Puede bloquearse el acceso a scripts a las que no queremos que ningún usuario pueda acceder mediante reglas en el archivo .htaccess, esto incluye /wp-includes/ que contiene la lógica de la aplicación.

Hay que asegurar que las reglas añadidas están fuera del bloque de WordPress para que este no las reescriba, las reglas serían las recomendadas en wordpress.org:

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
```

```
</IfModule>
```

También se pueden establecer configuraciones para establecer límites en los tamaños de los archivos y ejecución de los scripts, la configuración quedaría en .htaccess quedaría de la siguiente manera:

```
php_value upload_max_filesize 2M
php_value post_max_size 2M
php_value max_execution_time 300
php_value max_input_time 300
```

5.8. Medidas en wp-config

En primer lugar, se deberán utilizar claves seguras para toda la configuración de WordPress, incluyendo la clave de autenticación, los *nonces* utilizados, etc. Para ello se puede utilizar el generador[3] proporcionado por Wordpress.org.

En cuanto a el servidor, debemos asegurarnos de que el archivo no sea accesible por los usuarios. Esto puede realizarse denegando el acceso desde .htaccess en caso de que el servidor lo utilice.

El panel de administración de WordPress permite a los administradores editar archivos PHP, esto incluye por ejemplo los *plugins* o los archivos de los temas. Esto podría ser usado por un atacante para ejecutar código, por lo tanto, será necesario desactivar la edición de archivos desde *wp-config*.

Los distintos valores de wp-config se definirán desde un script cloud-init, este script se ejecuta cuando una máquina virtual inicia. Este script también definirá otros valores de configuración de las máquinas, como la configuración de Apache, los certificados para el uso de SSL, la configuración de .htaccess y la ruta de montaje de la carpeta compartida por las máquinas.

5.9. Firewall

Se añadirá un *Web Application Firewall* (WAF) como intermediario entre el tráfico de internet y el servidor. Este servicio actúa como un proxy inverso, de manera que acepta las peticiones y las reenvía al servidor, eliminando aquellas que

[3] https://api.wordpress.org/secret-key/1.1/salt/

sean maliciosas. Por lo tanto, esto permite filtrar el tráfico antes de que llegue al servidor de WordPress.

El WAF utilizado será el incluido con el servicio de Azure de *Application Gateway* [21], este incluye protección contra bots conocidos y reglas basadas en OWASP 3.2, las categorías de amenaza de las que protege son las siguientes:

- *Cross-site scripting*.
- Inyección de SQL.
- Inyección de comandos
- Contrabando de solicitudes HTTP (HTTP *request smuggling*).
- División de respuestas HTTP (*HTTP response splitting*).
- Inclusión de archivos remotos.
- Infracciones del protocolo HTTP.
- Anomalías del protocolo HTTP, como la falta de ciertos valores en los *headers*.
- Errores de configuración de Apache.
- Rastreadores y escáneres.
- Fijación de sesión.
- Ataques de Java.
- Ataques por inyección de PHP.

También pueden configurarse reglas personalizadas, estas se utilizarán, por ejemplo, para restringir el acceso a ciertas rutas como las del panel de administración de WordPress. Estas reglas también pueden utilizarse para limitar el número de conexiones desde una dirección cuando estas superan una cantidad determinada, esto junto a la protección contra bots ayudaría a cubrir frente a determinados ataques de denegación de servicio al aportar protección contra automatización y ante llamadas excesivas.

Por último, será el encargado de realizar la comunicación mediante TLS con el cliente y por lo tanto guardará el certificado necesario para la misma.

5.10. Seguridad por ocultación

Se puede aplicar la ocultación en ciertas áreas para añadir protección frente a un atacante de manera que este no pueda realizar movimientos por el sistema no pudiendo utilizar, por ejemplo, nombres por defecto.

Una forma de realizar esto en WordPress seria no utilizar ciertos nombres de usuario para las cuentas de administración como, por ejemplo, admin. También pueden modificarse los prefijos de las tablas de WordPress (wp_) de manera que puedan evitarse ciertos ataques de inyección de SQL que hacen uso de los nombres de las tablas por defecto.

5.11. Monitorización

Se guardarán los logs de las diferentes operaciones realizadas en WordPress y los obtenidos de los recursos de seguridad utilizados, como por ejemplo el WAF.

Se realizará una monitorización de los logs anteriores de manera que se podrá realizar un seguimiento de los cambios en el sistema y de los diferentes ataques que se intenten realizar al mismo.

Desde Wordpress podrá utilizarse un plugin como WP Activity Log [22] para realizar un seguimiento de lo siguiente:

- Cambios en las páginas y los posts.
- Cambios en las etiquetas y las categorías.
- Cambios en los menús y los widgets.
- Cambios en los usuarios.
- Cambios en los perfiles de los usuarios.
- Actividad de los usuarios.
- Cambios en el *core* de WordPress y en la configuración.
- Cambios en *plugins* y temas.
- Cambios en la base de datos.
- Cambios en archivos de WordPress.

También se realizará un seguimiento de los logs generados por el WAF y la base de datos desde Azure. Se podrá realizar una consulta centralizada de los mismos desde Azure Monitor o Microsoft Sentinel, el cual además proporcionará información avanzada del estado de la seguridad.

5.12. Seguridad en las redes

Se seguirán las pautas dadas por Microsoft para realizar controles en el tráfico de red que se origina en Azure, de esta forma se ayudara a detectar, contener y detener a los atacantes que logren entrar en la nube. [23]

En primer lugar, se establecerá una arquitectura de red segmentada con comunicaciones seguras entre los diferentes segmentos, de esta forma se evitarán posibles movimientos laterales de los atacantes si estos consiguen comprometer algún segmento del sistema.

También se protegerán los puntos de conexión públicos mediante Application Gateway y establecerán controles que permitan denegar el tráfico utilizando para ello reglas en el *Web Application Firewall* del *Application Gateway*.

Por último, la administración de las máquinas se realizará solo desde la red virtual privada, utilizando un *VPN Gateway*, de esta forma no se podrán intentar realizar ataques desde puntos de conexión públicos.

5.13. Seguridad en los datos

Se utilizarán las pautas dadas por Microsoft para clasificar, proteger y supervisar los datos, tanto en reposo como en tránsito. [24]

En primer lugar, se utilizarán los controles de acceso proporcionados por Azure para acceder a los recursos de la plataforma, incluyendo el segundo factor de autenticación proporcionado por el mismo.

También se utilizarán los cifrados proporcionados por Azure, por ejemplo, en MySQL Flexible Server para cifrar los datos en reposo. También el cifrado entre los diferentes puntos de la red.

5.14. Requisitos cubiertos

A continuación, se mostrará un resumen de los requisitos de seguridad que quedarían cubiertos con las medidas de las secciones anteriores, en la tabla se incluirá el identificador del requisito y las secciones que lo cubrirán.

Identificador del requisito	Secciones de las medidas de seguridad
1.9.1	Comunicación con el servidor, Medidas en wp-config, Firewall, Seguridad en las redes
2.1.1	Contraseñas, Medidas en wp-config
2.1.5	Contraseñas
2.1.6	Contraseñas
2.1.9	Contraseñas
2.4.1	Seguridad en los datos, Medidas en wp-config
4.1.3	Permisos de archivos, Seguridad en la base de datos, Medidas en el panel de administración de WordPress, Medidas en htaccess, Medidas en wp-config, Firewall
4.3.1	Contraseñas, Medidas en el panel de administración de WordPress.
7.1.4	Monitorización
7.3.1	Monitorización
7.1.3	Monitorización
8.1.5	Seguridad en la base de datos
9.1.1	Firewall, Seguridad en las redes
9.2.2	Comunicación con el servidor, Medidas en wp-config, Firewall, Seguridad en las redes
11.1.4	Firewall
12.1.1	Medidas en htaccess
14.2.1	Vulnerabilidades

Tabla 6: Requisitos cubiertos

Mediante estas medidas quedarían cubiertos todos los requisitos que habían sido propuestos en las secciones anteriores.

6. Arquitectura del sistema

En esta sección se describe la arquitectura del sistema, incluyendo una descripción de los componentes que se utilizarán y el flujo que un usuario y un administrador tendrían en el sistema.

En la ilustración inferior puede verse el diagrama con la arquitectura del sistema que se utilizara.

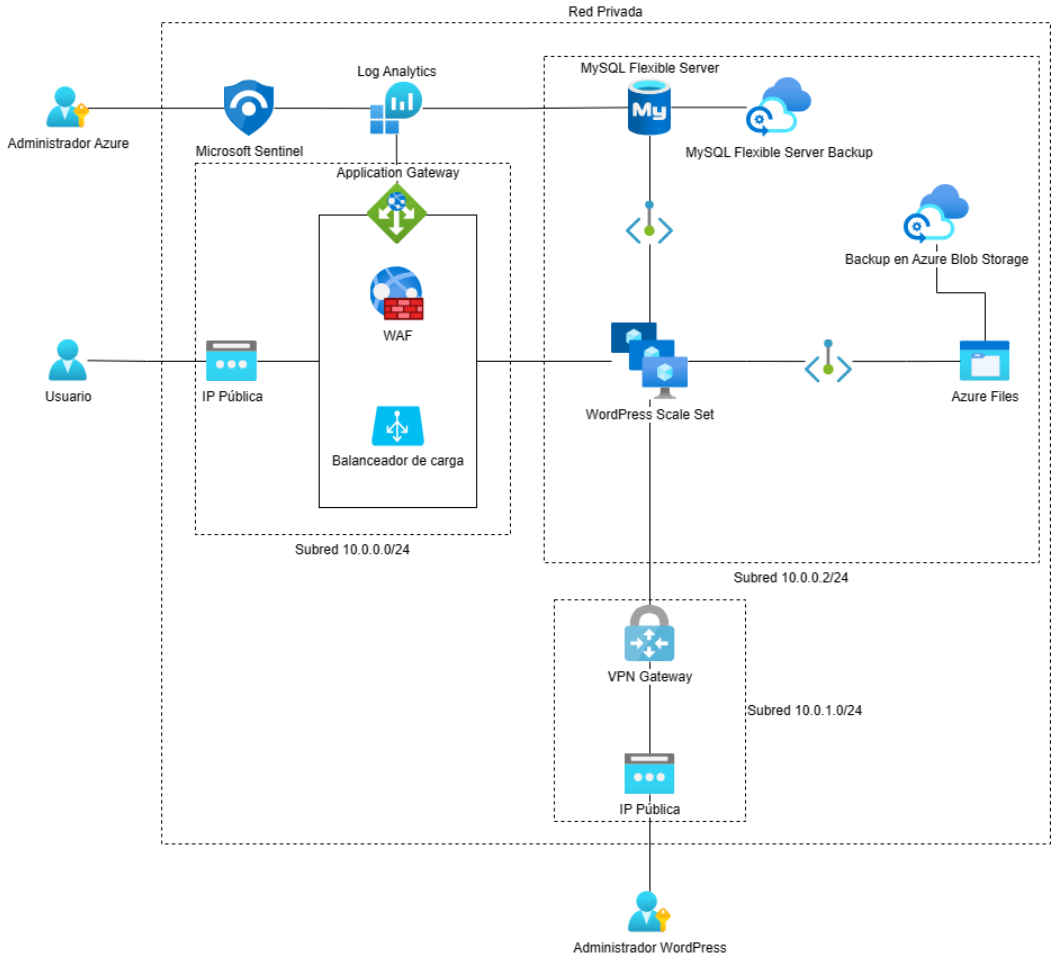


Ilustración 14: Arquitectura propuesta

6.1. Descripción de los componentes

En primer lugar, para realizar el acceso al *front-end* se hace uso de un *Application Gateway*, este incluye un *firewall* de aplicaciones que se encargará de proteger de ciertos intentos de ataque. También incluye un balanceador de carga que se encargará de distribuir las solicitudes de los usuarios. Este componente se encarga de ofrecer el certificado necesario para realizar las conexiones HTTPS, la

conexión entre el *Application Gateway* y las diferentes máquinas también se realizará mediante SSL.

El panel de configuración general del *Application Gateway* sería el siguiente:

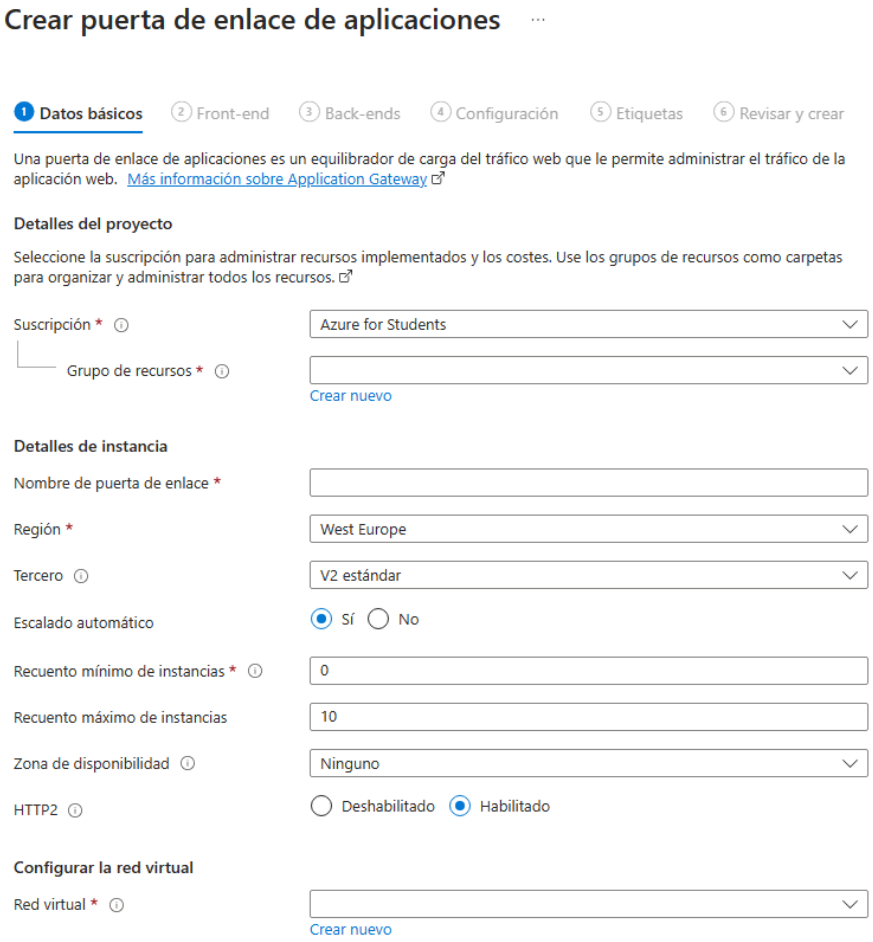


Ilustración 15: Panel de configuración de Application Gateway

Este panel nos permitiría configurar:

- Tipo de puerta de enlace según el cual incluirá el *Web Application Firewall* o solo el balanceador de carga.
- Si las instancias se escalarán automáticamente, en cuyo caso se podrá indicar el número máximo y mínimo.
- La zona de disponibilidad para poder desplegar las instancias en múltiples zonas dentro de la misma región, aumentando así la disponibilidad.
- El *front-end* que incluye la dirección pública con la que se conectará un cliente.

- El *back-end* que incluye los servidores a los que distribuirá la carga el balanceador de carga.

El conjunto de máquinas virtuales será el encargado de ejecutar las máquinas con WordPress, el contenido de la carpeta WordPress se guardará en el almacenamiento compartido, se realizarán copias de seguridad de este contenido mediante el plugin UpdraftPlus que permitirá descargarlas en local o almacenarlas en servicios como OneDrive o Google Drive. El contenido dinámico se guardará en una base de datos MySQL flexible que además realizará copias de seguridad periódicas, estas copias serán configuradas desde el propio servicio de Azure, el cual también permite restaurarlas a la base de datos activa.

Se utilizará un script *cloud-init* para configurar las máquinas cuando éstas se inicien. Incluirá la configuración de WordPress, la configuración de Apache y los certificados del servidor necesarios para establecer la conexión SSL con el *Application Gateway*, también se encargará de montar la carpeta con el almacenamiento compartido.

El panel de configuración del conjunto de máquinas virtuales es el siguiente:

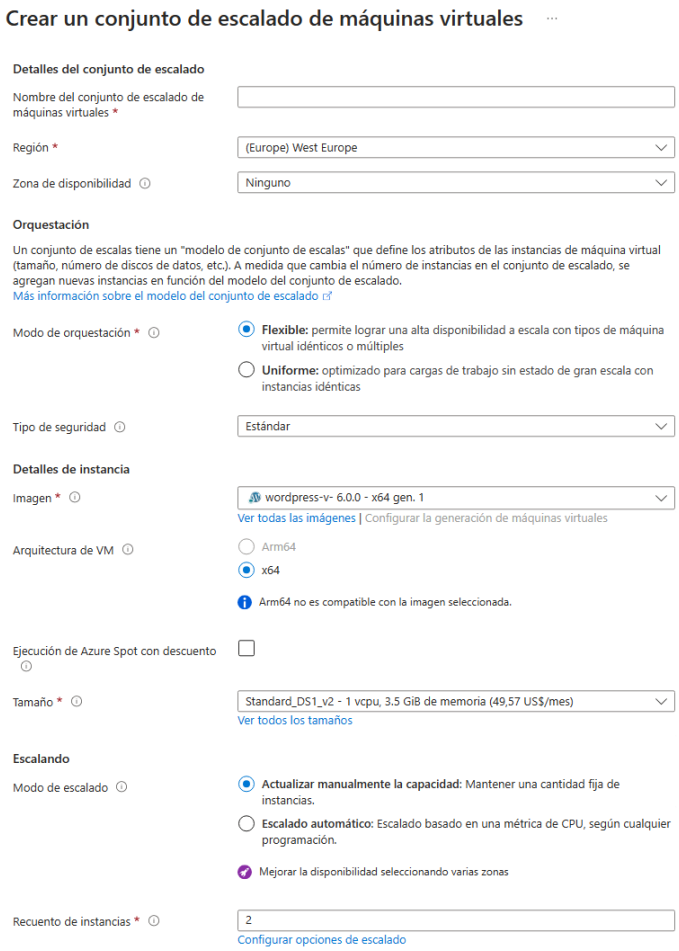


Ilustración 16: Panel de configuración del conjunto de máquinas virtuales

Vemos que se pueden configurar la imagen que se utilizará y los tipos de escalado, también si la máquina será del tipo spot reduciendo así los costes de la misma.

Otras opciones de configuración importantes serían las de discos y redes cuyos paneles son los siguientes:

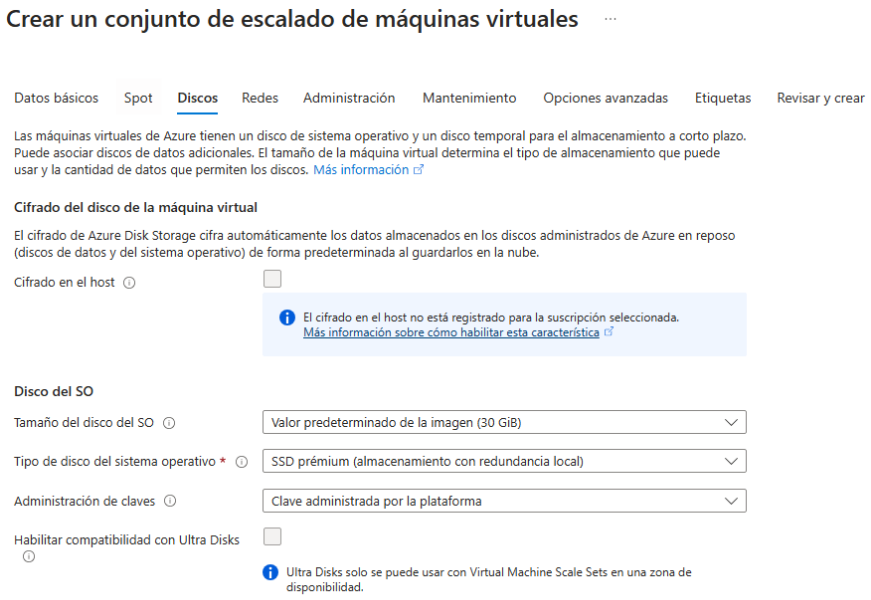


Ilustración 17: Panel de configuración de discos del conjunto de máquinas virtuales

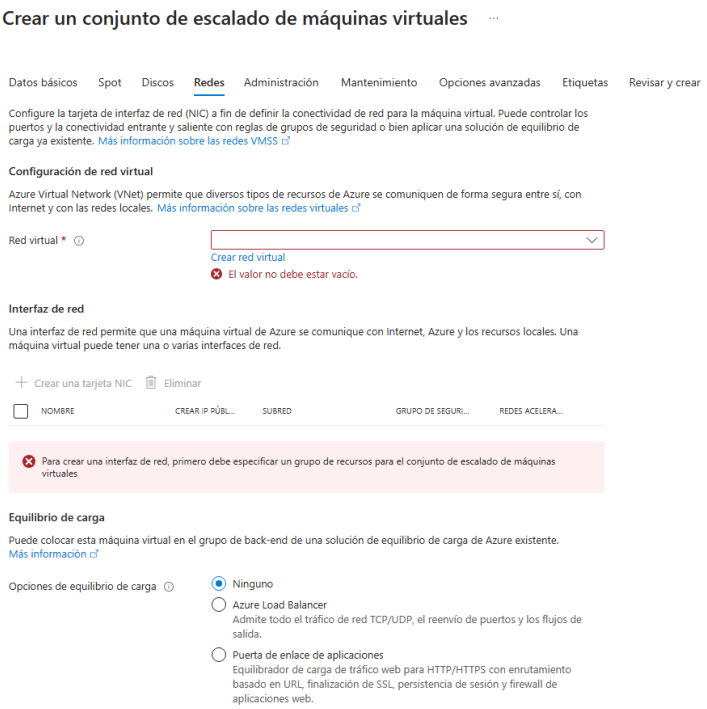


Ilustración 18: Panel de configuración de redes del conjunto de máquinas virtuales

Vemos que en la configuración de discos se puede elegir el tipo y el tamaño, también se pueden cifrar, aunque con la suscripción de estudiante no se permite. En la parte de red se puede añadir la red virtual y la interfaz de red que incluirá el grupo de seguridad y las direcciones privadas y públicas, en este punto también se puede añadir al balanceador de carga.

Para poder añadir el script cloud-init mencionado anteriormente se tendría que hacer uso de la configuración avanzada dentro de la configuración del conjunto de máquinas.

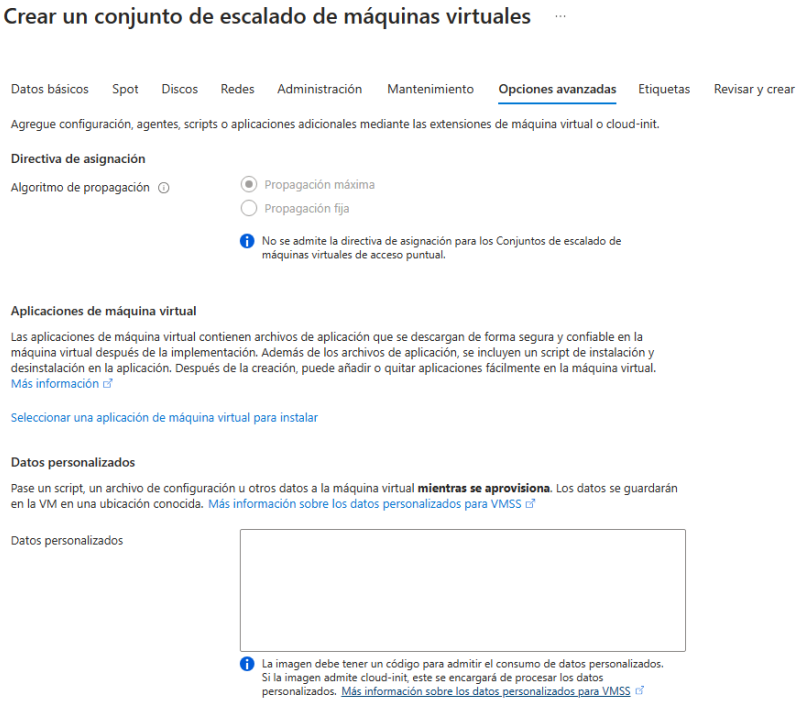


Ilustración 19: Panel de configuración de opciones avanzadas del conjunto de máquinas virtuales

Por otro lado, el panel de configuración básico de MySQL Flexible Server sería el siguiente:

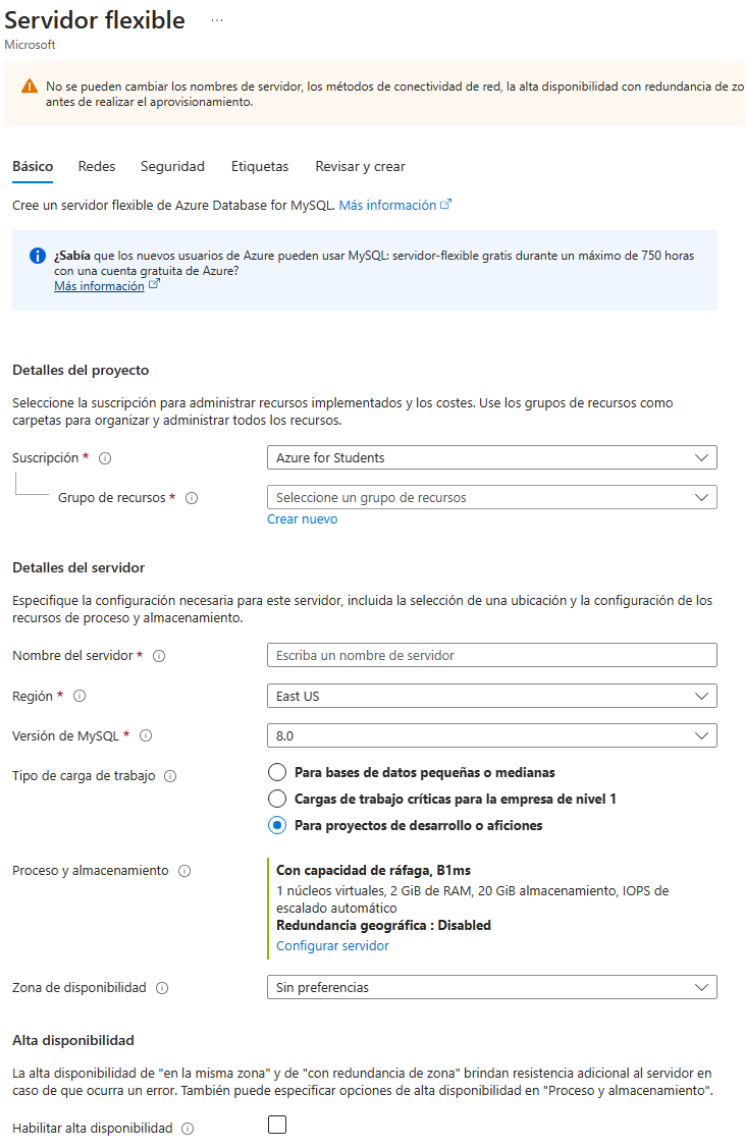


Ilustración 20: Panel de configuración de MySQL Flexible Server

Vemos que se puede elegir la versión de MySQL a utilizar y las zonas de disponibilidad, también las características de la base de datos. Desde el panel de redes podrían seleccionarse los rangos de redes con acceso a la base de datos y desde el de seguridad realizar configuración del cifrado, sus paneles son los siguientes:

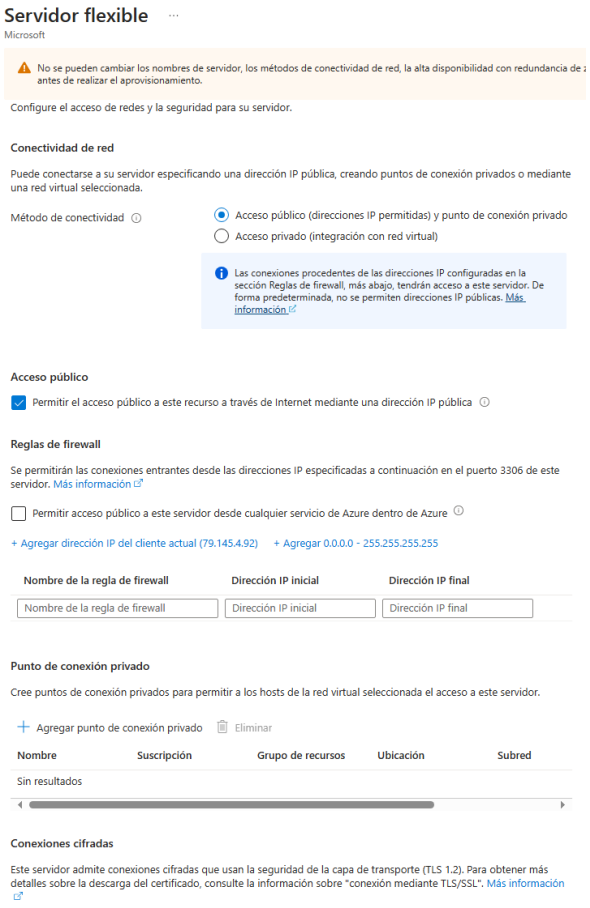


Ilustración 21: Panel de configuración de redes del servidor flexible

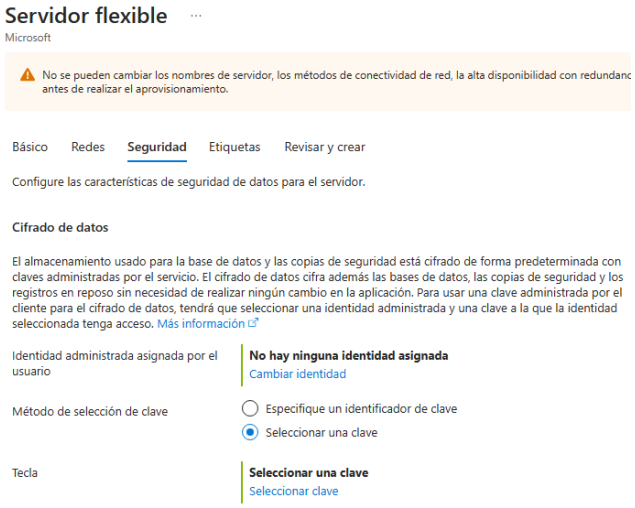


Ilustración 22: Panel de configuración de seguridad del servidor flexible

Se dispondrá de un *VPN Gateway* para poder establecer túneles VPN del tipo *point-to-site*, esto permitirá a los administradores conectarse a las máquinas de WordPress mediante SSH sin que las máquinas tengan que estar expuestas a Internet. Su panel de configuración sería el siguiente:

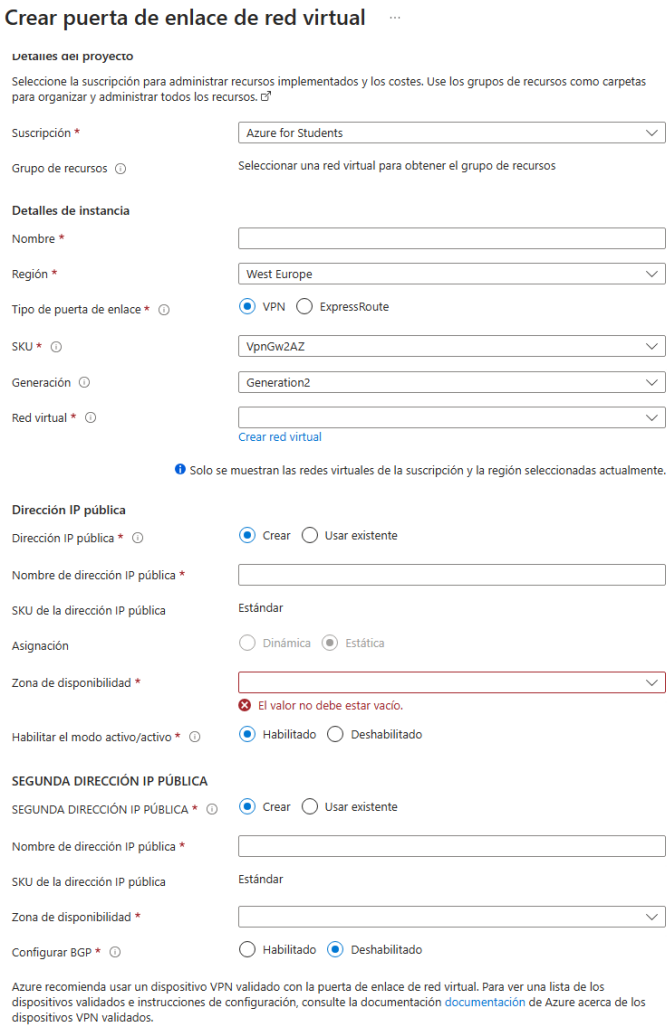


Ilustración 23: Panel de configuración del VPN Gateway

Se restringirá el acceso al panel de administración de WordPress haciendo uso de una regla en el *Application Gateway* de forma que solo sea permitido el tráfico proveniente de ciertas IP a las rutas del panel de administración.

La información de los logs de *Application Gateway* y MySQL Flexible Server serán recogidos por Microsoft Sentinel que permitirá monitorizar los mismos y ofrecerá información de seguridad. En WordPress se utilizará el plugin *WP Activity Log* para realizar el seguimiento.

6.2. Flujos de trabajo

Existen varios flujos de trabajo dependiendo de los usuarios y de las tareas que se quieran realizar, el primero para los usuarios que acceden al sitio web, otro para

los administradores de WordPress cuando estos se conectan al servidor y un último para cuando los administradores se conectan al panel de administración.

El flujo para un usuario que hace uso de la web es el siguiente:

1. Los usuarios acceden al *front-end* a través de un *Application Gateway* el cual mantiene el certificado necesario para establecer la conexión HTTPS.
2. El firewall de aplicaciones del *Application Gateway* filtra las solicitudes para detectar posibles ataques, el tráfico también será bloqueado en caso de que algún usuario intente acceder a rutas del panel de administración.
3. El balanceador de carga del *Application Gateway* distribuye las solicitudes entre las diferentes maquinas del conjunto de máquinas virtuales.
4. El usuario realiza acciones en WordPress, este obtiene el contenido dinámico de la base de datos MySQL, las máquinas comparten el contenido estático mediante el almacenamiento compartido.

El flujo de los administradores que se conectan a las máquinas es el siguiente:

1. El administrador utiliza un certificado para autenticarse y realizar una conexión VPN a la red interna.
2. El administrador utiliza SSH o RDP para conectarse a una máquina de la red interna, para ello hace uso de otro certificado.
3. El administrador realiza cambios en las máquinas, si los cambios se producen en la carpeta compartida estos se verán reflejados en todas las máquinas.

El flujo de los administradores que se conectan al panel de administración es el siguiente:

1. El administrador accede a WordPress con una IP reconocida por la regla del *Application Gateway*.
2. El administrador inicia sesión con sus credenciales usando un segundo factor de autenticación en el proceso.
3. El administrador realiza cambios desde el panel de administración, estos se verán reflejados en la base de datos y en el almacenamiento compartido de las máquinas.

7. Análisis de costes

En este apartado se analizarán los costes de la arquitectura propuesta anteriormente, para ello se utilizará la calculadora de precio proporcionada en Azure. [25]

Se realizarán dos análisis, uno para el sistema en producción y otro para el sistema que se tendría para realizar las pruebas.

7.1. Análisis de costes en producción

Los costes en producción del sistema desplegado en Azure por mes sería el siguiente:

Descripción del servicio	Precio mensual estimado
IP pública estática x 2	5,00 €
VPN Gateway, nivel básico	25,00 €
Application Gateway, tier V2, una instancia	335,02 €
Cuenta de almacenamiento con archivos de Azure, acceso frecuente, 100GB en reposo, 100GB instantáneas, 1GB metadatos	5,33 €
Cuenta de almacenamiento en blobs, acceso esporádico, 1000GB	12,26 €
Servidor MySQL Flexible, uso general, 2 núcleos virtuales, 10GB, 20GB copias de seguridad	144,24 €
Conjunto de máquinas virtuales, una instancia, 4 núcleos, 8GB de RAM	127,09 €
Microsoft Sentinel, 1GB de ingesta diario	32,82 €
Total	**686,76 €**

Tabla 7: Análisis de costes mensual en producción

A este precio añadiríamos el de otros servicios anuales externos a los de Azure, lo que daría el siguiente coste anual:

Descripción del servicio	Precio anual estimado
UpdraftPlus Premium	66,5 €
Dominio .es x 2	14,5 €
Certificado OV Digicert x 2	500,00 €
Servicios Azure	8241,12 €
Total	**8822,12 €**

Tabla 8: Análisis de costes anual en producción

7.2. Análisis de costes del sistema de pruebas

En el sistema de pruebas se intentarán utilizar los servicios en su formato más económico, se supondrá además que el sistema está trabajando el día al completo, aunque es posible que algunos de estos servicios solo se desplieguen en momentos

concretos. En el caso de Microsoft Sentinel se tendrá una ingesta diaria de 1GB puesto que es el mínimo que se permite, pero en la realidad sería mucho menor. El análisis serie el siguiente:

Descripción del servicio	Precio mensual estimado
IP pública estática x 2	5,00 €
VPN Gateway, nivel básico	25,00 €
Application Gateway, tier V2, una instancia	335,02 €
Cuenta de almacenamiento con archivos de Azure, acceso frecuente, 100GB en reposo, 100GB instantáneas, 1GB metadatos	3,38 €
Servidor MySQL Flexible, uso general, 2 núcleos virtuales, 10GB, 20GB copias de seguridad	144,24 €
Conjunto de máquinas virtuales, una instancia, 1 núcleos, 3,5GB de RAM, Spot	4,86 €
Microsoft Sentinel, 1GB de ingesta diario	32,82 €
Total	**549,34 €**

Tabla 9: Análisis de costes mensual en pruebas

Al ser un sistema que probablemente no se encuentre con todos los componentes funcionando todo el tiempo tal vez sería mejor analizar el precio del mismo por horas con lo que se podría calcular cuánto se gastaría si se realizaran las pruebas durante un tiempo determinado. En este cálculo no se tendrá en cuenta Microsoft Sentinel al calcularse su precio por datos ingestados y no por tiempo, quedaría de la siguiente manera:

Descripción del servicio	Precio por hora estimado
IP pública estática x 2	0,006 €
VPN Gateway, nivel básico	0,034 €
Application Gateway, tier V2, una instancia	0,458 €
Cuenta de almacenamiento con archivos de Azure, acceso frecuente, 100GB en reposo, 100GB instantáneas, 1GB metadatos	0,004 €
Servidor MySQL Flexible, uso general, 2 núcleos virtuales, 10GB, 20GB copias de seguridad	0,197 €
Conjunto de máquinas virtuales, una instancia, 1 núcleos, 3,5GB de RAM, Spot	0,006 €
Total	**0,709 €**

Tabla 10: Análisis de costes anual en pruebas

Los costes para el desarrollo del proyecto se han cubierto mediante el programa de créditos de Azure para estudiantes, el cual ofrece 100 dólares durante los primeros 12 meses. [26]

8. Despliegue del sistema

En esta sección se describe cómo realizar el despliegue en Azure de una prueba del sistema propuesto. Este se trata de un entorno de experimentación que utiliza algunas suscripciones de los productos diferentes de las que se utilizarían en un entorno de producción para poder ahorrar costes y algunos cambios en el uso de los componentes para simplificar el despliegue.

Para poder realizar el despliegue se utilizan los fondos gratuitos que son ofrecidos a los estudiantes, en total 100 dólares durante 12 meses. También se ofrecen algunos servicios gratuitos hasta llegar a cierto uso del recurso, por ejemplo, es posible utilizar *Azure App Service* de forma gratuita durante 1 hora al día. [26]

8.1. Creación del Grupo de recursos y la red virtual

En primer lugar, es necesario crear un grupo de recursos, un contenedor que relaciona los recursos de Azure para una solución en concreto. [27]

Para crearlo es necesario indicar un nombre, la suscripción desde donde se cobrarán los recursos y la región donde se realizará el despliegue.

Ilustración 24: Creación de un grupo de recursos

A continuación, es necesario crear la red virtual, un entorno aislado en donde se desplegará la infraestructura. Los datos básicos de la misma incluyen la suscripción donde se cobrará, el grupo de recursos, el nombre y la región. [28]

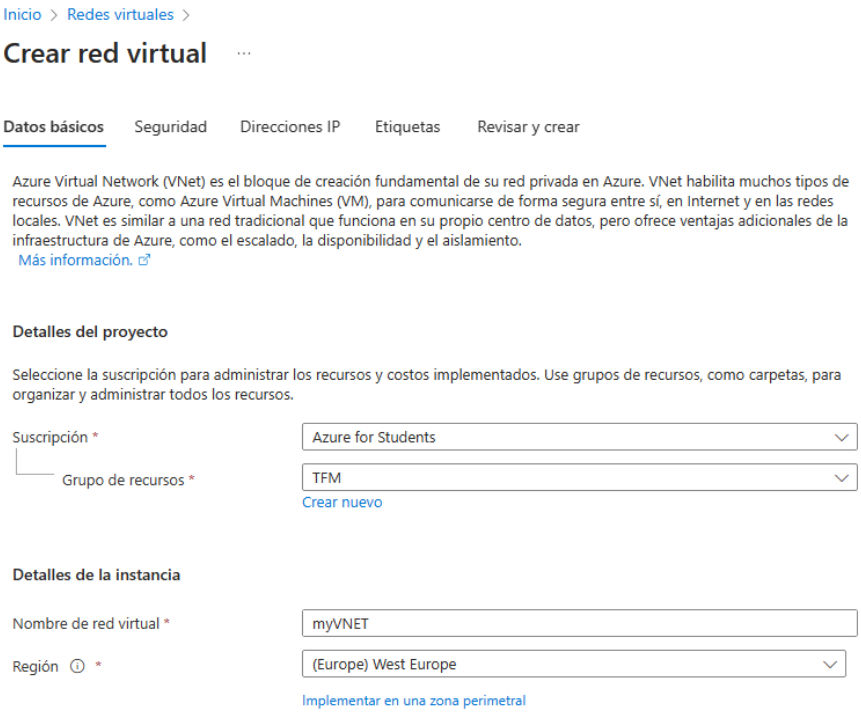


Ilustración 25: Datos básicos de la red virtual

Permite añadir cierta configuración de seguridad a toda la red virtual, como un Firewall que protege toda la red, protección DDOS o máquinas *Azure Bastion* para realizar conexiones SSH a las máquinas virtuales. En este caso no se seleccionará ninguno puesto que se utilizarán otros elementos.

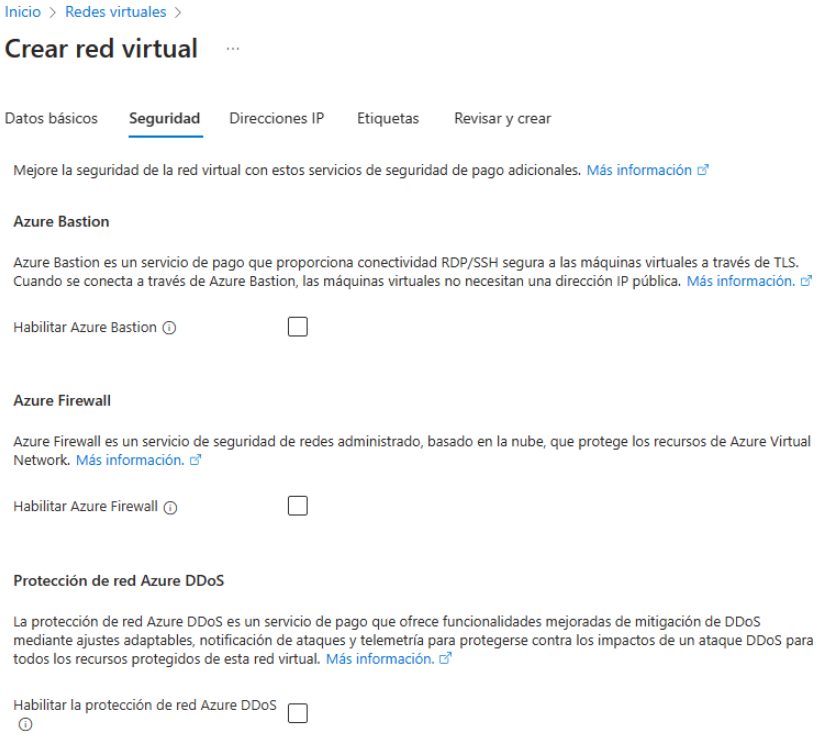


Ilustración 26: Seguridad de la red virtual

A continuación, permite definir el rango de direcciones privadas que estarán disponibles en la red virtual y definir diferentes subredes.

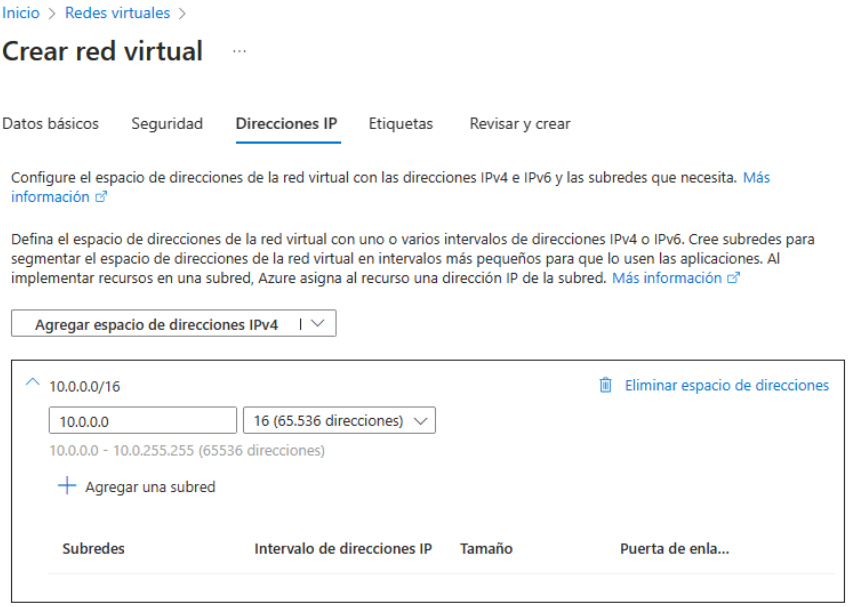


Ilustración 27: Direcciones de la red virtual

En las subredes virtuales también puede definirse el rango de direcciones, dentro de las de la red privada, que esta tendrá. Permite añadir ciertas opciones de seguridad, como una puerta de enlace NAT para conectar los servicios de forma privada a internet, un grupo de seguridad de red para limitar el tráfico y una tabla de rutas para enrutar el tráfico de la red. Crearemos un par de subredes privadas, una para el *Application Gateway* que actuará de puerta de entrada para la aplicación y otra para el *back-end* que contendrá los otros elementos.

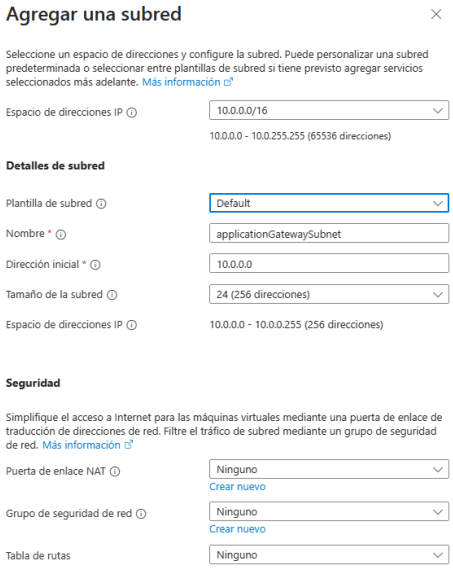


Ilustración 28: Creación de la subred del Application Gateway

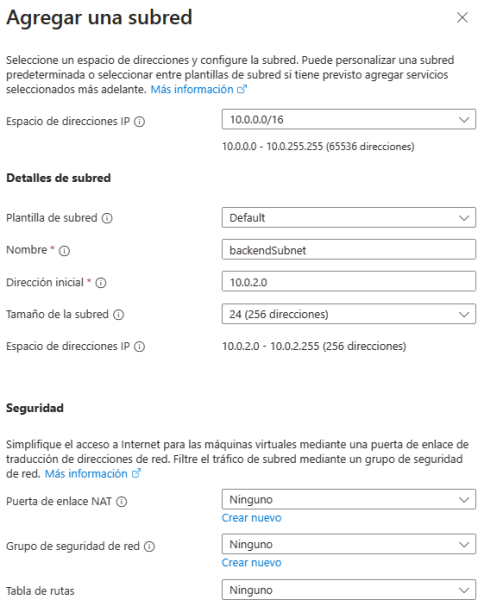


Ilustración 29: Creación de la subred del *back-end*

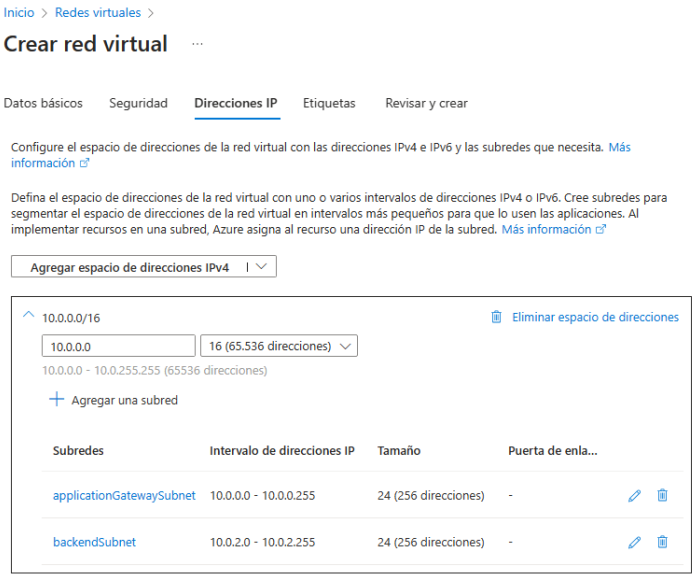


Ilustración 30: Red virtual y subredes creadas

Se podrá ver un resumen de la configuración al final y permitirá crear el recurso si no existen fallos en la misma.

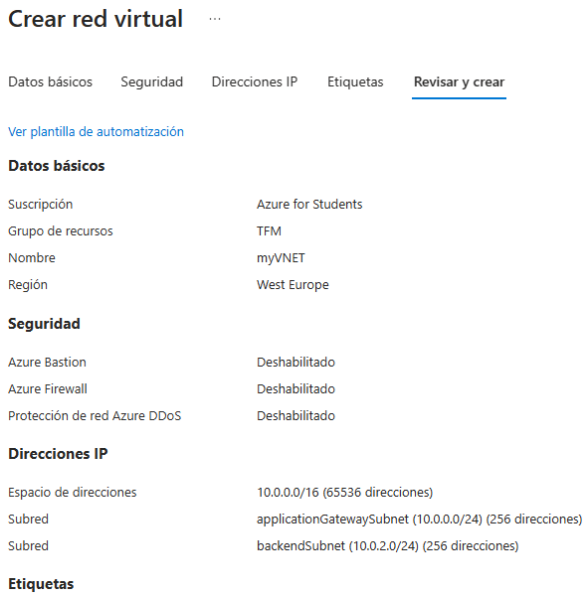


Ilustración 31: Resumen red virtual

8.2. Creación de una dirección IP pública

La creación de una dirección IP pública permitirá a un recurso realizar la conexión a internet. Se utilizará para permitir al *Application Gateway* exponer el servidor a internet. [29]

En primer lugar, será necesario indicar la región donde se generará, la versión IP, diferentes zonas de disponibilidad en caso de querer redundancia, el nivel de la IP que tendrá que ser global en caso de querer utilizar balanceadores de entre regiones y el SKU cuya versión estándar permite nivel global, zonas de redundancia y seguridad por defecto mediante grupos de seguridad.

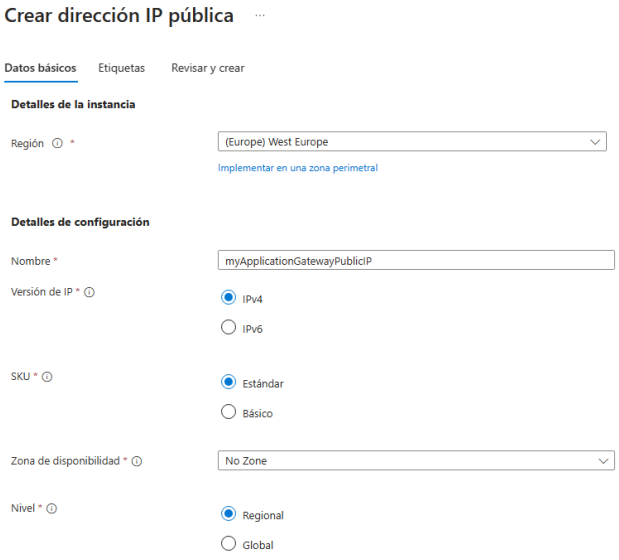


Ilustración 32: Datos básicos de la dirección IP

A continuación, puede indicarse si se quiere una asignación estática o dinámica (mediante SKU estándar sólo permite estática) y que enrutamiento se utilizara. Si se enruta el tráfico mediante la red de Microsoft es posible que se consiga una menor latencia al utilizar los puntos de presencia de Microsoft, aunque el coste será algo mayor.

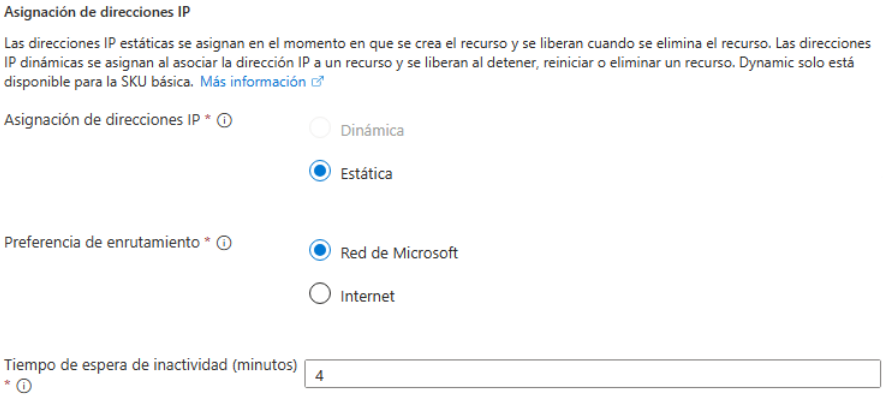


Ilustración 33: Preferencias de Dirección IP

8.3. Creación del Application Gateway

Un *Application Gateway* permitirá balancear la carga que se dirige al *back-end* y proteger el mismo analizando el tráfico mediante su Firewall de aplicaciones web (WAF). [30]

Algunos de los datos básicos para su creación incluyen:

- Tipo: Solo balanceador de carga o balanceador de carga y WAF.
- Escalado automático: Si se quiere que la puerta escale según la carga para no perder peticiones.
- Recuento de instancias: Número de instancias mínimo y máximo de la puerta. En caso de indicar 0 en el mínimo se podrá parar la instancia para ahorrar costes.
- Directiva WAF: Incluye las reglas que utilizará el WAF su creación se verá a continuación.
- Red virtual: La red virtual donde se desplegará y la subred del *Application Gateway*. Ambas ya han sido creadas anteriormente.

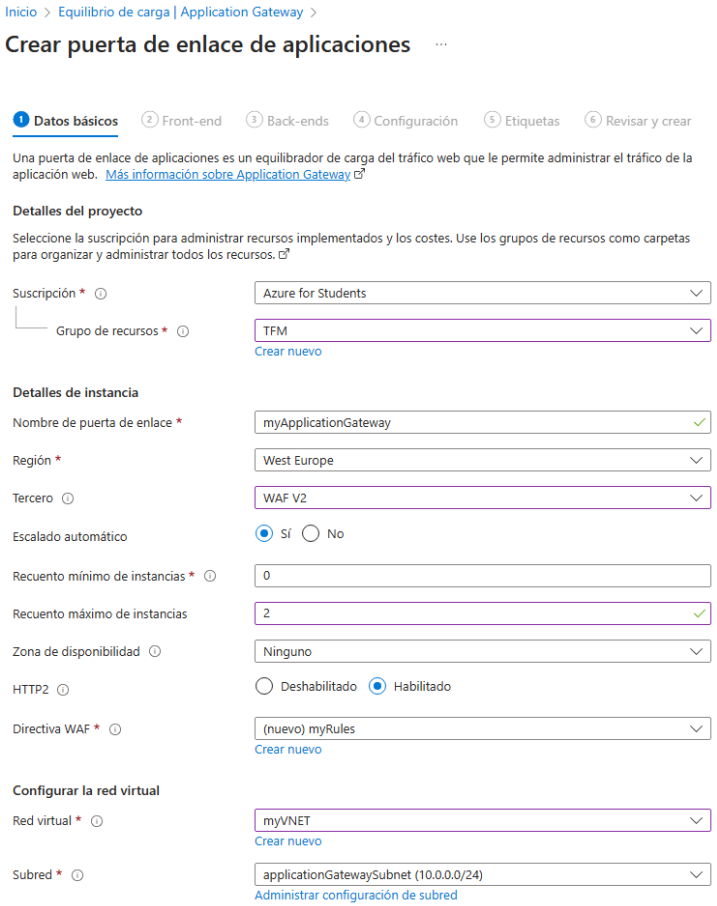


Ilustración 34: Datos básicos del *Application Gateway*

En el campo de reglas WAF permite definir las reglas (incluirá un conjunto por defecto) y agregar protección contra *bots*. Las reglas se verán con más profundidad en secciones posteriores.

Ilustración 35: Creación de reglas WAF

A continuación, nos permite crear una dirección IP, añadimos la creada anteriormente.

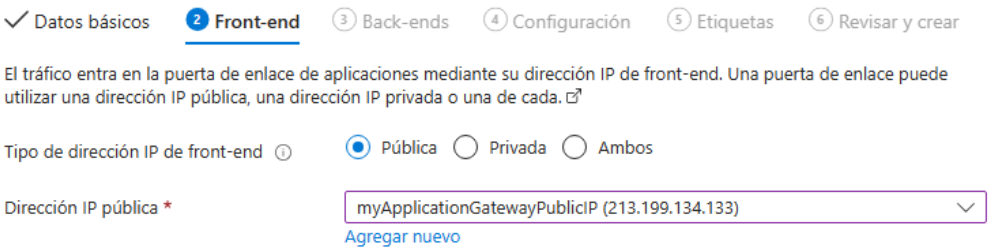


Ilustración 36: Dirección pública del *Application Gateway*

En próximo paso consiste en definir el *back-end* al que se conectara, es necesario crear un grupo *back-end* al que más tarde se añadirán las máquinas con la aplicación.

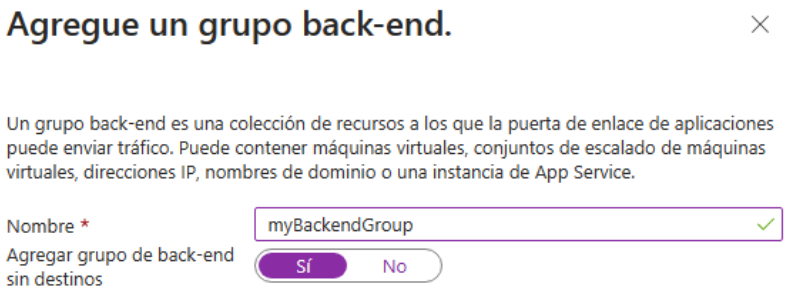


Ilustración 37: Creación de un grupo *back-end*

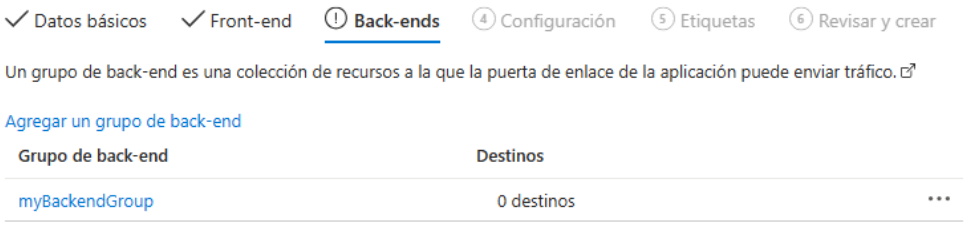


Ilustración 38: Configuración *back-end* en *Application Gateway*

A continuación, es necesario definir las reglas de enrutamiento de la puerta. Para ello hay que configurar un agente de escucha, de momento estará escuchando en el puerto 80. También se configurará el grupo *back-end* al que se enruta el tráfico, aunque de momento este se encontrará vacío.

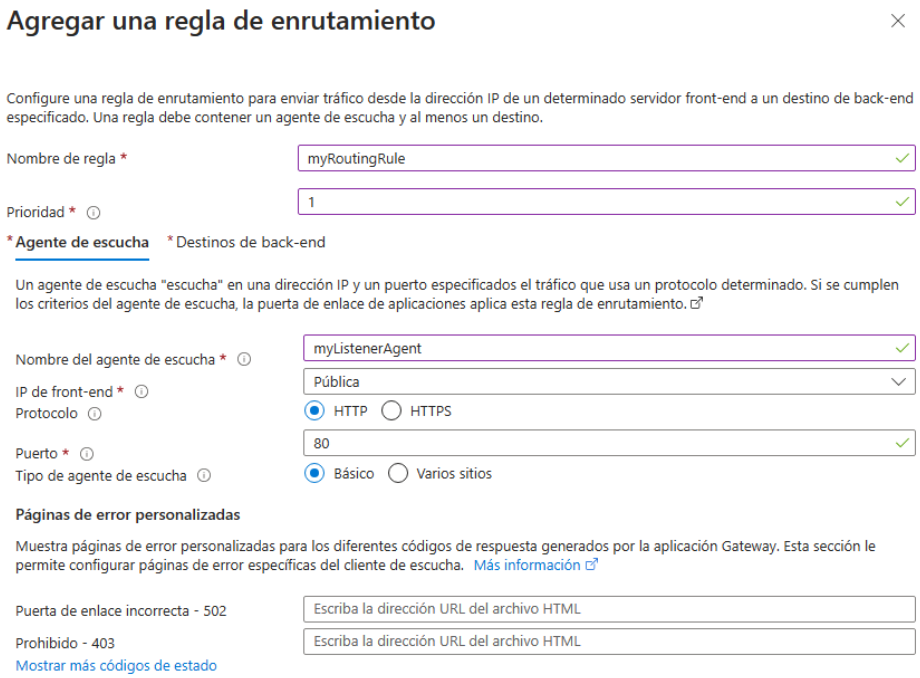


Ilustración 39: Agente de escucha para HTTP

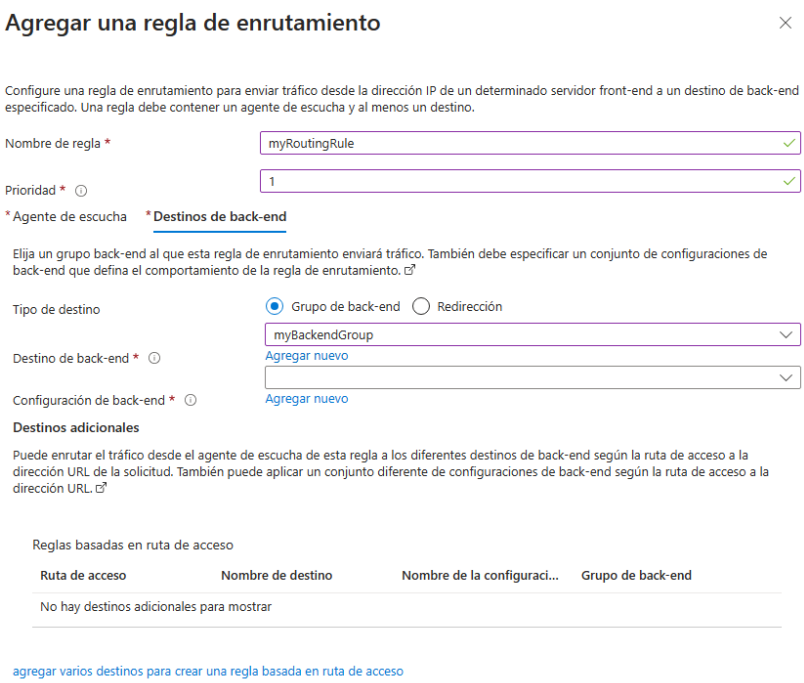


Ilustración 40: Regla de enrutamiento al *back-end* para HTTP

Para poder agregar el destino back-end, también será necesario añadir una configuración de back-end, esta de momento también realizará la conexión mediante HTTP.

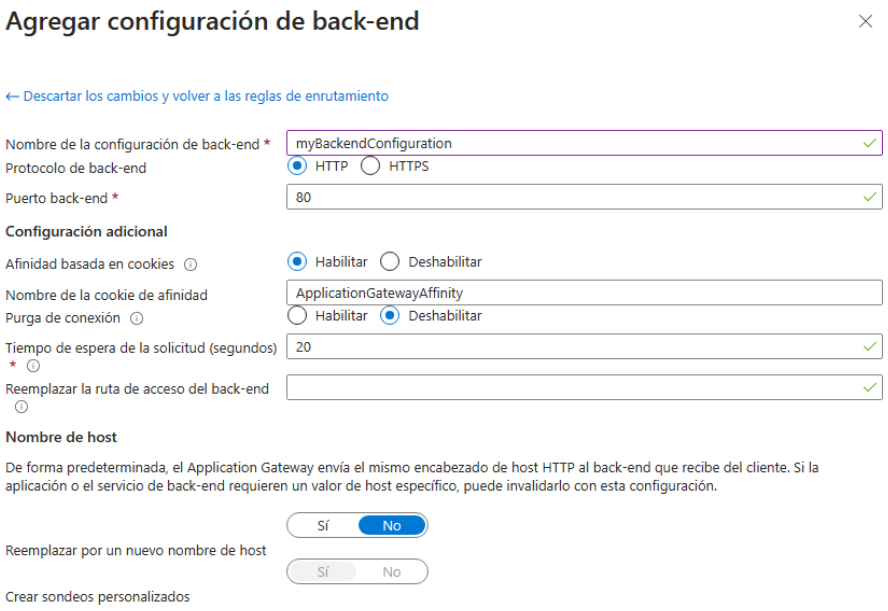


Ilustración 41: Creación de configuración de *back-end*

Se podrá observar un resumen con los 3 tipos de configuración (*front-end back-end* y reglas de enrutamiento) y crear el *Application Gateway* tras verificar la configuración.

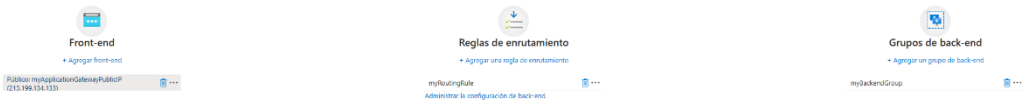


Ilustración 42: Resumen de configuraciones en Application Gateway

8.4. Creación de una cuenta de almacenamiento

Se utilizarán los recursos compartidos de archivos NFS para mantener los datos de WordPress entre las diferentes máquinas virtuales. Para ello será necesario crear una cuenta de almacenamiento donde se crearán los recursos compartidos. [31]

En primer lugar, se añadirán algunos datos básicos, se utilizará una cuenta premium puesto que el acceso a la misma será constante y se seleccionará la cuenta de tipo recursos compartidos de archivos para poder compartir los archivos de WordPress entre las máquinas. Como se desplegará en un ámbito regional puede utilizarse un almacenamiento con redundancia local.

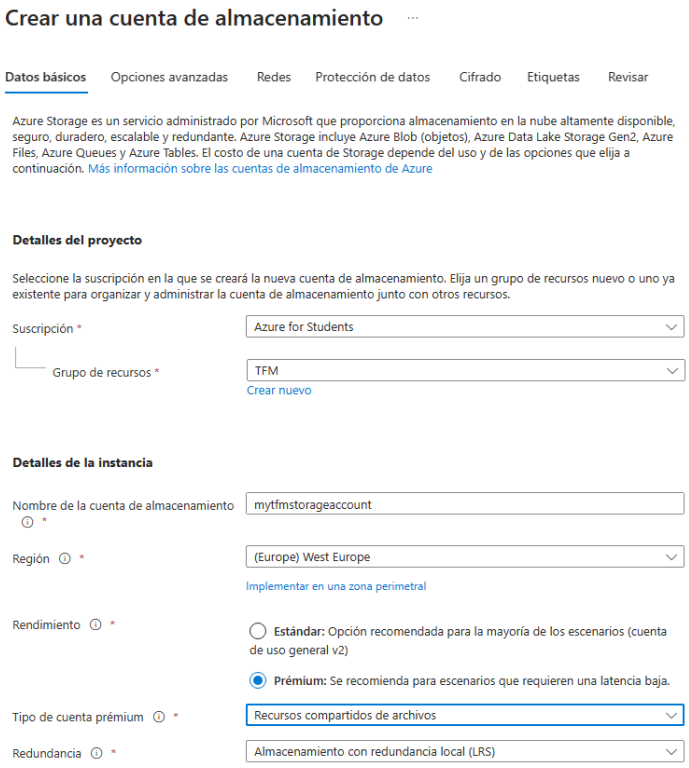


Ilustración 43: Datos básicos de una cuenta de almacenamiento

A continuación, pueden definirse las redes que podrán conectarse a la cuenta. Se habilitará el acceso desde la red virtual, seleccionando además el acceso solo a la subred del *back-end* donde se encontrarán los servidores.

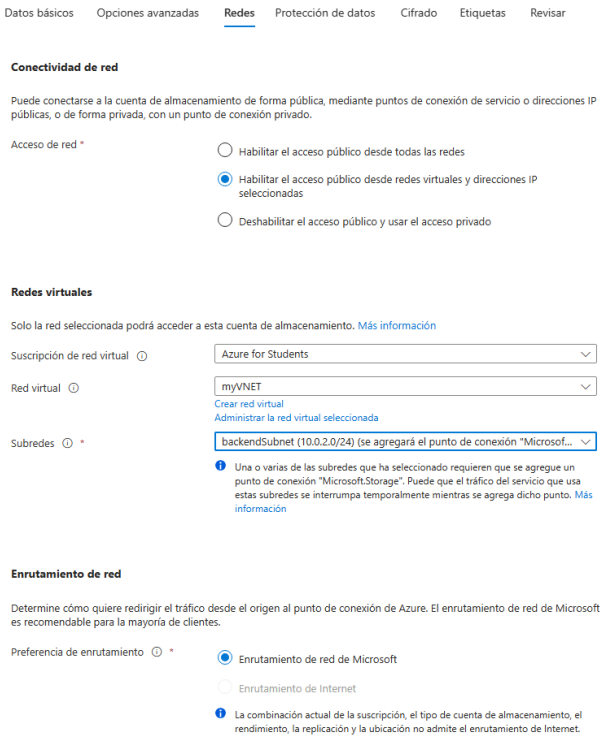


Ilustración 44: Redes de la cuenta de almacenamiento

Se habilitará la eliminación temporal de los recursos para que solo se eliminen por completo pasado un tiempo para proteger los datos en caso de una eliminación accidental.

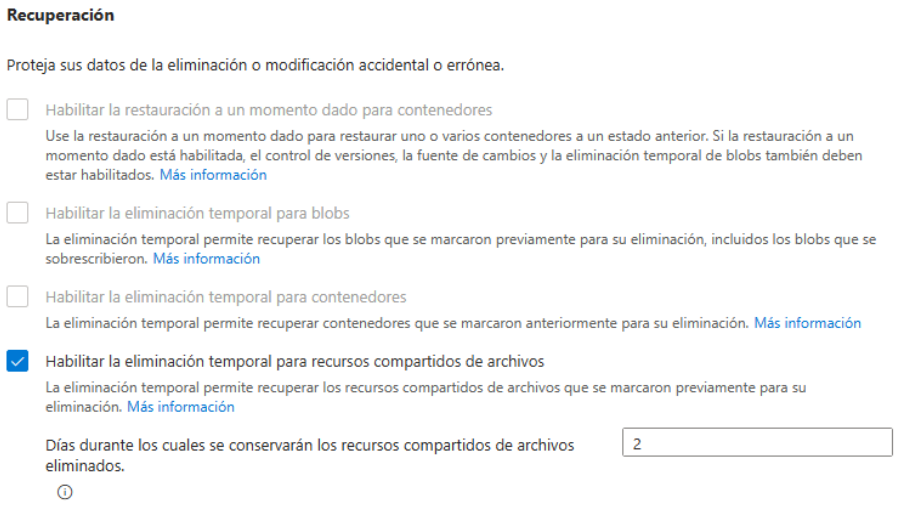


Ilustración 45: Recuperación de los datos la cuenta de almacenamiento

Se seleccionará el cifrado de archivos y permitiremos que Microsoft sea el encargado de administrar las claves.

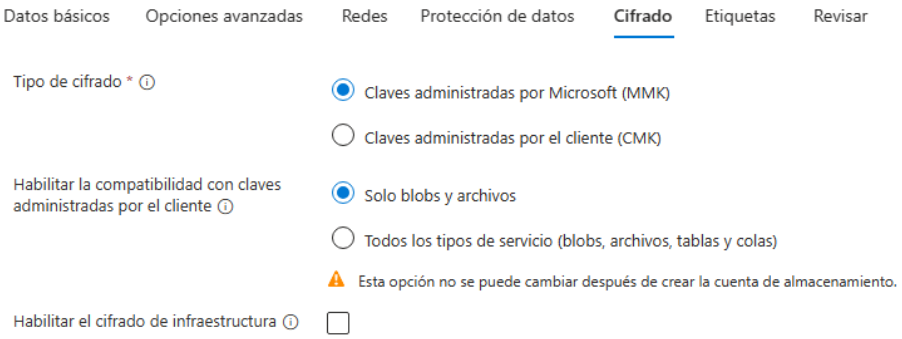


Ilustración 46: Cifrados de archivos en la cuenta de almacenamiento

8.5. Creación de recursos compartidos mediante NFS

Sera necesario crear un recurso compartido de archivos que será el que utilizaran las máquinas, se puede crear desde la cuenta de almacenamiento. [32]

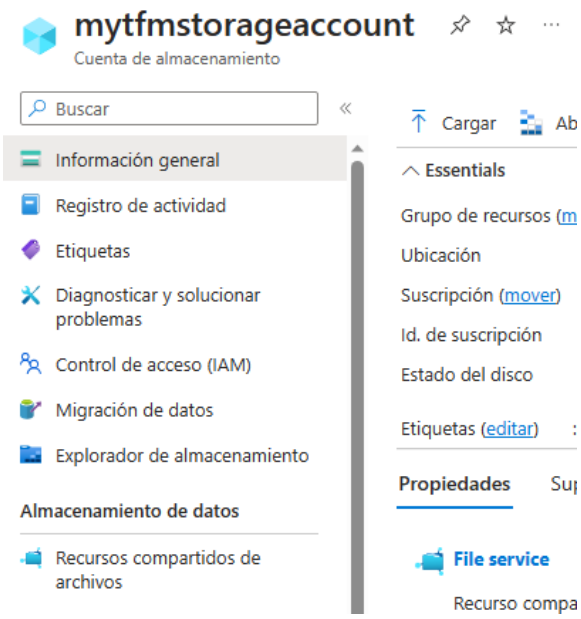


Ilustración 47: Recursos compartidos de archivos

Será necesario aprovisionar la capacidad del almacenamiento y seleccionar el protocolo utilizado.

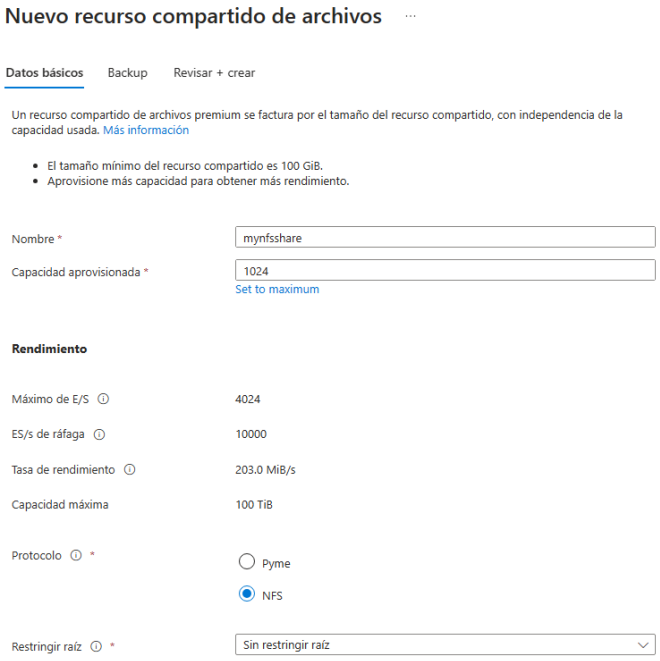


Ilustración 48: Creación de un recurso compartido

8.6. Configuración de un punto de conexión privado

Un punto de conexión privado proporcionará a la cuenta de almacenamiento una dirección IP privada. En los datos básicos de su creación se tendrá que añadir el nombre y la región. Se generará una interfaz de red en el proceso.

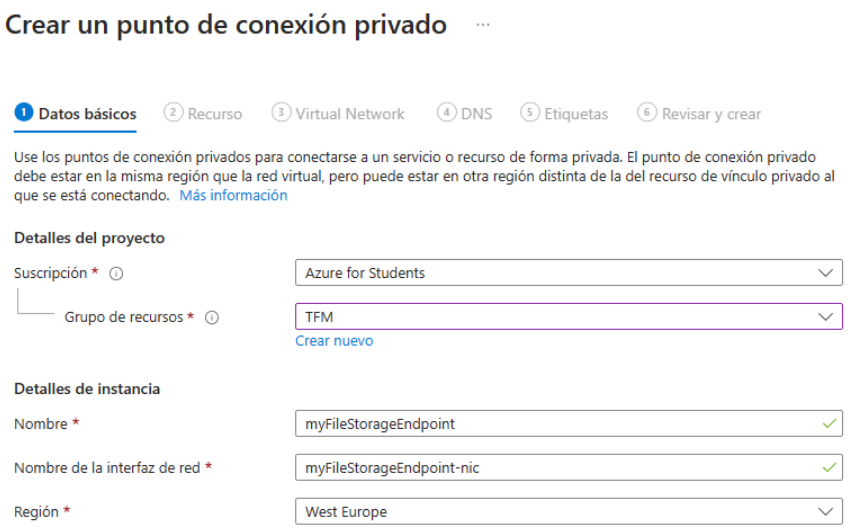


Ilustración 49: Datos básicos de un punto de conexión privado

A continuación, tendrá que proporcionar el id del recurso que se enlazará al punto de conexión. Para poder ver el id de la cuenta de almacenamiento se tendrá que abrir la vista de JSON del recurso.

Ilustración 50: JSON de la cuenta de almacenamiento

Tras incluir el id seleccionaremos el subrecurso de la cuenta al que se conectara.

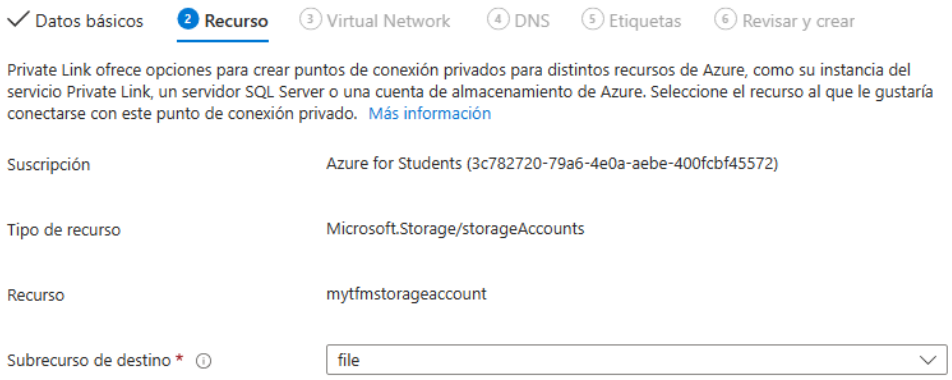


Ilustración 51: Selección del subrecurso para el punto privado

A continuación, se añadirá la red y subred a la que pertenece y si la dirección privada será estática o dinámica.

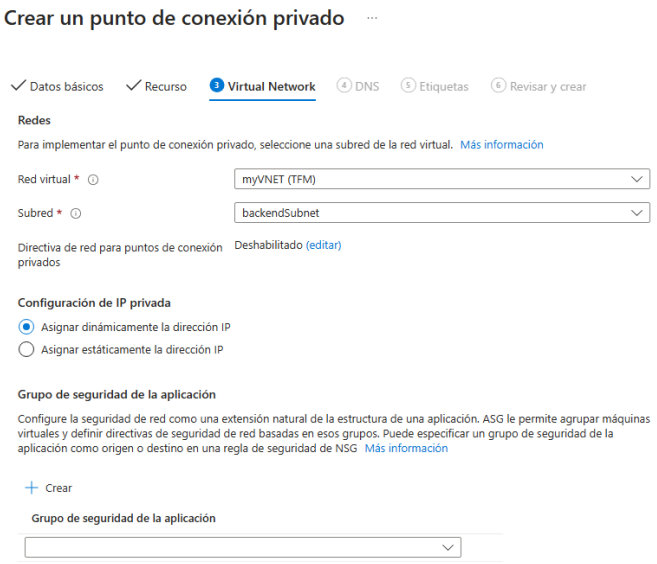


Ilustración 52: Red virtual del punto de conexión privado

Por último, se creará una zona DNS privada que permitirá utilizar nombres de dominio personalizados para la cuenta de almacenamiento.

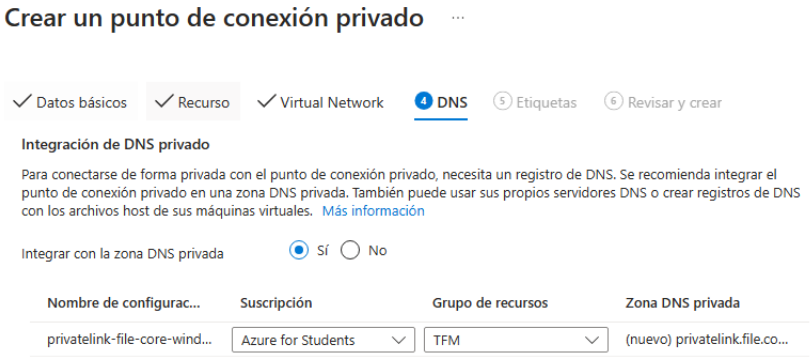


Ilustración 53: Creación de una zona DNS privada

8.7. Creación de la base de datos

Se utilizará MySQL flexible server para crear la base de datos que será utilizada por WordPress. [33]

La base de datos se configurará de manera que el coste sea el menor posible, por lo tanto, se desactivaran algunas opciones como la alta disponibilidad y se configurara la copia de seguridad para que solo tenga redundancia local y que ésta sea retenida durante un día. El almacenamiento de la base de datos, el rendimiento y el *tier* serán también los más bajos.

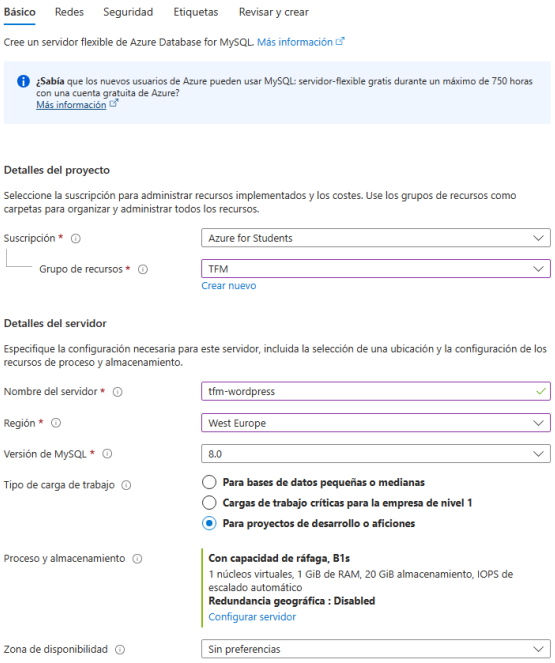


Ilustración 54: Datos básicos de la base de datos

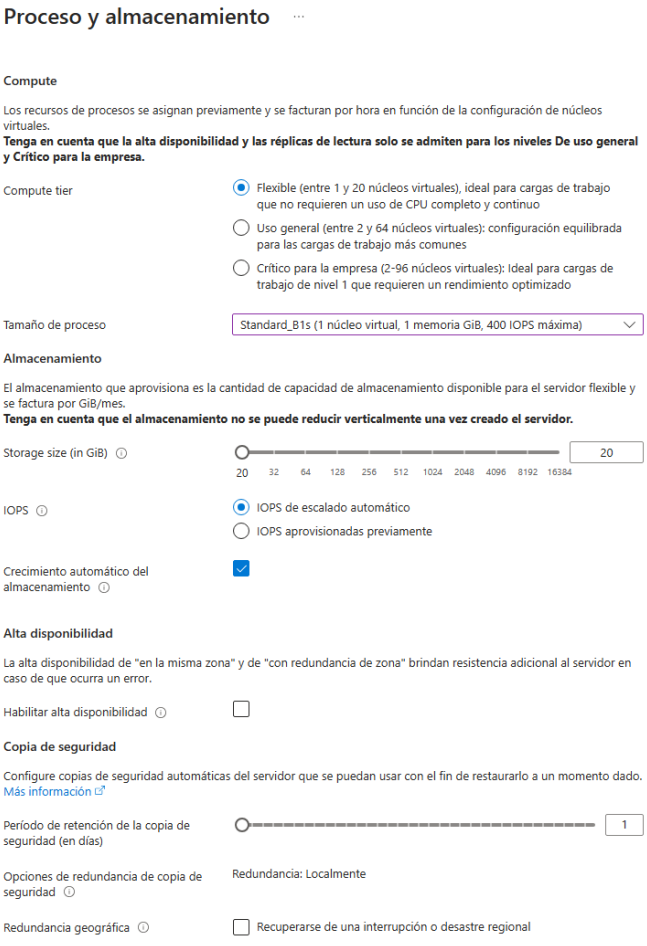


Ilustración 55: Configuración del proceso y almacenamiento

Se crearán las credenciales del administrador de la base de datos, para generar una contraseña segura se puede utilizar algún gestor de contraseñas, como por ejemplo KeePassXC.

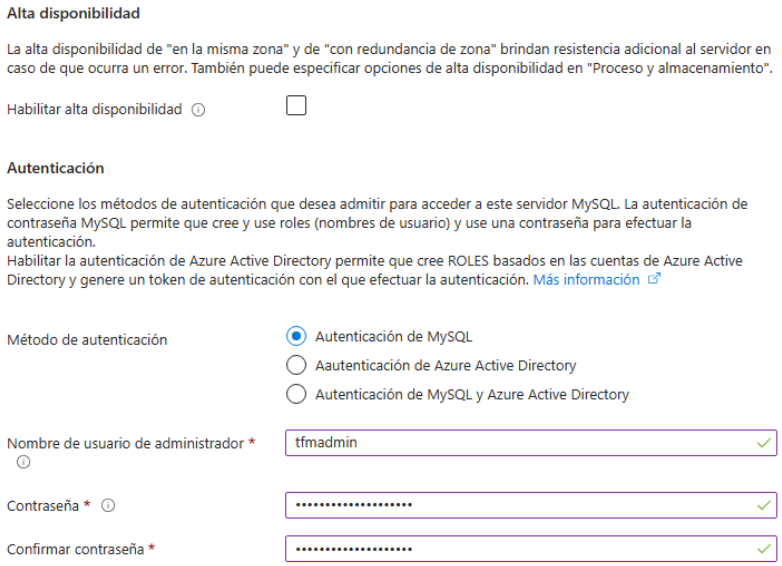


Ilustración 56: Credenciales de la base de datos

Sera necesario crear un punto de acceso privado dentro de la subred para poder realizar conexiones privadas a la base de datos.

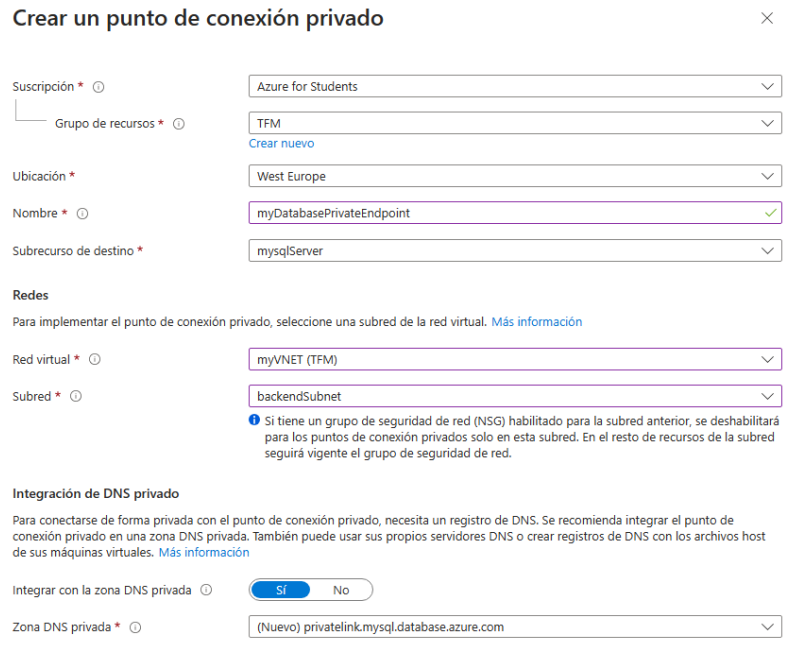


Ilustración 57: Creación de un punto de conexión privado

En la configuración de red será necesario aceptar el acceso público para poder utilizar el punto de conexión, aunque este no tendrá acceso a internet.

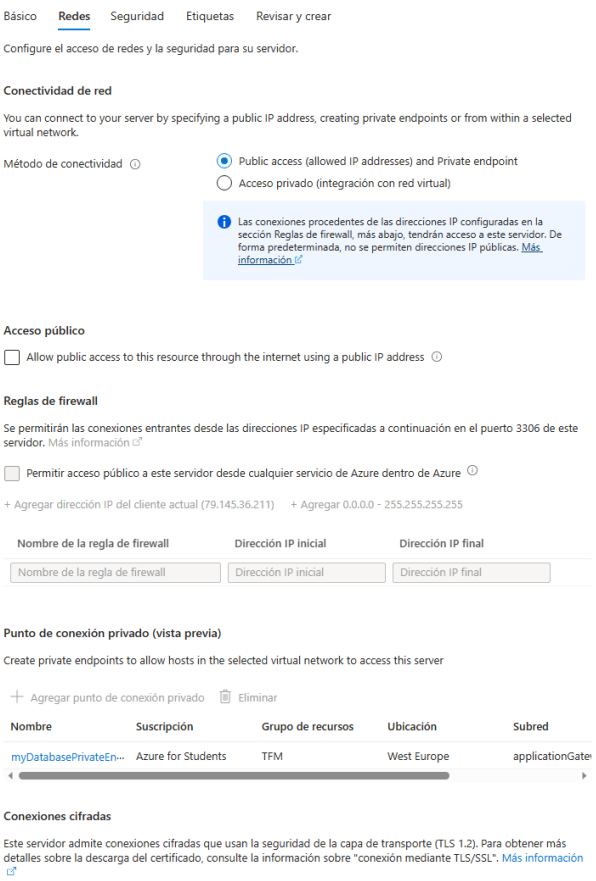


Ilustración 58: Configuración de red de la base de datos

Una vez creada podemos ver la configuración de las copias de seguridad, también se pueden realizar de forma manual. Las copias se realizan de manera automática una vez al día, estas son eliminadas tras un día para ahorrar costes en el despliegue de prueba.

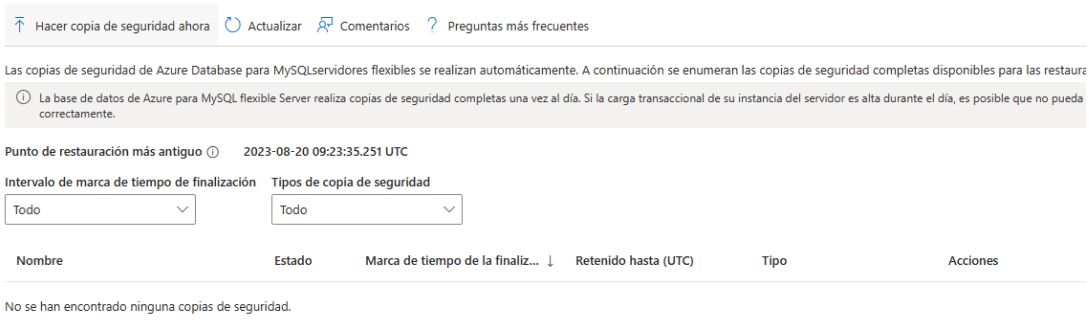


Ilustración 59: Copias de seguridad en MySQL flexible server

A continuación, crearemos la base de datos que utilizará WordPress desde la propia interfaz de MySQL flexible server.

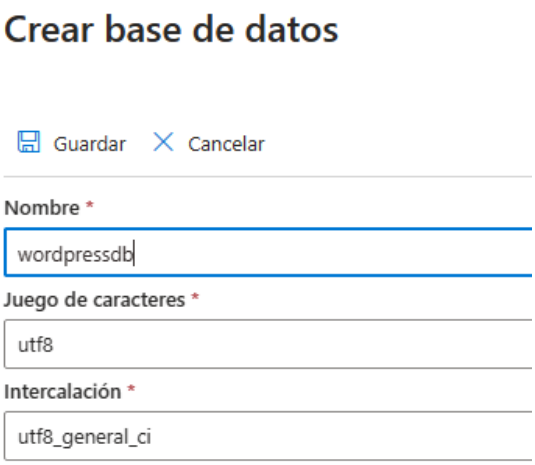


Ilustración 60: Creación de la base de datos de Wordpress

Es necesario crear el usuario de WordPress que solo tendrá acceso a esta base de datos, para poder realizar la conexión habilitaremos una IP pública y en las reglas del Firewall permitiremos solo conexiones desde servicios de Azure, de esta manera se podrá utilizar la terminal de Azure para realizar la conexión a la base de datos.

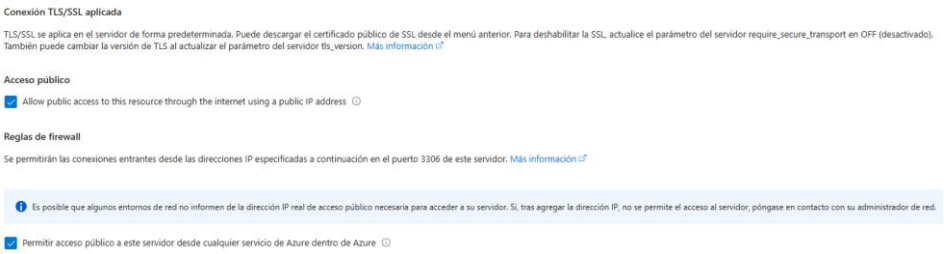


Ilustración 61: Opciones de conexión de la base de datos

A continuación, realizamos la conexión y creamos el usuario para WordPress.

```
bv100003 [ ~ ]$ mysql -h tfm-wordpress.mysql.database.azure.com -u tfmadmin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 8.0.32 Source distribution
```

Ilustración 62: Conexión a la base de datos

```
mysql> CREATE USER 'wordpress-user'@'%' IDENTIFIED BY 'eMgUqjvu0O0v3SI7hGsy';
Query OK, 0 rows affected (0.02 sec)
```

Ilustración 63: Creación del usuario de la base de datos

```
mysql> GRANT ALL PRIVILEGES ON wordpressdb . * TO 'wordpress-user'@'%';
Query OK, 0 rows affected (0.01 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.01 sec)
```

Ilustración 64: Privilegios del usuario para la base de datos

8.8. Creación del conjunto de máquinas virtuales

Se generará un conjunto de máquinas virtuales que compartirán la carpeta de WordPress mediante los recursos compartidos creados anteriormente.

Se utilizará una imagen con WordPress ya instalado, la carpeta con WordPress se moverá a la ruta donde se monte el almacenamiento de los recursos compartidos, esto solo será necesario realizarlo una vez para evitar sobrescribir los ficheros. Durante la configuración se marcará la ejecución con Azure Spot para conseguir un descuento y se seleccionará la configuración de rendimiento más económica, también se generarán un par de claves para poder realizar conexiones SSH a las máquinas.

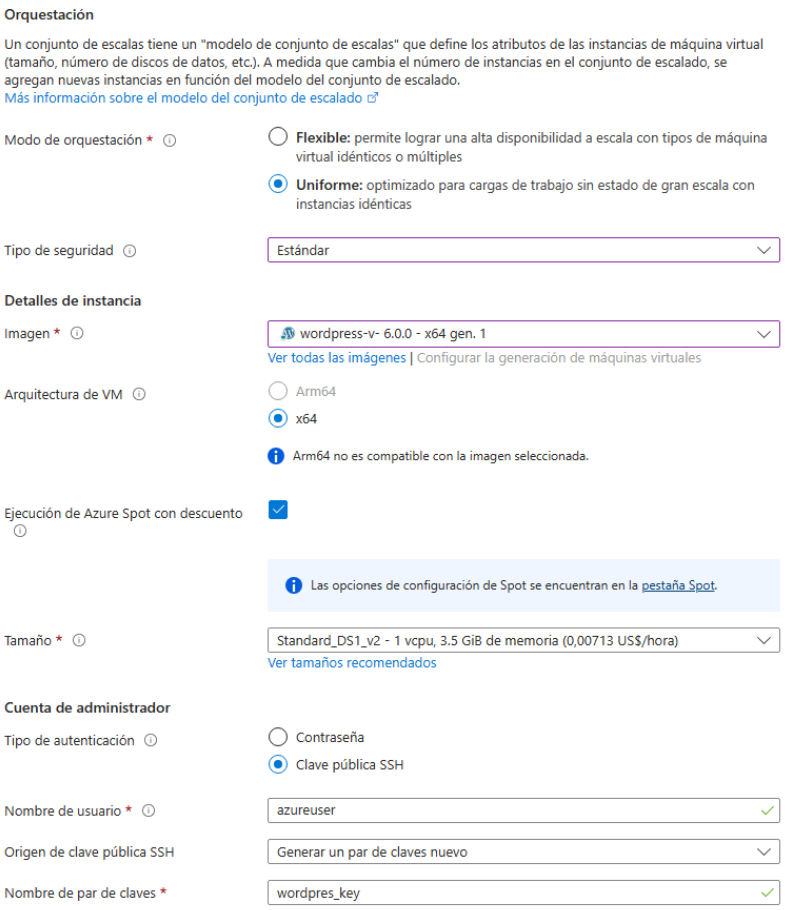


Ilustración 65: Datos básicos de VMSS

Configuraremos que se detenga la máquina automáticamente en caso de que supere cierto gasto por hora.

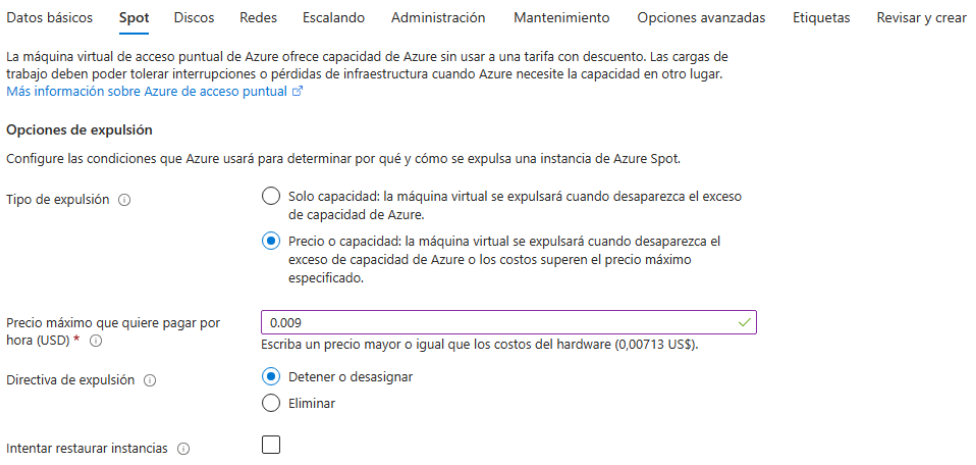


Ilustración 66: Configuración Azure Spot

Se elegirá un disco HDD con una clave de cifrado administrada por Azure.

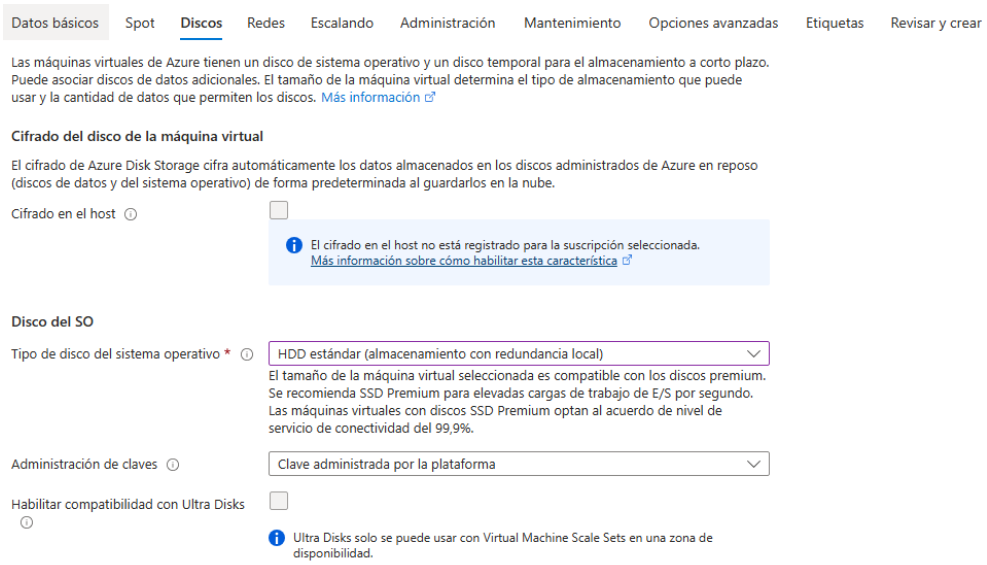


Ilustración 67: Configuración de disco de VMSS

En la configuración de red se creará una nueva interfaz de red para las máquinas y se elegirá el *Application Gateway* creado anteriormente como equilibrador de carga, también se añadirá el conjunto de máquinas al grupo de *back-end* que se creó anteriormente.

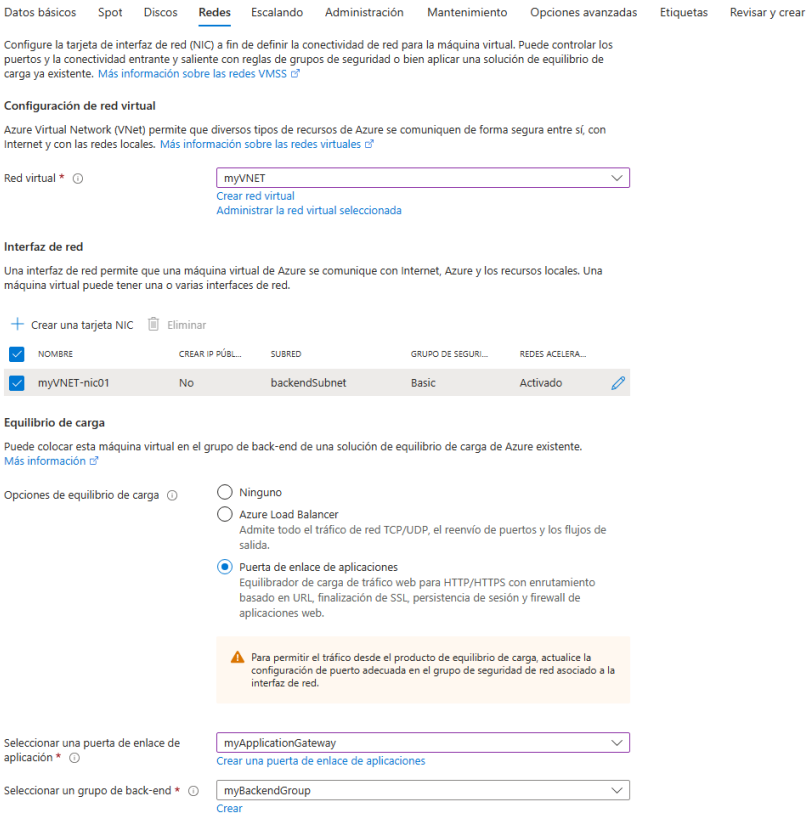


Ilustración 68: Configuración de red de VMSS

Para poder realizar conexiones SSH a las máquinas añadiremos una IP pública a la interfaz de red y permitiremos el tráfico por el puerto 22. Esto podrá ser modificado cuando se puedan realizar conexiones mediante VPN.

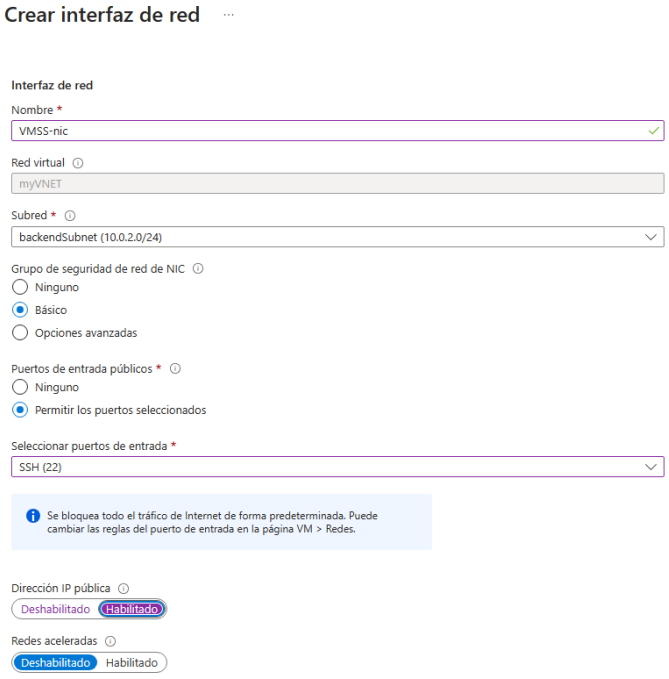


Ilustración 69: Configuración de la interfaz de red para VMSS

Para realizar pruebas activaremos el escalado manual y solo una instancia puesto que no serán necesarias más.

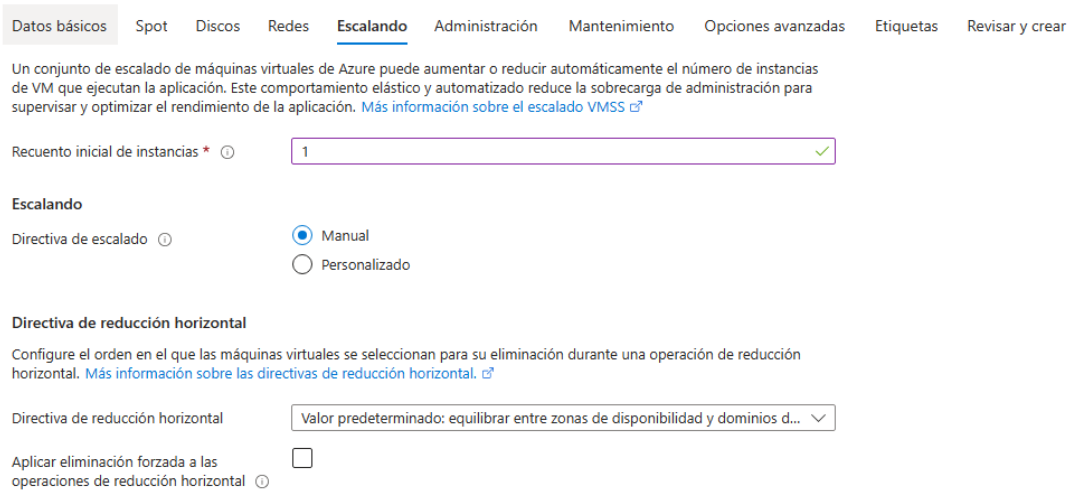


Ilustración 70: Configuración escalado de VMSS

En las opciones avanzadas añadiremos un script *cloud-init* para realizar configuraciones en las máquinas cuando estas se inicien.

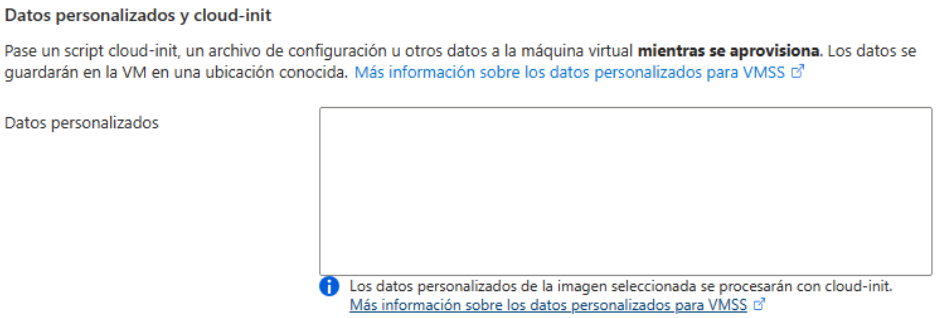


Ilustración 71: Opciones avanzadas en VMSS

El script puede realizar las siguientes tareas:

- Actualización de librerías.
- Montaje de la carpeta con los archivos compartidos de WordPress.
- Creación del archivo .htaccess.
- Creación de los certificados necesarios para realizar la conexión SSL.
- Modificación del archivo de configuración de Apache.
- Modificación de archivo wp-config.
- Reinicio de Apache.

Puede encontrarse un ejemplo de este script en el material complementario entregado junto a la memoria.

Una vez creado el conjunto se puede hacer un seguimiento de sus máquinas y observar la consola serie para ver cuando el *cloud-init* termina de ejecutarse.

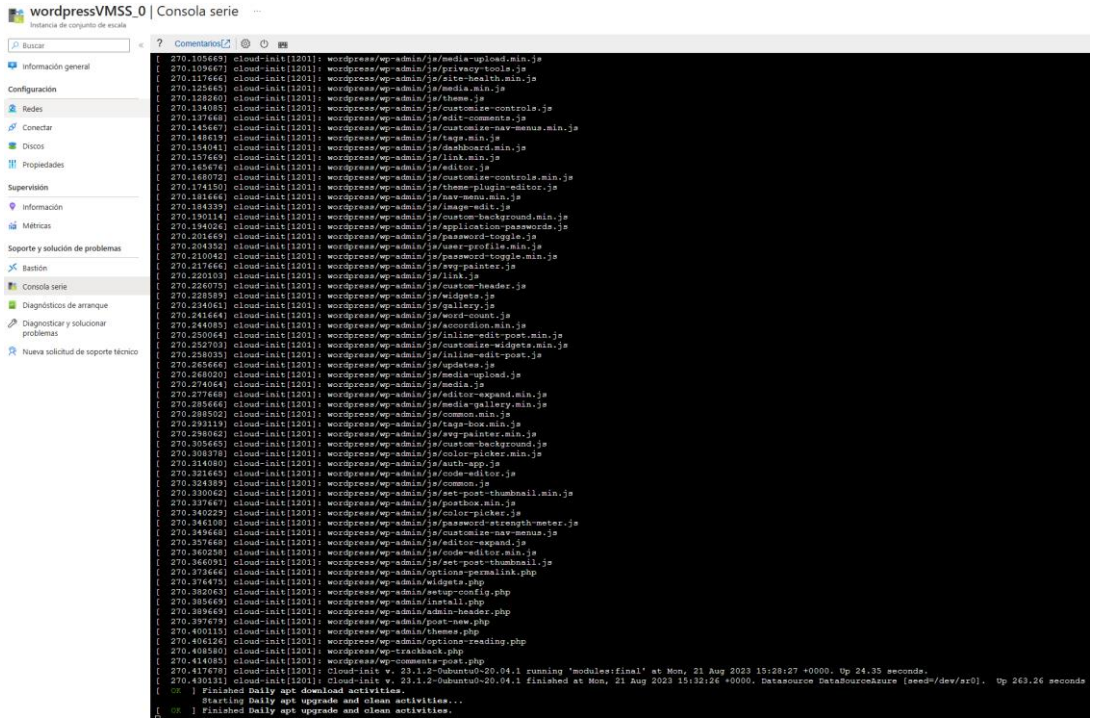


Ilustración 72: Consola serie de las máquinas

Se puede comprobar la conexión a las máquinas mediante SSH, aunque de momento esta se realizara mediante IP pública.

Ilustración 73: Conexión a la máquina mediante SSH

Podemos comprobar que el montaje del recurso compartido se ha realizado correctamente.

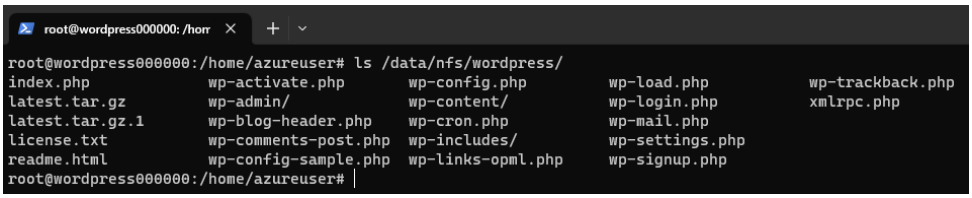


Ilustración 74: Montaje del recurso compartido

Comprobamos que podemos conectarnos a través de la IP del *Application Gateway* mediante HTTP.

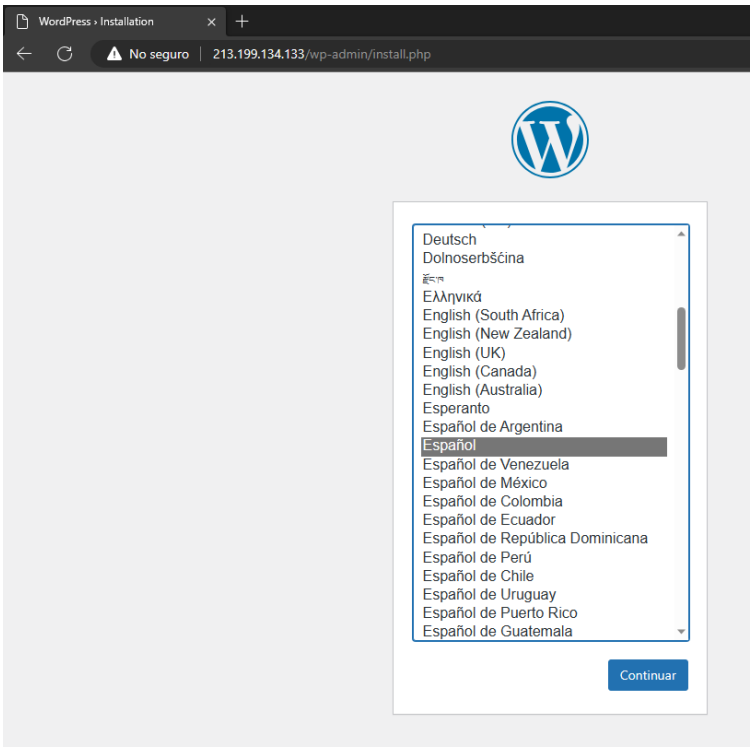


Ilustración 75: Acceso a la web

Puesto que hemos generado el archivo de configuración de WordPress mediante el *cloud-init* no nos pedirá la base de datos durante la instalación. Procedemos a generar una contraseña mediante un gestor de contraseñas y a añadir el usuario administrador.

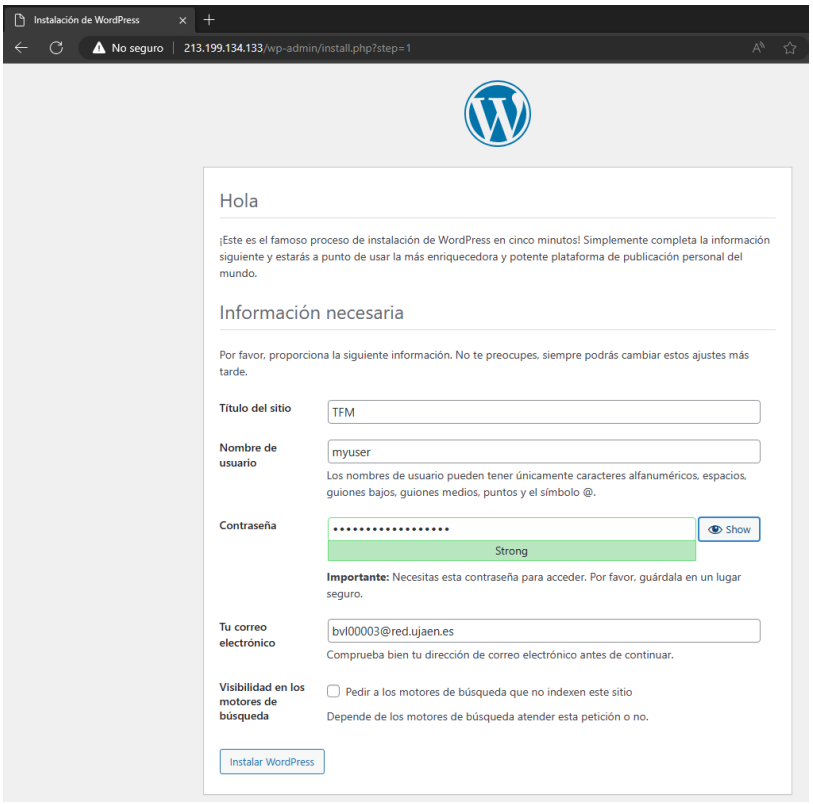


Ilustración 76: Configuración de la cuenta de administración en Wordpress

Cuando termine la instalación ya podremos acceder a la web y al panel de administración.

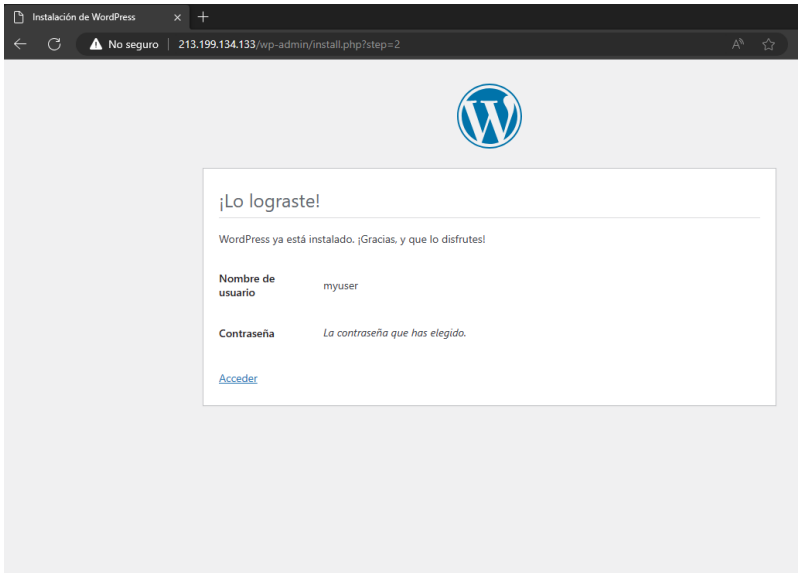


Ilustración 77: Instalación de Wordpress terminada

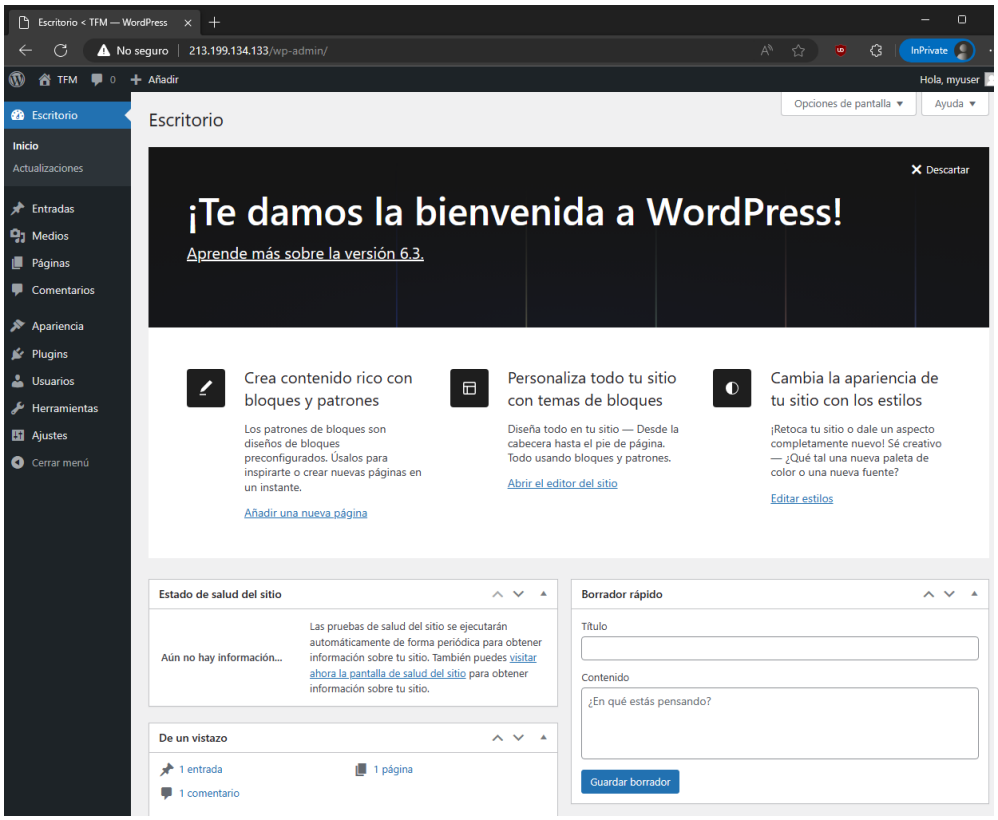


Ilustración 78: Panel de administración de Wordpress

8.9. Configuración SSL en Application Gateway

En el *Application Gateway* pueden configurarse certificados para habilitar SSL tanto entre el cliente y el *Application Gateway*, como entre el *Application* Gateway y el servidor. [34]

Si se tratara de un entorno de producción lo ideal sería utilizar una entidad certificadora externa para firmar los certificados del servidor y el *Application Gateway*, sin embargo, en este entorno de experimentación generaremos un certificado raíz para firmar estos certificados [35]. Primero debe generarse una clave cifrada y una solicitud de firma de certificado mediante los siguientes comandos:

```
openssl ecparam -out cert.key -name prime256v1 -genkey
openssl req -new -sha256 -key cert.key -out cert.csr
```

A continuación, se genera el certificado raíz:

```
azureuser@wordpress000000:~$ openssl x509 -req -sha256 -days 365 -in cert.csr -signkey cert.key -out cert.crt
Signature ok
subject=C = ES, ST = Ja\C3\83\C2\A9n, L = Ja\C3\83\C2\A9n, O = TFM, OU = IT, CN = Blas, emailAddress = bvl00003@red.ujaen.es
Getting Private key
```

Ilustración 79: Generación de un certificado raíz

Ya se pueden obtener los certificados para el servidor y el Application Gateway, ambos se generan de la misma forma. En primer lugar, se obtiene la clave del certificado y la solicitud de firma de la misma manera que se ha visto anteriormente.

```
azureuser@wordpress000000:~$ openssl req -new -sha256 -key cert.key -out cert.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Jaén
Locality Name (eg, city) []:Jaén
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TFM
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:213.199.134.133
Email Address []:bvl00003@red.ujaen.es
```

Ilustración 80: Generación de una solicitud de firma

Es importante añadir el host que servirá el *Application Gateway* (en este caso una IP) en ambos certificados dentro del campo *Common Name*, puesto que el servidor también utilizará ese host. A continuación, se firma con el certificado raíz:

```
azureuser@wordpress000000:~$ openssl x509 -req -in cert.csr -CA ./root_certificates/cert.crt -CAkey ./root_certificates/
cert.key -CAcreateserial -out cert.crt -days 365 -sha256
Signature ok
subject=C = ES, ST = Ja\C3\83\C2\A9n, L = Ja\C3\83\C2\A9n, O = TFM, OU = IT, CN = 213.199.134.133, emailAddress = bvl000
03@red.ujaen.es
Getting CA Private Key
```

Ilustración 81: Generación de un certificado firmado

Una vez se tiene el certificado hay que generar un nuevo agente de escucha para el puerto 443 en el *Application Gateway*:

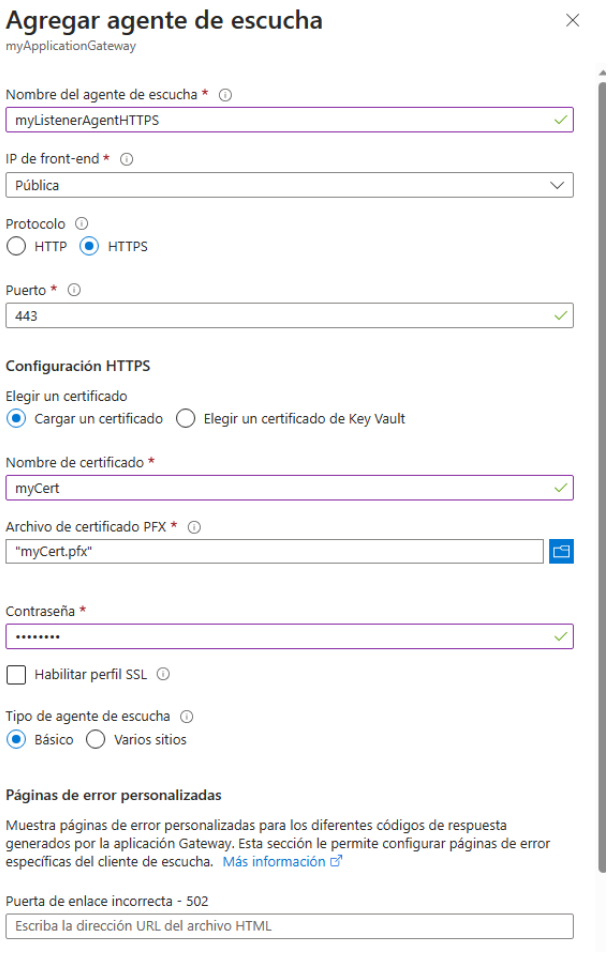


Ilustración 82: Configuración agente de escucha HTTPS

Es necesario generar el certificado en formato pfx así que lo creamos mediante el anterior:

```
azureuser@wordpress000000:~$ openssl pkcs12 -export -out cert.pfx -inkey cert.key -in cert.crt
Enter Export Password:
Verifying - Enter Export Password:
azureuser@wordpress000000:~$
```

Ilustración 83: Generación de un certificado pfx

A continuación, creamos una nueva regla de enrutamiento para el agente de escucha que nos lleve a los servidores del *back-end*:

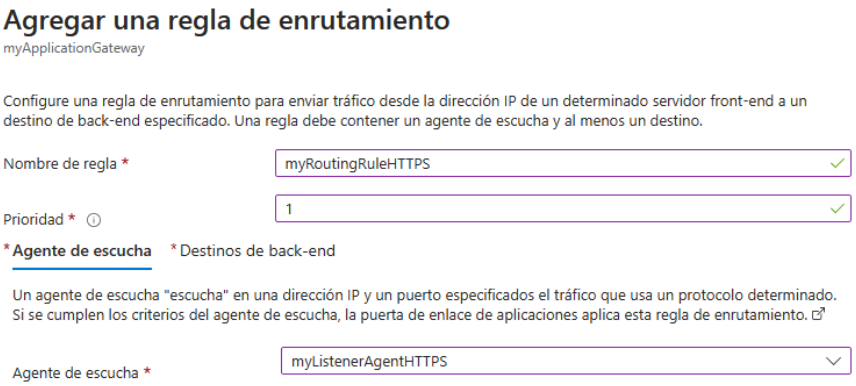


Ilustración 84: Regla de enrutamiento HTTPS

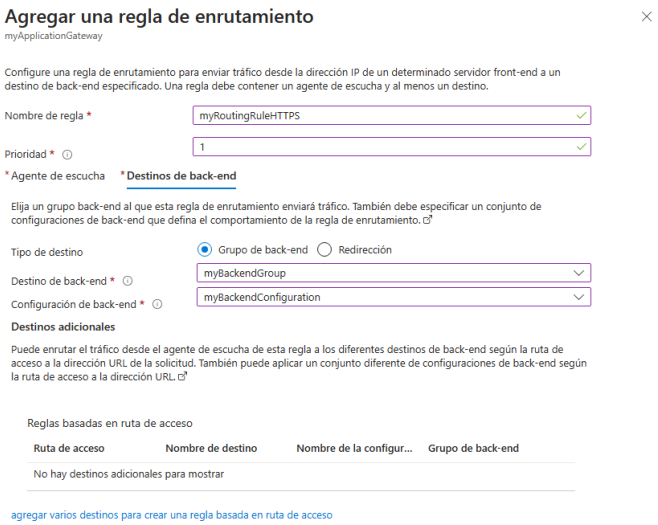


Ilustración 85: Regla de enrutamiento HTTPS a *back-end*

Modificamos la regla de enrutamiento del puerto 80 para que redirija al agente de escucha del puerto 443:

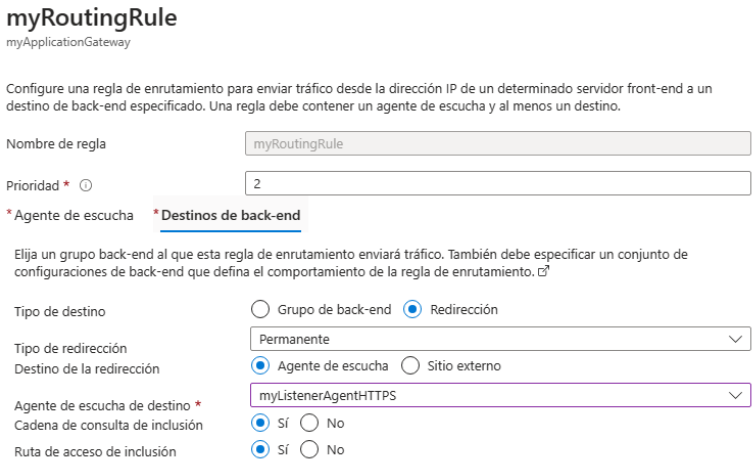


Ilustración 86: Agente de escucha redirigido a puerto 443

A continuación, vamos a añadir SSL entre el servidor y el *Application Gateway*, para ello movemos el certificado y la clave privada a los almacenes para que sean obtenidos por apache:

```
root@wordpress000000:/home/azureuser# mv cert.crt /etc/ssl/certs/apache-selfsigned.crt
root@wordpress000000:/home/azureuser# mv cert.key /etc/ssl/private/apache-selfsigned.key
root@wordpress000000:/home/azureuser#
```

Ilustración 87: Almacén de certificados en el servidor

Modificamos el archivo de configuración de apache para escuchar el puerto 443 y añadimos las siguientes líneas:

```
<VirtualHost *:443>

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
    SSLCertificateChainFile /home/azureuser/root_certificates/cert.crt
```

A continuación, activamos SSL en el servidor:

```
root@wordpress000000:/etc/apache2# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@wordpress000000:/etc/apache2# service apache2 restart
```

Ilustración 88: Activación SSL en Apache

Por último, es necesario modificar la configuración del *back-end* en Application Gateway, cambiando el protocolo a HTTPS y añadiendo el certificado raíz que ha firmado el certificado del servidor:

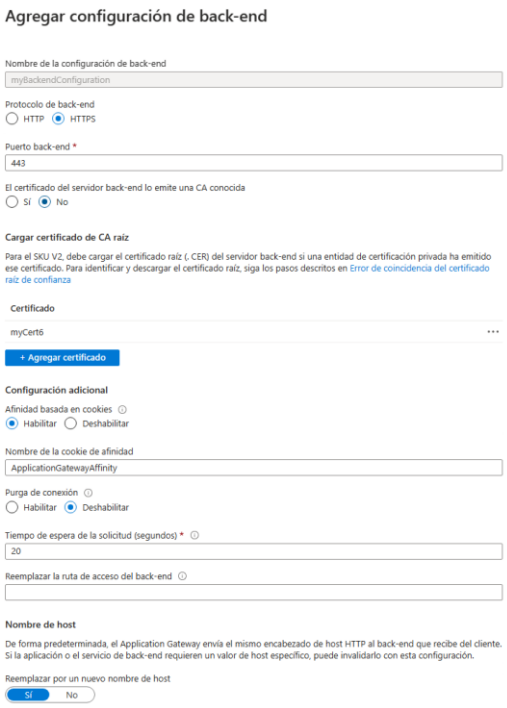


Ilustración 89: Configuración del *back-end* para HTTPS

Para asegurar que el *Application Gateway* acepte el certificado del servidor, reemplazamos el nombre del host por el dominio específico usado en el certificado:

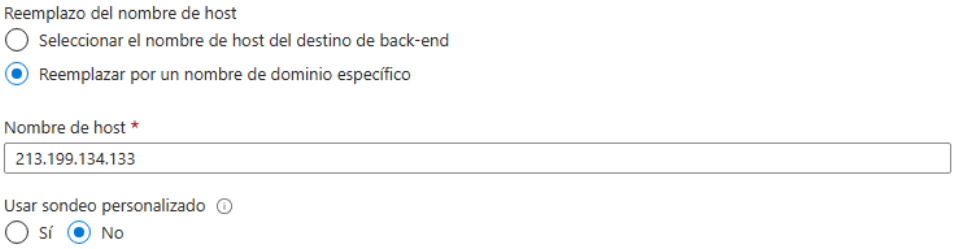


Ilustración 90: Nombre del host en configuración de *back-end*

Si el certificado es aceptado podremos ver el estado del servidor como correcto para el puerto 443 en el *Application Gateway*:

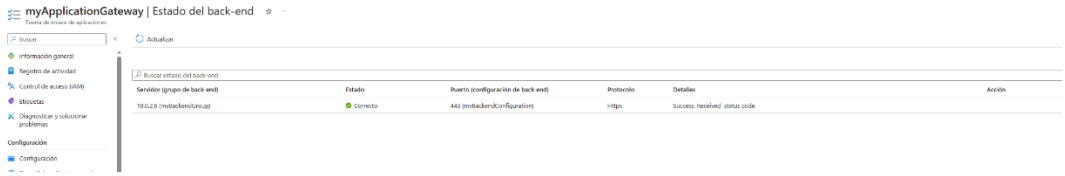


Ilustración 91: Estado del *back-end*

Comprobamos que podemos acceder mediante HTTPS:

Ilustración 92: Acceso mediante HTTPS

Podemos ver diferente información del certificado:

Ilustración 93: Información del certificado

8.10. Creación de un VPN Gateway

Para poder establecer un túnel VPN entre el administrador y el servidor será necesario crear un *VPN Gateway*. Para ello primero es necesario crear una subred para la el VPN Gateway. [36]

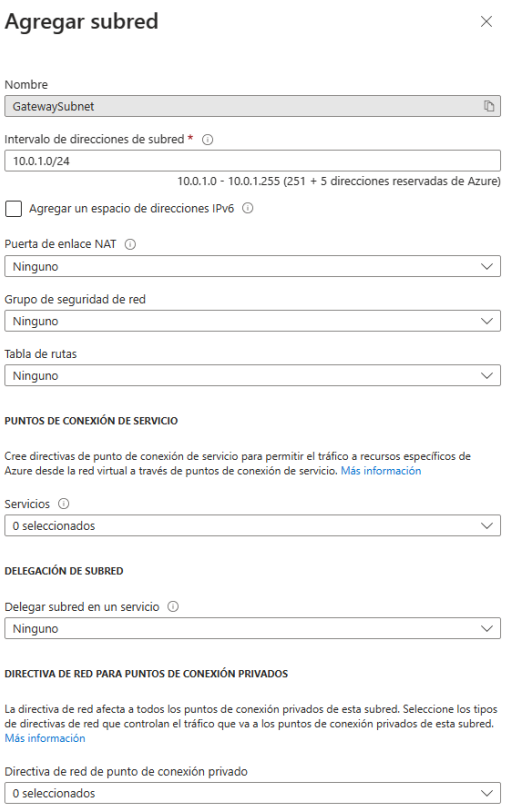


Ilustración 94: Subred de VPN Gateway

A continuación, creamos el VPN Gateway especificando sus datos básicos:

- Red privada y subred creada anteriormente.
- VPN como tipo de puerta de enlace.
- VPN basada en enrutamiento.
- La suscripción de menor coste.

También se generará una nueva IP pública estática durante el proceso, esta será utilizada para poder realizar la conexión a la puerta de enlace.

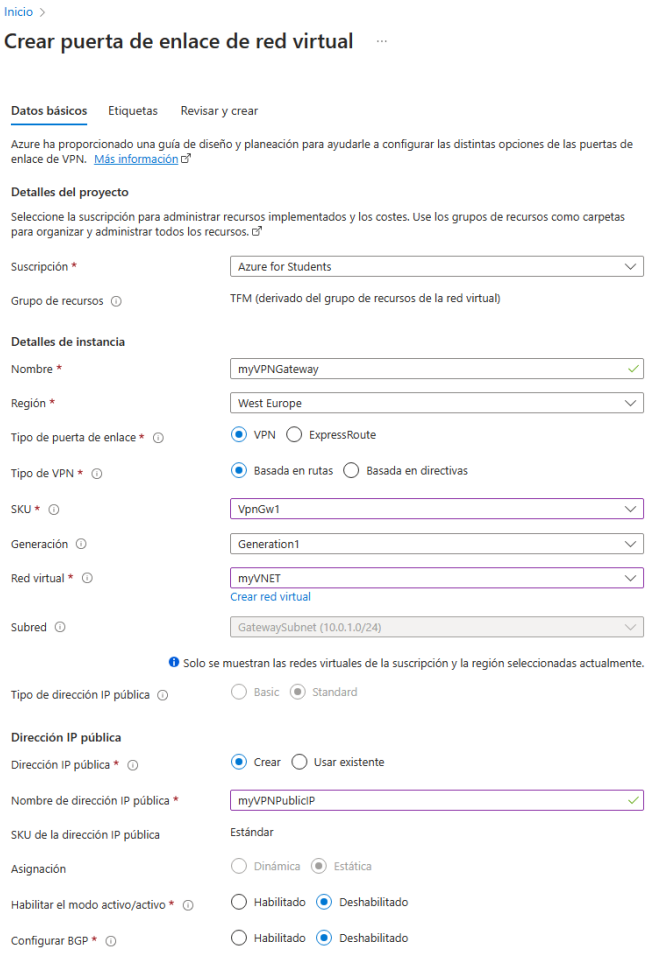


Ilustración 95: Datos básicos de VPN Gateway

Será necesario generar un certificado para poder realizar la conexión *point-to-site*, para ello se seguirán los pasos descritos por Microsoft. [35]

En primer lugar, creamos un certificado raíz autofirmado, como ya se ha mencionado anteriormente, si se tratase de un entorno de producción, lo ideal sería utilizar una entidad externa para firmar los certificados.

```
PS C:\Users\Blas> $params = @{
>>     Type = 'Custom'
>>     Subject = 'CN=P2SRootCert'
>>     KeySpec = 'Signature'
>>     KeyExportPolicy = 'Exportable'
>>     KeyUsage = 'CertSign'
>>     KeyUsageProperty = 'Sign'
>>     KeyLength = 2048
>>     HashAlgorithm = 'sha256'
>>     NotAfter = (Get-Date).AddMonths(24)
>>     CertStoreLocation = 'Cert:\CurrentUser\My'
>> }
>> New-SelfSignedCertificate @params


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
6F41D495E13BEE73099ED7E91F22A18FEB63FB2B  CN=P2SRootCert
```

Ilustración 96: Creación de certificado raíz en PowerShell

Este se instalará automáticamente en el sistema. A continuación, generamos un certificado para el cliente desde el certificado raíz, este es el que usará para poder autenticarse.

```
PS C:\Users\Blas>    $params = @{
>>         Type = 'Custom'
>>         Subject = 'CN=P2SChildCert'
>>         DnsName = 'P2SChildCert'
>>         KeySpec = 'Signature'
>>         KeyExportPolicy = 'Exportable'
>>         KeyLength = 2048
>>         HashAlgorithm = 'sha256'
>>         NotAfter = (Get-Date).AddMonths(18)
>>         CertStoreLocation = 'Cert:\CurrentUser\My'
>>         TextExtension = @(
>>          '2.5.29.37={text}1.3.6.1.5.5.7.3.2')
>>     }
PS C:\Users\Blas> New-SelfSignedCertificate @params


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
6F5178178340307BE7D8A2483372AF907534D7C9  CN=P2SChildCert
```

Ilustración 97: Creación de certificado cliente en PowerShell

Este certificado también se instalará automáticamente en el sistema. En caso de querer utilizarlo en otro equipo podríamos exportarlo como .pfx desde el almacén de certificados de Windows.

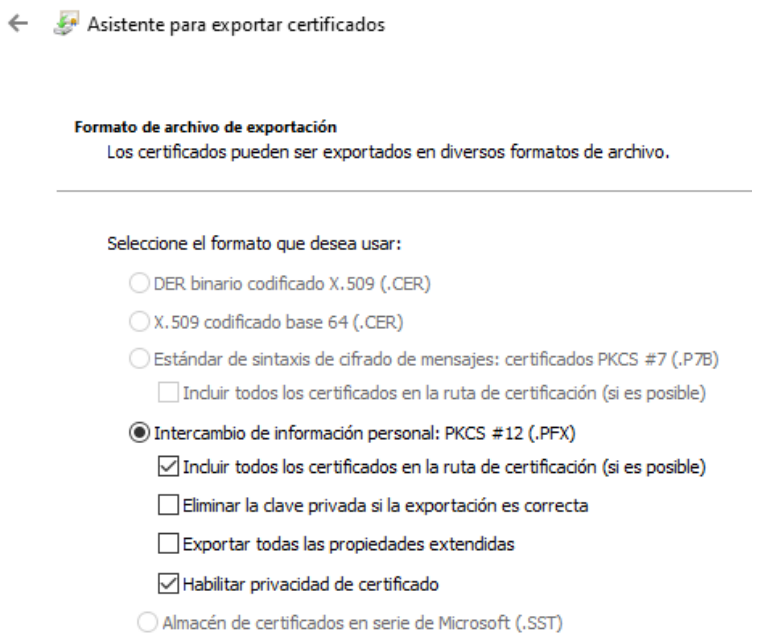


Ilustración 98: Exportación de certificado cliente

Es necesario exportar el certificado raíz puesto que tendremos que añadirlo al VPN Gateway. La exportación también puede realizarse desde el almacén de certificados.

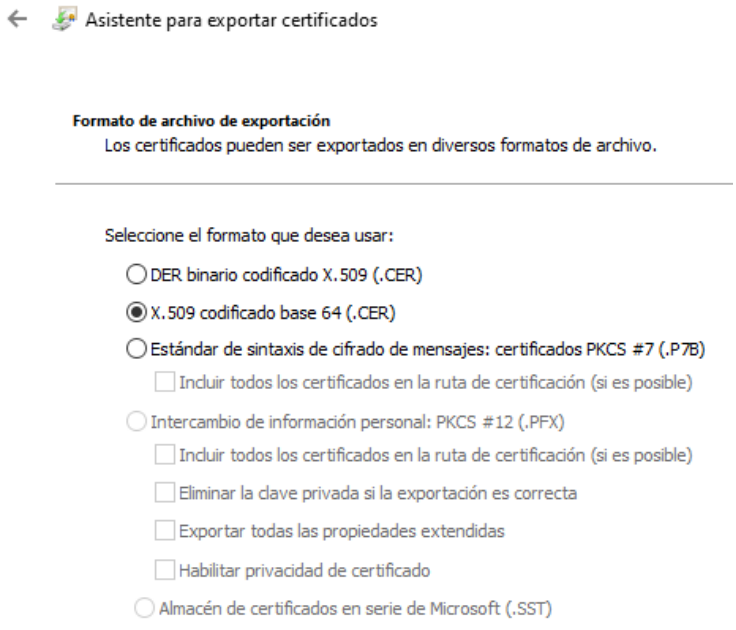


Ilustración 99: Creación de certificado raíz en PowerShell

Una vez guardado el archivo exportado será necesario copiar su certificado sin incluir ni la primera ni la última línea.

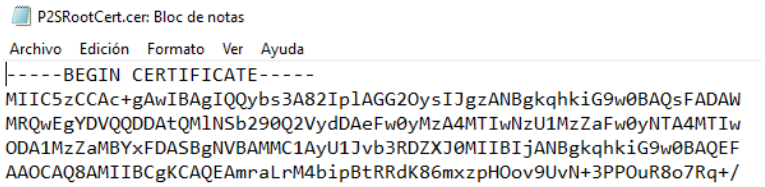


Ilustración 100: Certificado raíz generado para la VPN

A continuación, configuraremos la conexión de punto a sitio en el VPN Gateway.

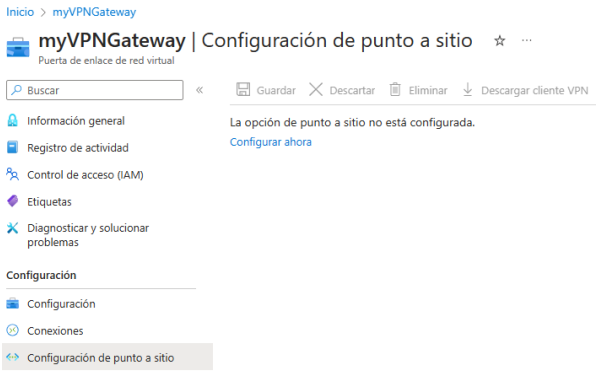


Ilustración 101: Configuración punto a sitio

Sera necesario establecer un grupo de direcciones para las máquinas y añadir el certificado raíz copiado anteriormente.

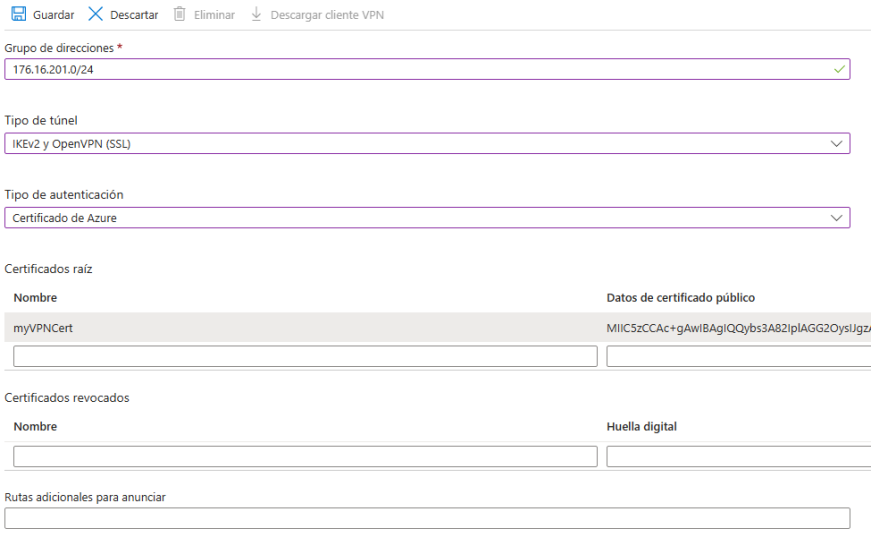


Ilustración 102: Direcciones y certificado del VPN

Tras realizar la configuración se nos dará la opción de descargar el cliente VPN.

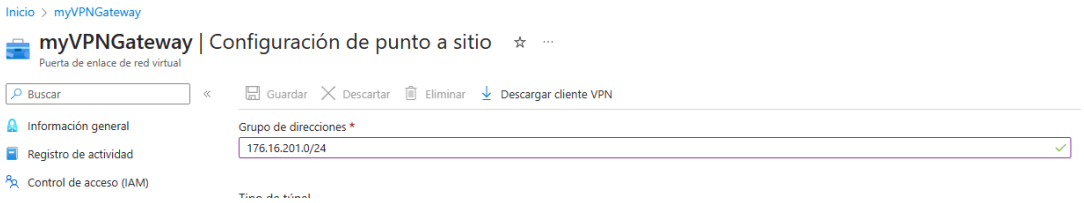


Ilustración 103: Descarga del cliente VPN

Este cliente está disponible para diferentes aplicaciones.

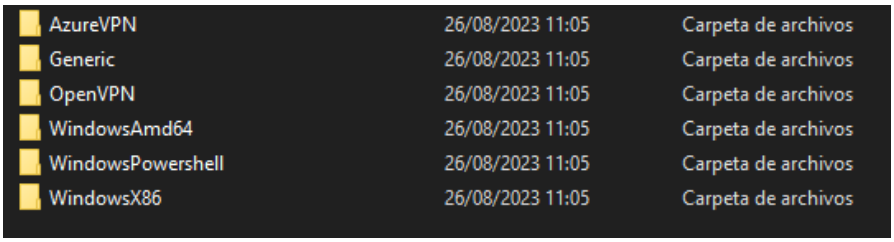


Ilustración 104: Cliente VPN

Utilizaremos la versión que configurará un cliente para el VPN incluido en Windows. Tras el proceso veremos como la VPN a la red privada es añadida.

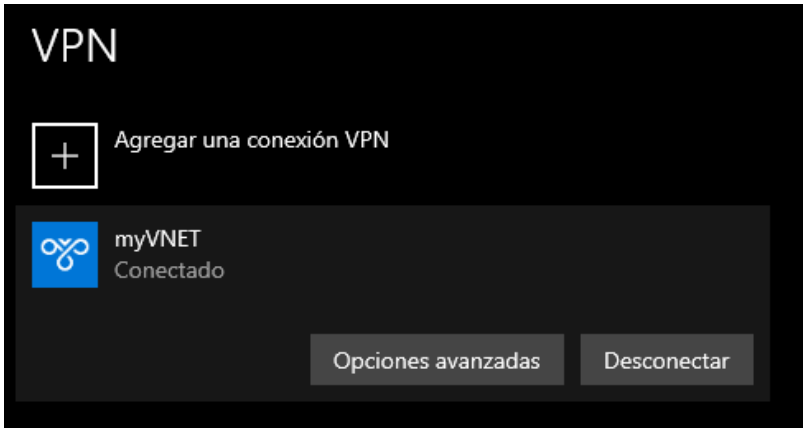


Ilustración 105: VPN instalado

Podremos conectarnos sin especificar el certificado puesto que este ya está instalado en el sistema.

Ilustración 106: Uso de Azure VPN

Podemos comprobar mediante *ipconfig* en Windows que efectivamente se ha realizado la conexión.

```
Adaptador PPP myVNET:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 176.16.201.2
   Máscara de subred . . . . . . . . . . . . : 255.255.255.255
   Puerta de enlace predeterminada . . . . . :
```

Ilustración 107: Conexión VPN realizada

Por último, comprobamos que podemos realizar la conexión SSH a la máquina mediante su IP privada.

```
PS C:\Users\Blas> ssh -i .\Downloads\wordp_key.pem azureuser@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ECDSA key fingerprint is SHA256:HnXdXKZUwx2guv5AEmxOzbKEYJ57Yh4cwbwJO0YsABA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1109-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Aug 26 09:19:03 UTC 2023

  System load:  0.01              Processes:           127
  Usage of /:   9.7% of 28.89GB   Users logged in:     1
  Memory usage: 19%               IP address for eth0: 10.0.2.6
  Swap usage:   0%
```

Ilustración 108: Conexión SSH mediante IP privada

8.11. Configuración de reglas en Application Gateway

A continuación, vamos a configurar una regla WAF en el *Application Gateway* para bloquear el acceso al panel de administración, solo ciertas IP podrán

conectarse. También se configurará una reglar para limitar el número de accesos que podrán realizarse desde una dirección en un tiempo determinado.

Las reglas se pueden añadir desde el recurso de reglas de *Application Gateway*, este incluye las reglas de OWASP [37] y la protección anti bots.

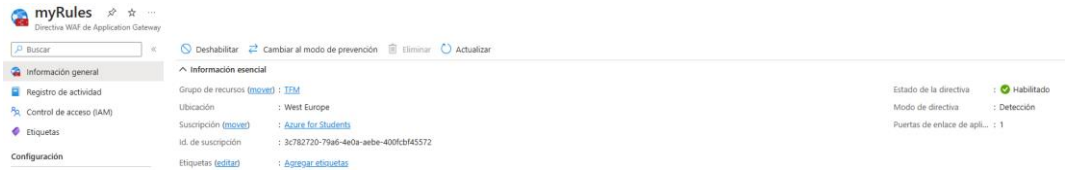


Ilustración 109: Reglas de Application Gateway

En primer lugar, para añadir la regla de bloqueo al panel de administración será necesario añadir una regla personalizada del tipo coincidencia.

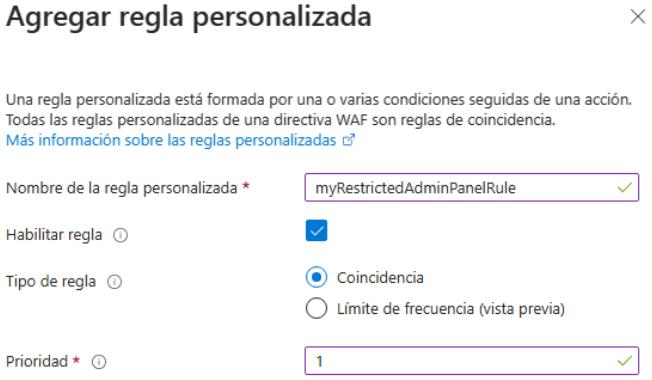


Ilustración 110: Regla personalizada en Application Gateway

A continuación, se establecen las condiciones de la regla. Se establecerá que se deniegue el tráfico a cualquier URL que contenga *wp-admin* siempre que la IP no sea la establecida.

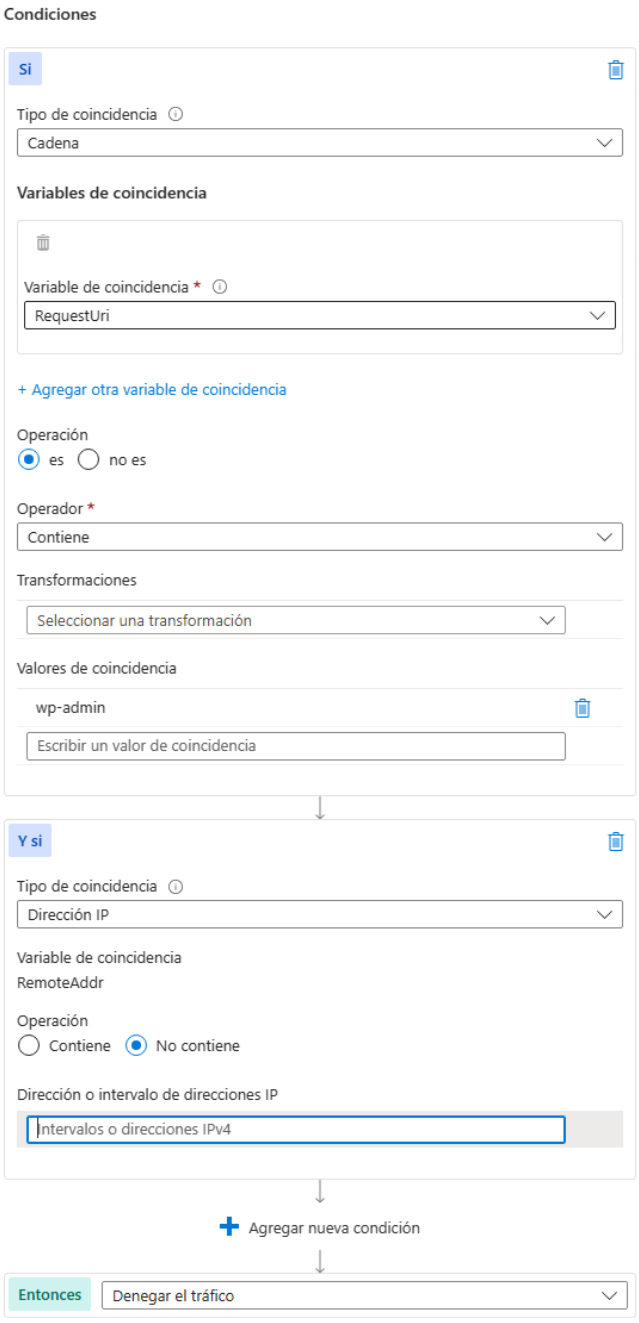


Ilustración 111: Condiciones de regla personalizada

Comprobamos que la nueva regla se ha habilitado.

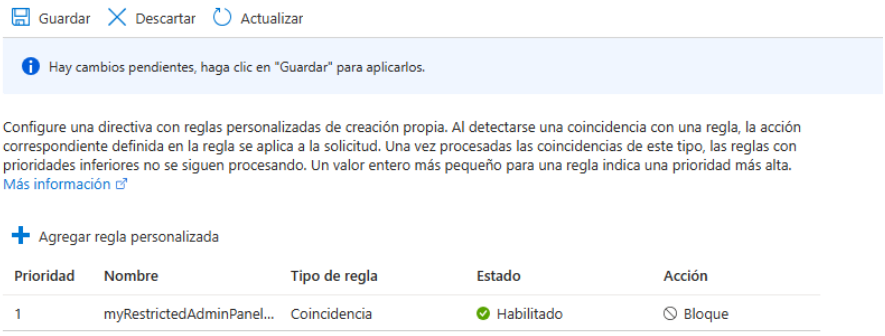


Ilustración 112: Regla personalizada habilitada

A continuación, es necesario cambiar el comportamiento de las reglas puesto que por defecto se encuentra en modo detección, con lo que no bloqueará el tráfico. Cambiamos al modo prevención desde la pestaña de información general.

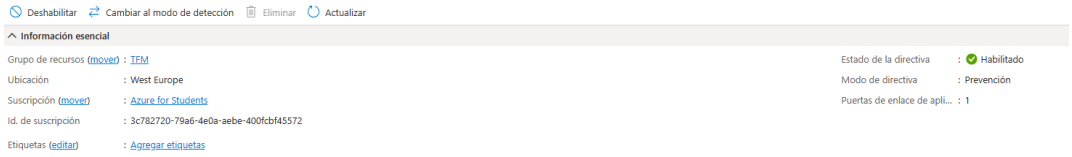


Ilustración 113: Modo prevención activado

Intentamos acceder a una URL con *wp-admin* desde una IP no permitida y comprobamos que el *Application Gateway* bloquea el tráfico.

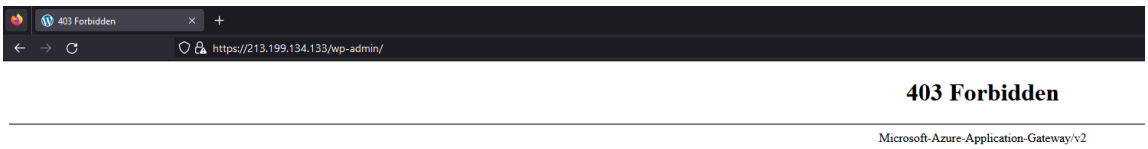


Ilustración 114: Bloqueo del tráfico desde Application Gateway

Para configurar el límite de conexiones establecemos una regla de forma similar, pero esta vez del tipo de límite de frecuencia. Es necesario establecer la duración del límite y el umbral de solicitudes que se aceptara desde una dirección. También añadiremos una condición para que esta regla no se tenga en cuenta dentro de la red privada.

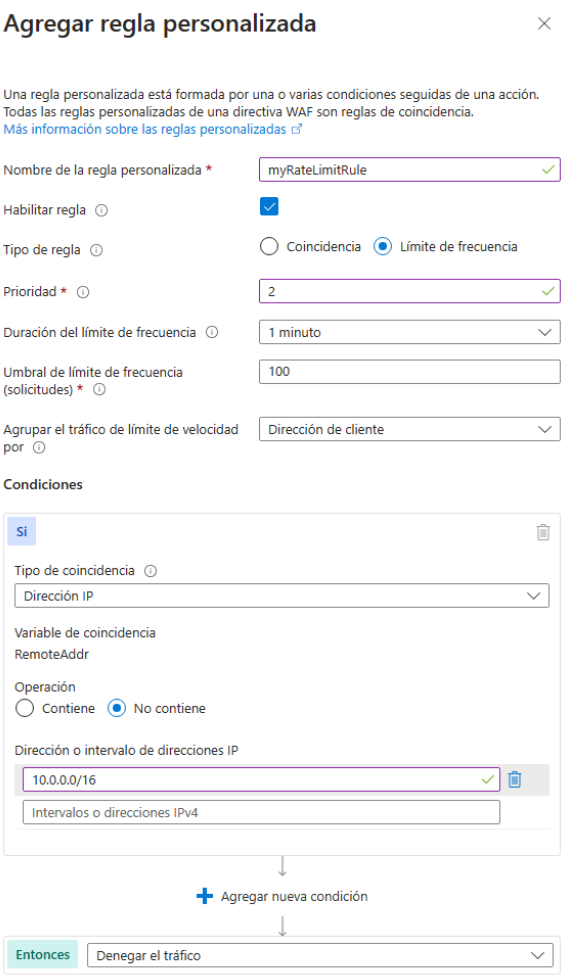


Ilustración 115: Límite de conexiones desde una dirección

8.12. Configuración de la copia de seguridad de WordPress

La copia de seguridad de WordPress se guardará en almacenamiento en la nube, para ello se utilizará el plugin UpdraftPlus. En primer lugar, instalamos y activamos el plugin.

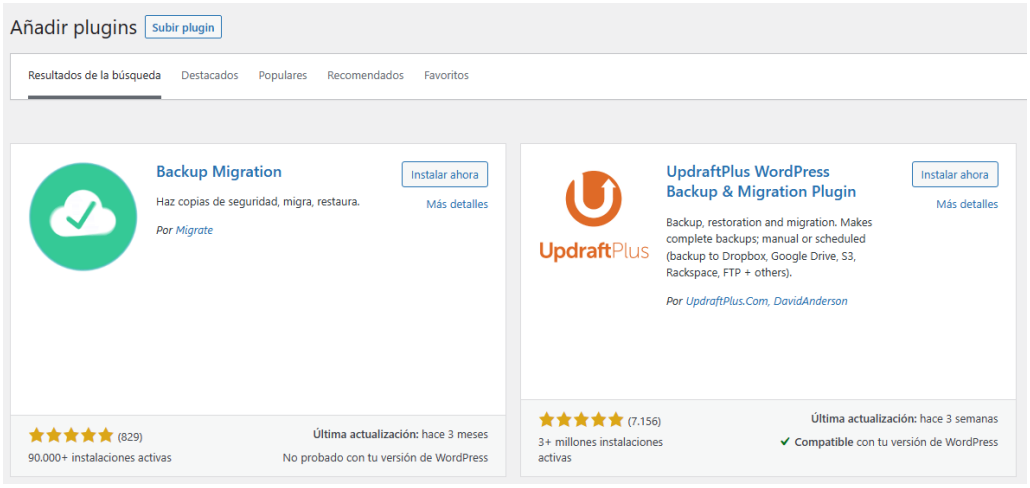


Ilustración 116: Plugin para copias de seguridad

A continuación, configuramos el plugin para realizar copias de forma manual, aunque puede configurarse para que se realicen automáticamente, también configuramos el número de copias máximas en dos, es decir, solo se guardarán las dos últimas copias.

El plugin permite utilizar el almacenamiento blob de Azure para realizar las copias de seguridad, sin embargo, es necesario adquirir la versión de pago para poder utilizar esta opción, por lo que en el entorno de experimentación utilizaremos el almacenamiento en Dropbox en su lugar, para ello se tendrán que dar permisos a la aplicación desde Dropbox.

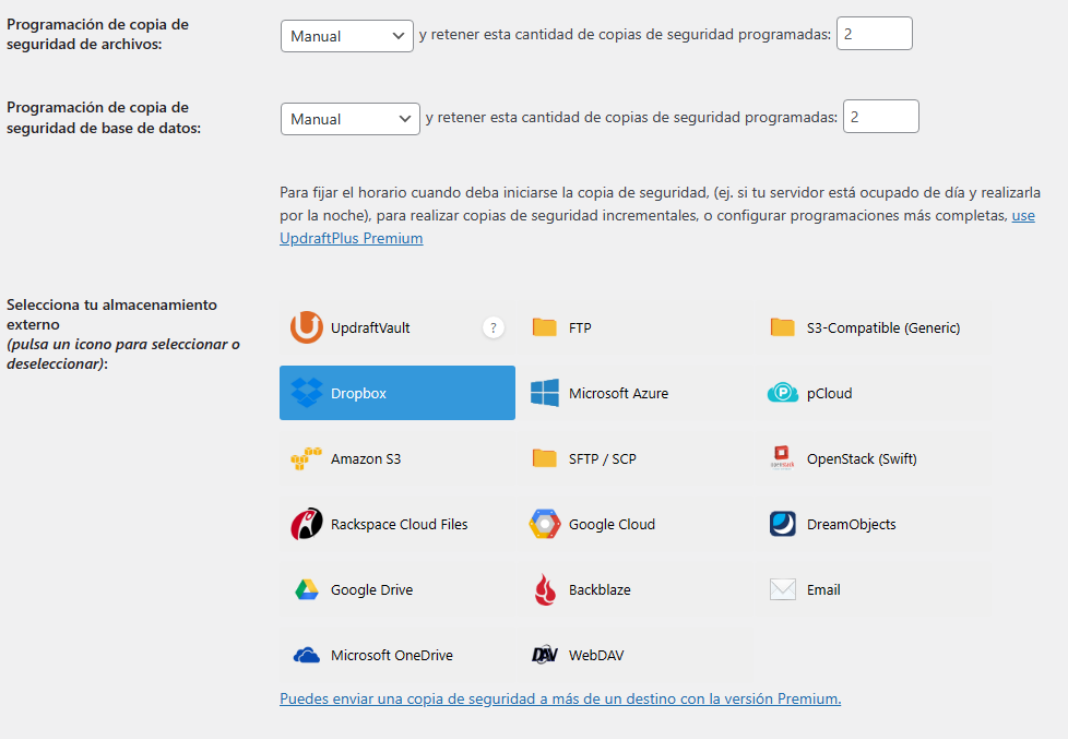


Ilustración 117: Configuración del plugin de copias de seguridad

A continuación, se puede configurar los archivos que se excluirán en las subidas, en este caso se configurara por defecto, evitando que se suban archivos como otras copias de seguridad, cache o logs de debug.

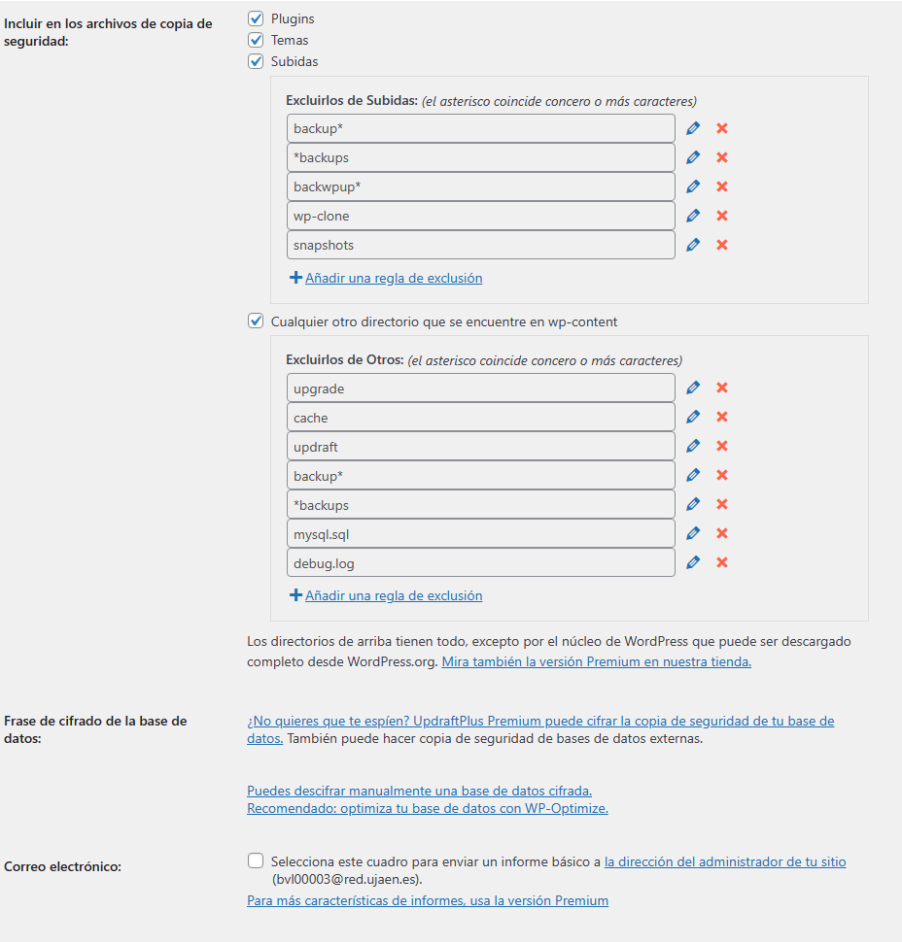


Ilustración 118: Configuración de exclusiones en la copia de seguridad

Una vez configurado podemos probar a realizar una copia de seguridad, se marcará solo de archivos puesto que para las copias de la base de datos ya se utiliza el servicio administrado por Azure.

Ilustración 119: Creación copia de seguridad de WordPress

Una vez creada podremos verla desde el propio plugin y restaurarla en cualquier momento.

Ilustración 120: Copia de seguridad creada

Podemos ver que las copias de las carpetas se han guardado en Dropbox.

Ilustración 121: Copias de seguridad en Dropbox

En un entorno de producción lo ideal sería pagar por la versión premium de la aplicación, puesto que esta permitiría cifrar las copias de seguridad.

8.13. Configuración y ejemplo de uso de WPSchoolPress

En primer lugar, es necesario instalar y activar el plugin que se encuentra en los repositorios de WordPress.

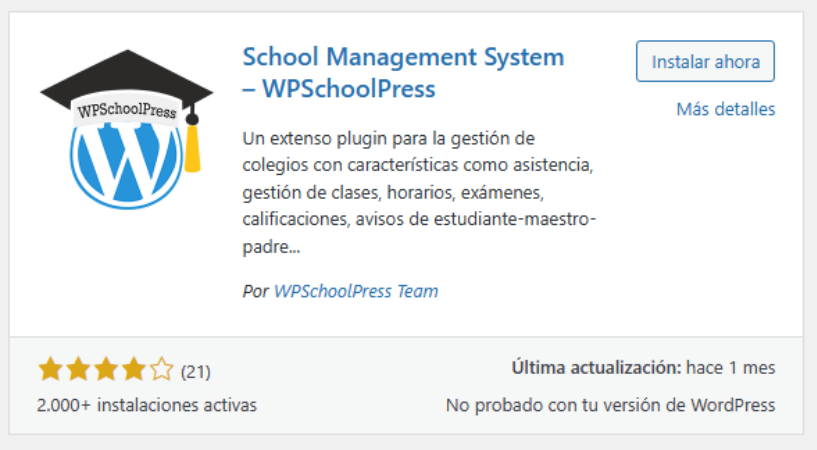


Ilustración 122: Plugin WPSchoolPress

Una vez activado podemos importar datos de prueba para rellenar el sistema con alumnos y profesores.

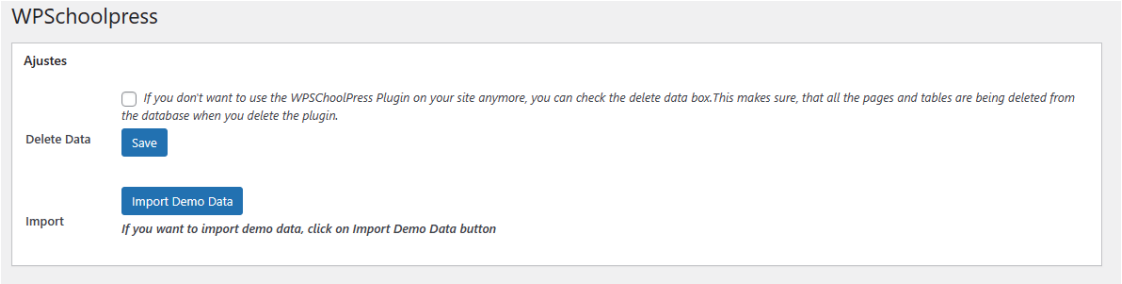


Ilustración 123: Importación de demo en WPSchoolPress

El plugin permite cuatro roles en el sistema, estos serían el administrador, el profesor, el alumno y el padre. El panel que veríamos como administrador al entrar en el sistema de gestión sería el siguiente:

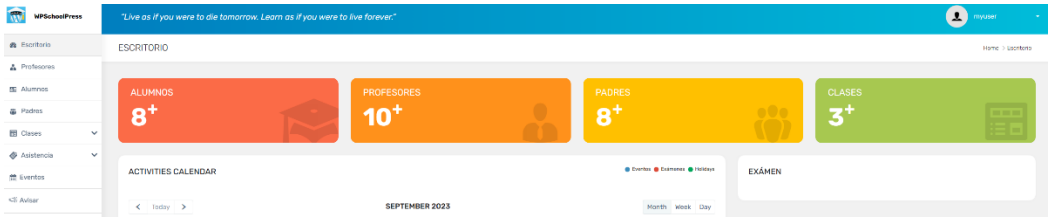


Ilustración 124: Panel de WPSchoolPress

Los administradores son los que tendrían que añadir los nuevos usuarios, por ejemplo, podrían crearse nuevos alumnos desde la vista de alumnos.

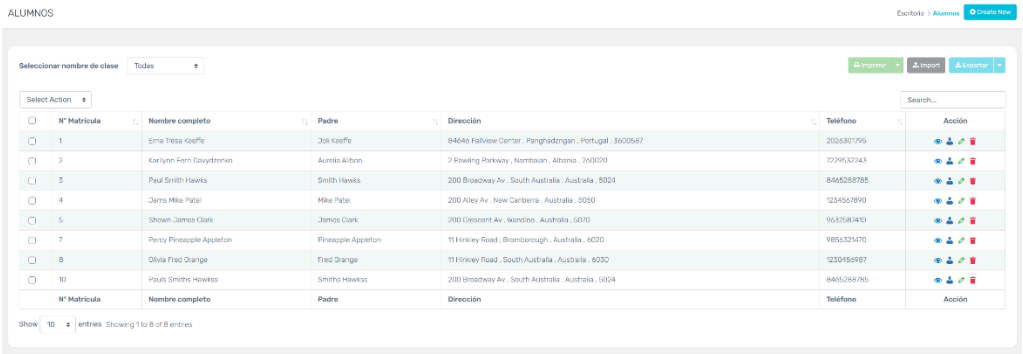


Ilustración 125: Lista de alumnos

Durante la creación se tendrían que dar una serie de datos, los personales serán opcionales excepto por el nombre y el apellido.

Ilustración 126: Datos del alumno

Durante el proceso podrían añadirse un padre al alumno, para ambos se debe rellenar la información de la cuenta, la cual se usará para iniciar sesión. El alumno también se tendrá que dar de alta en una clase.

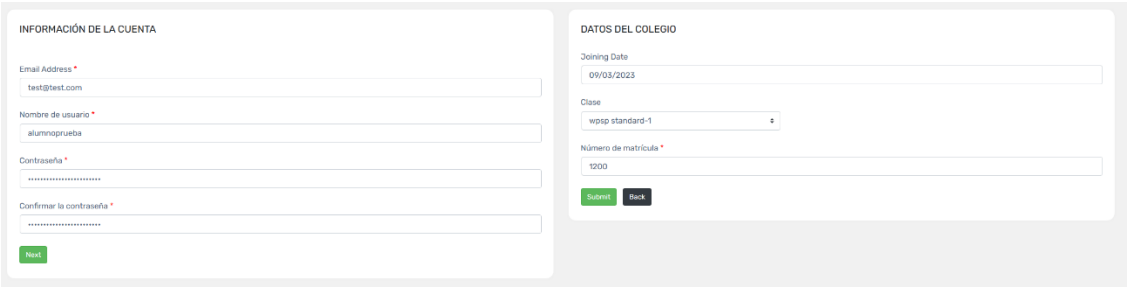


Ilustración 127: Información de la cuenta de alumno

Los profesores se crearían de forma similar, pero cambiarían los datos del colegio.

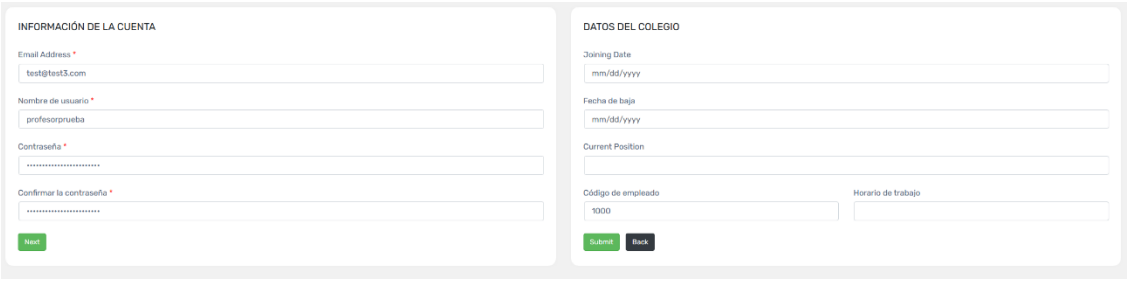


Ilustración 128: Información de la cuenta de profesor

El administrador podría añadir al profesor a una clase a la cual tendría acceso. También podría añadirlo a las asignaturas correspondientes.

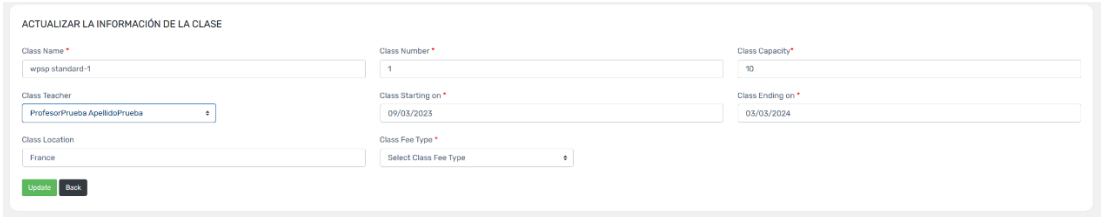


Ilustración 129: Información de la clase

Ilustración 130: Información de la asignatura

Una vez en una clase el profesor podría marcar la asistencia de los alumnos para una fecha determinada.

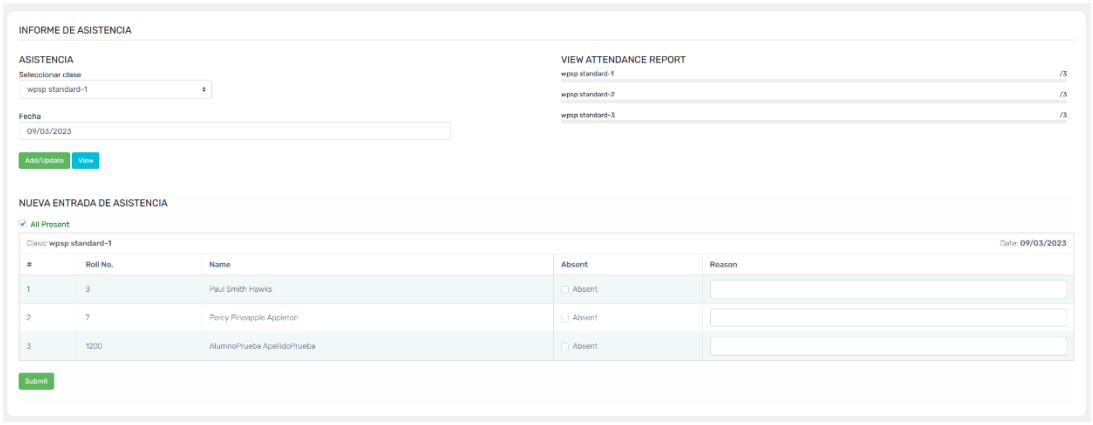


Ilustración 131: Información de la asistencia a clase

El profesor también podría añadir fechas de exámenes y notas de los mismos.

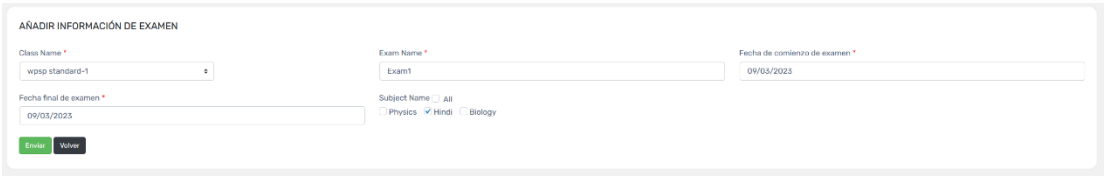


Ilustración 132: Información de examen

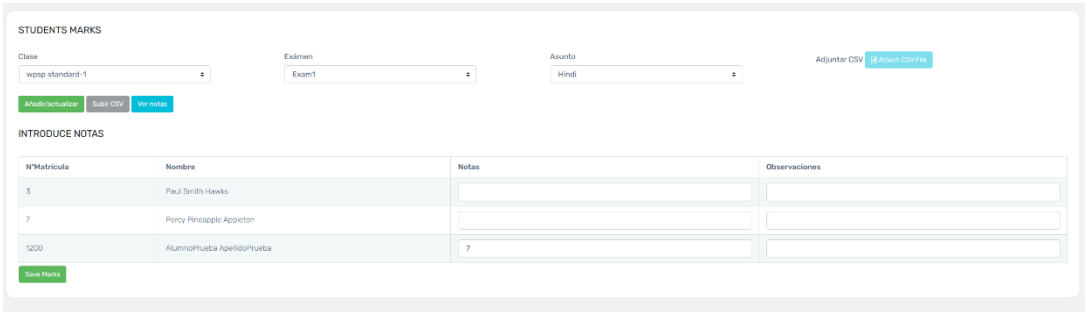


Ilustración 133: Notas de examen

También es posible añadir eventos al calendario, estos pueden ser vistos por todos o solo por profesores.

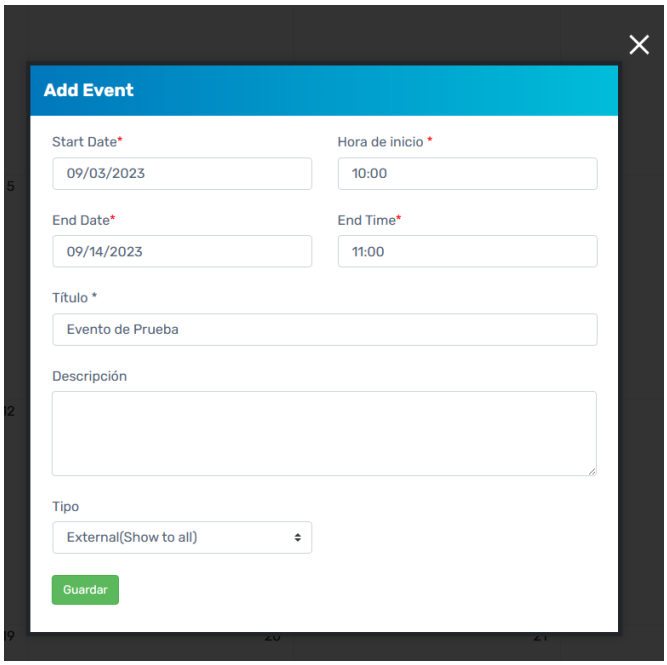


Ilustración 134: Información de evento

Los alumnos podrán ver los eventos y las fechas de los exámenes en su calendario.

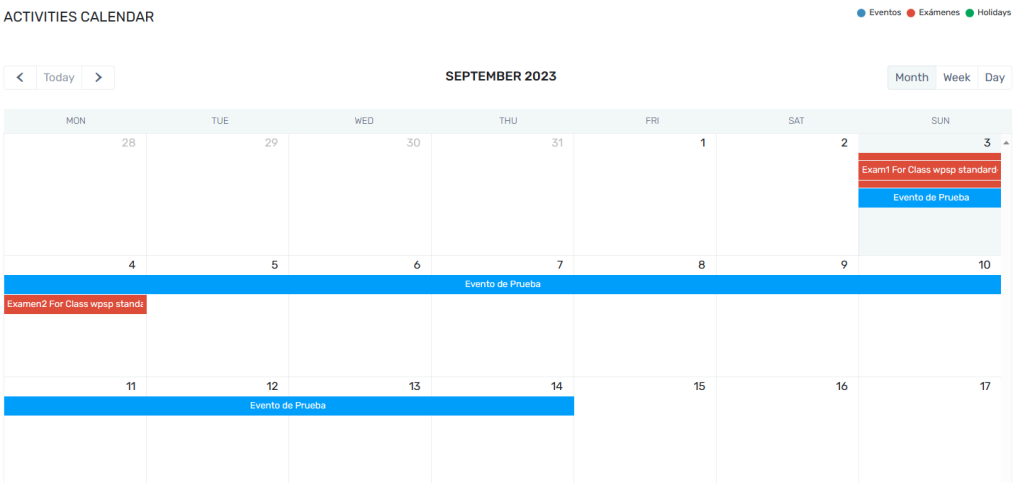


Ilustración 135: Calendario del instituto

También podrá ver un resumen de una clase indicando la fecha y la asistencia que se ha cumplido.

Ilustración 136: Información de la asistencia para el alumno

8.14. Configuración de IThemes Security

Para gestionar diferentes aspectos de seguridad del sitio web se instalará el plugin de *IThemes Security*. [38]

Los aspectos de los que se encargará serán los siguientes:

- Aplicación de una política de contraseñas.
- Segundo factor de autenticación.
- Escaneos del sitio web.
- Detección de cambios en archivos y comprobación de permisos.

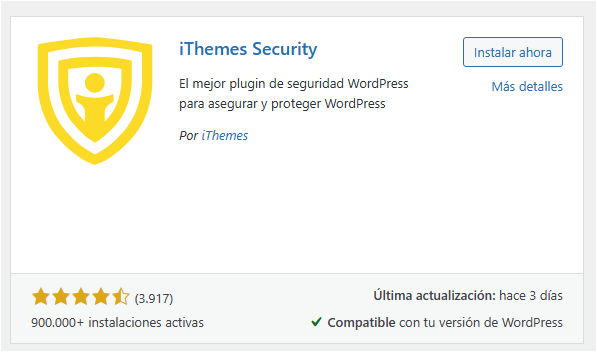


Ilustración 137: Plugin de IThemes Security

Durante el proceso se preguntará qué rol será el encargado de gestionar la seguridad mediante este plugin.

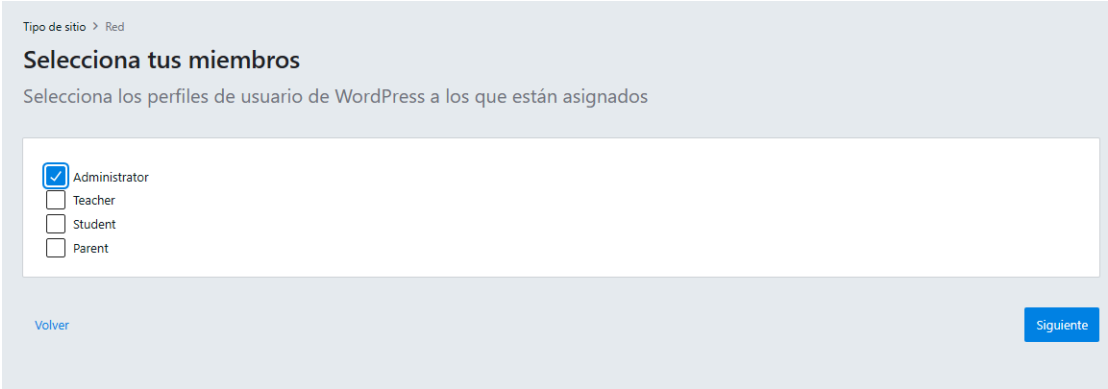


Ilustración 138: Selección rol de seguridad de IThemes Security

Se activará una política de contraseñas que obligará a los usuarios a utilizar una contraseña fuerte.

Ilustración 139: Política de contraseñas

Se configurarán las diferentes opciones de seguridad, ya se dispone del *Application Gateway* que protege de varios de estos aspectos con lo que solo se activará la autenticación de dos factores y la exploración del sitio para buscar vulnerabilidades.

La exploración de vulnerabilidades se realiza sobre la aplicación de WordPress, los plugins y los temas instalados, en este proceso también se realiza una comprobación para detectar si el sitio web se encuentra en las listas de bloqueo de Google [39]. Para realizar la exploración hace uso de la base de datos ofrecida por Patchstack que consta con más de 30000 vulnerabilidades del núcleo de Wordpress, de plugins y de temas. En las vulnerabilidades vienen incluidas las versiones afectadas, la clasificación CVSS, cuando se lanzará un parche y diferentes detalles técnicos, como el CVE o la clasificación OWASP a la que pertenece. [40]

Una vez instalado el plugin podremos ver un panel desde donde se puede realizar un seguimiento de bloqueos, copias de seguridad en caso de que se usará

esta utilidad y exploraciones del sitio. Realizaremos una exploración del sitio en busca de vulnerabilidades:

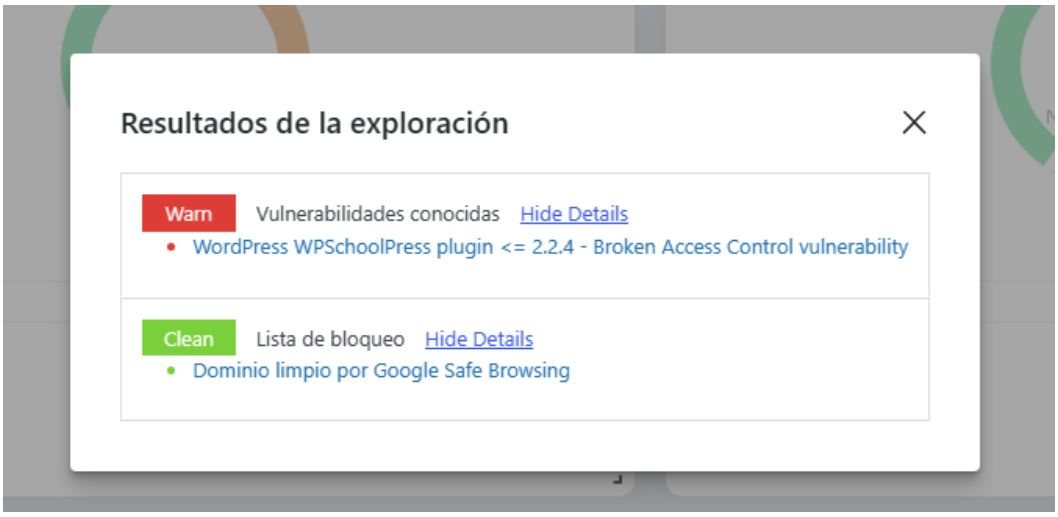


Ilustración 140: Exploración de vulnerabilidades con IThemes Security

Podemos ver que ha encontrado una vulnerabilidad en el plugin instalado anteriormente. Nos permite buscar más información y el CVE al que hace referencia.

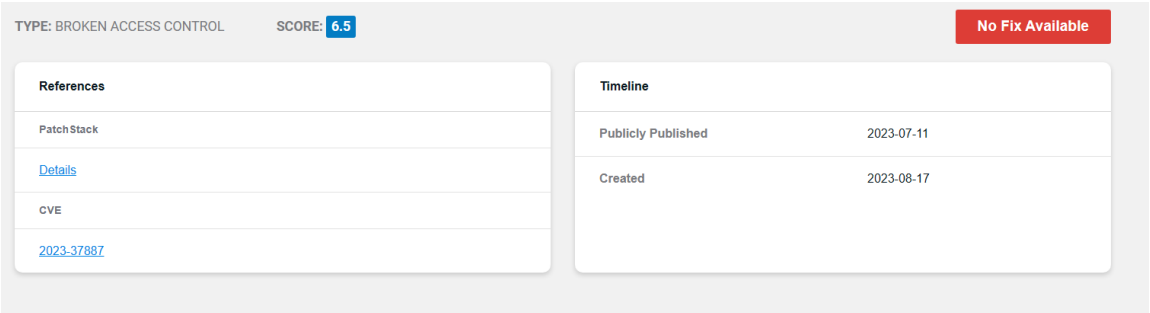


Ilustración 141: Resumen de vulnerabilidad con IThemes Security

A continuación, activaremos el doble factor de autenticación en un usuario administrador, para ello es necesario entrar en el usuario y activar el servicio mediante identificación móvil.

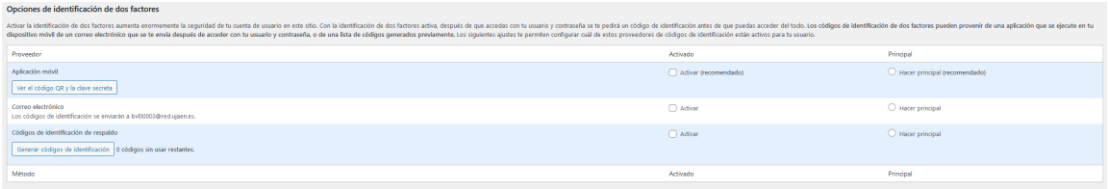


Ilustración 142: Activación del segundo factor de autenticación

Nos proporcionará un código QR que será necesario escanear mediante alguna aplicación de doble factor de autenticación, por ejemplo, *Microsoft*

Authenticator. Esta aplicación generará un código que tendremos que añadir a WordPress, tras esto el dispositivo se vinculará.

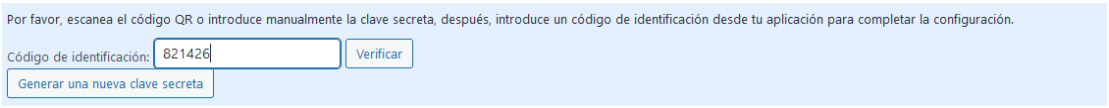


Ilustración 143: Vinculando dispositivo de doble factor de autenticación

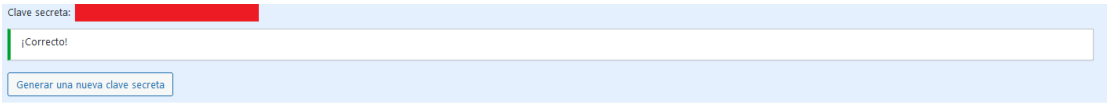


Ilustración 144: Dispositivo de doble factor de autenticación vinculado

A partir de ahora, al intentar iniciar sesión, el sistema pedirá un código suministrado por la aplicación vinculada.

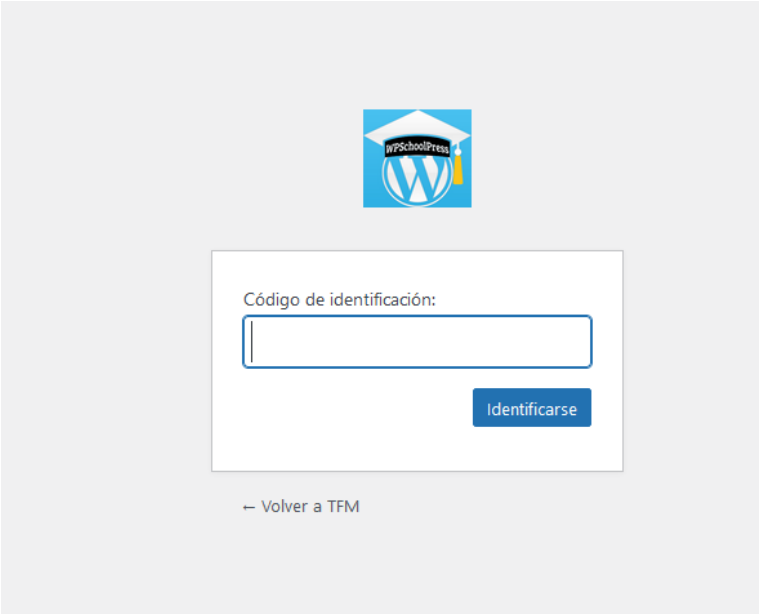


Ilustración 145: Segundo factor de autenticación requerido

8.15. Configuración de WP Activity Log

se utilizará el plugin WP Activity Log para realizar un seguimiento de los diferentes cambios que se producen en WordPress, incluyendo sus contenidos, archivos de configuración, ficheros de instalación y su base de datos. En primer lugar, lo instalamos y activamos desde WordPress.

Ilustración 146: Instalación de WP Activity Log

A continuación, lo configuramos mediante su asistente. En primer lugar, le pedimos que nos muestre la máxima información posible.

Ilustración 147: Cantidad de información de WP Activity Log

Marcamos que solo usamos las páginas por defecto de WordPress.

Ilustración 148: Páginas por defecto WP Activity Log

Por último, lo configuramos para que guarde los registros durante 6 meses tras lo cual se borraran.

Ilustración 149: Tipo de retención de registros en WP Activity Log

Una vez configurado podemos observar que ya muestra, por ejemplo, los inicios y cierres de sesión de los usuarios.

Ilustración 150: Registros de WP Activity Log

De cada registro puede verse información como la IP desde la que se ha realizado, la severidad, el tipo de evento y diferente información del usuario.

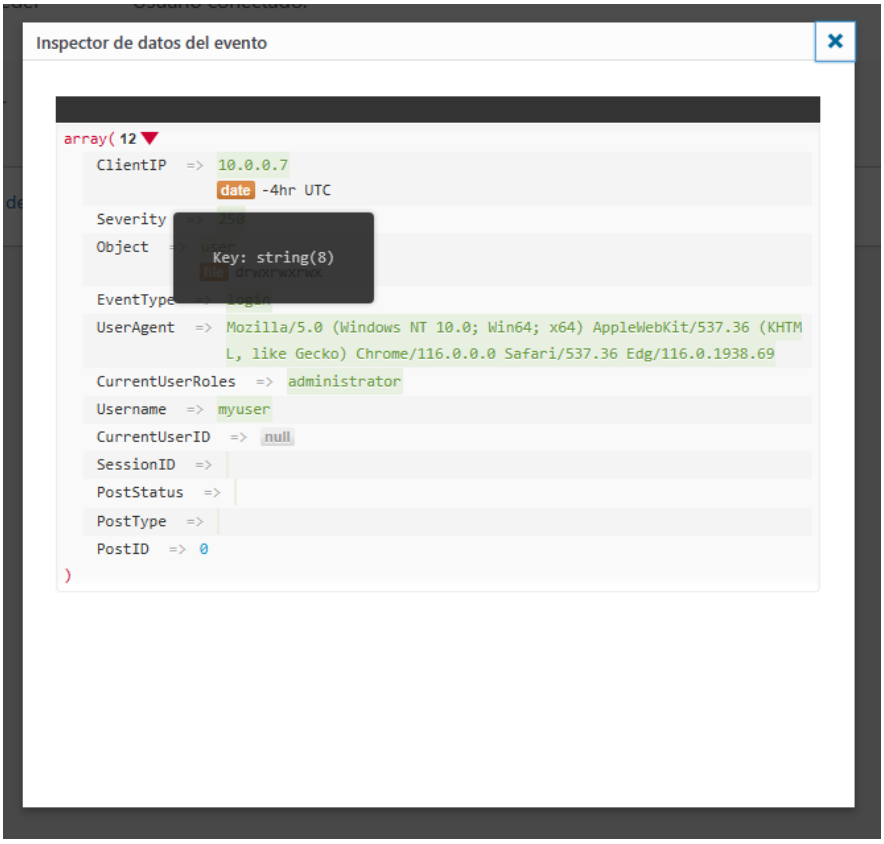


Ilustración 151: Información de los registros de WP Activity Log

8.16. Configuración de Microsoft Sentinel

Se realizará la configuración de Microsoft Sentinel, el SIEM nativo ofrecido en Azure, en este caso la configuración servirá para mostrar alertas de los eventos producidos en el *Application Gateway*. En primer lugar, es necesario crear un área de trabajo de *Log Analytics*, aquí es a donde se enviarán los logs generados, estos serán más tarde consultados por Microsoft Sentinel. [41]

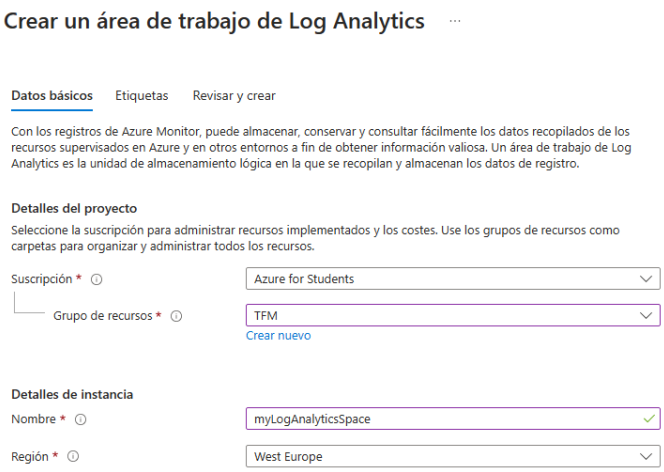


Ilustración 152: Creación de un área de trabajo de Log Analytics

Desde la configuración de diagnóstico de *Application Gateway* añadiremos una nueva configuración para los logs.

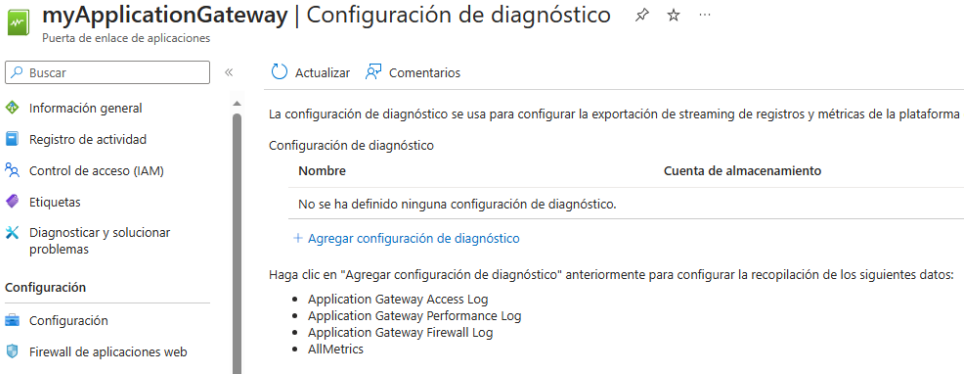


Ilustración 153: Configuración de diagnóstico de Application Gateway

Marcamos que añada todos los tipos de logs, incluyendo los del Firewall, los de acceso y los de rendimiento. Enviamos estos logs al área de trabajo creada anteriormente.

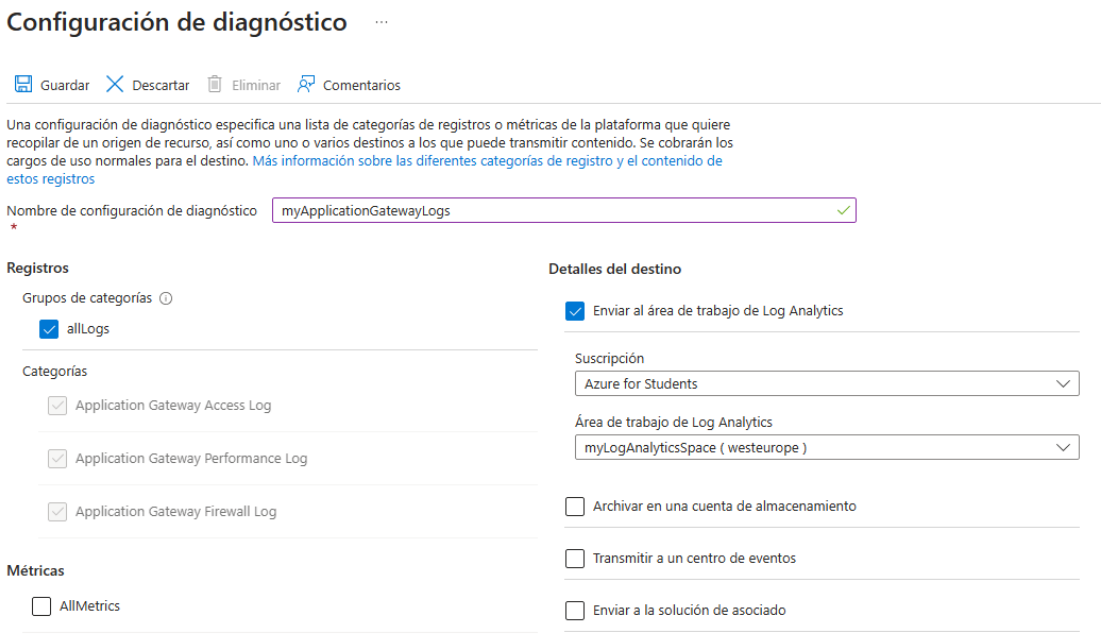


Ilustración 154: Selección de logs en configuración de diagnóstico

A continuación, configuramos Microsoft Sentinel, nos pedirá que seleccionemos el área de trabajo desde donde recogerá los logs.

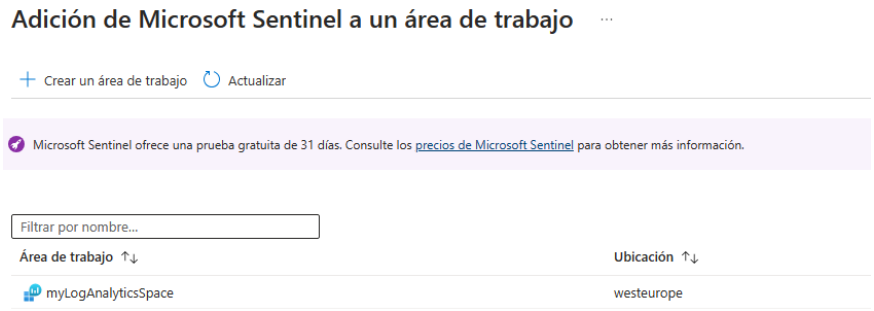


Ilustración 155: Selección de área de trabajo en Microsoft Sentinel

A continuación, es necesario añadir un conector al *Application Gateway*, buscamos la solución en el centro de contenido de Microsoft Sentinel.

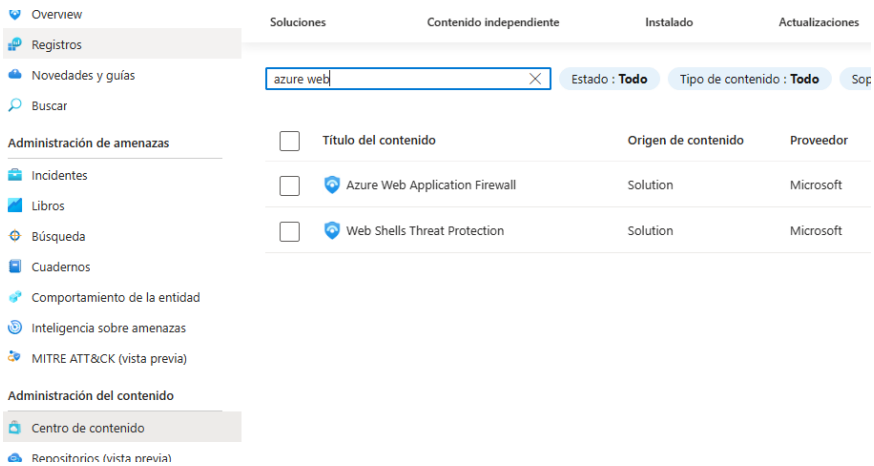


Ilustración 156: Centro de contenido en Microsoft Sentinel

Una vez instalado podremos ver que el conector se encuentra activo.

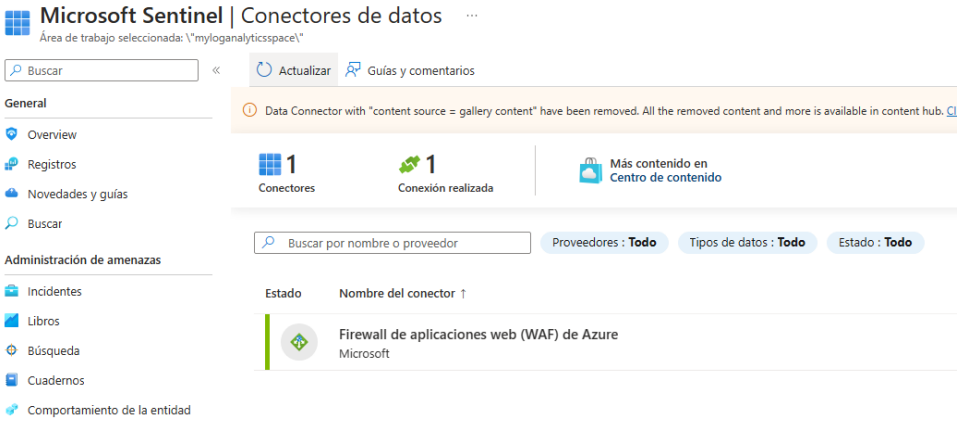


Ilustración 157: Conector en Microsoft Sentinel

Una vez instalado el conector podemos ver las diferentes reglas de alertas que incluye.

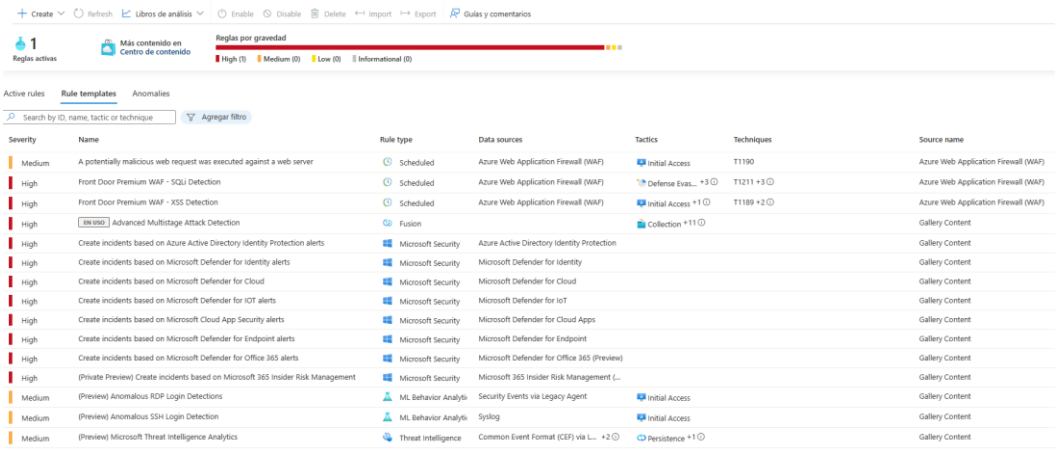


Ilustración 158: Reglas en Microsoft Sentinel

También puede verse un resumen de los datos recibidos desde el conector.

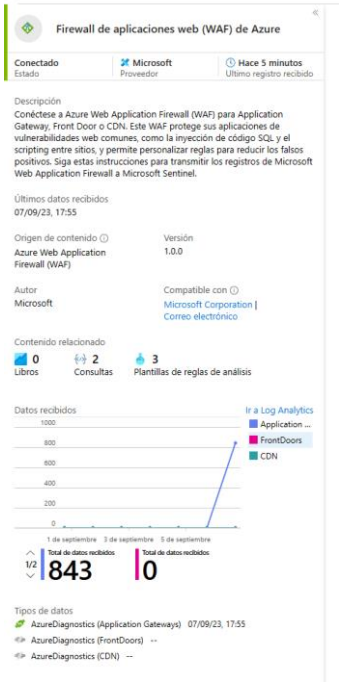


Ilustración 159: Resumen del conector de datos

Por último, vamos a crear una regla para que nos muestre una alerta siempre que observe nuevos logs del Firewall. Realizará la comprobación de la misma cada 6 minutos.

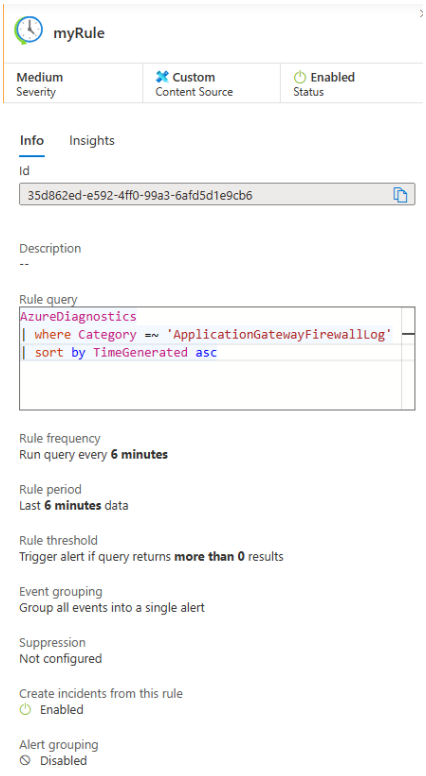


Ilustración 160: Regla en Microsoft Sentinel

9. Evaluación de la seguridad

Se realizarán una serie de evaluaciones con varios experimentos para comprobar algunas de las medidas de seguridad, viendo que efectivamente se han cumplido los requisitos que debían cubrir.

9.1. Evaluación de restauración del sistema

Se va a simular un escenario donde se perderán todos los datos del servidor y este tendrá que restaurarse por completo, para ello crearemos una máquina a parte y restauraremos las copias de seguridad. Esta evaluación indicaría que se ha cumplido el requisito 8.1.5.

La nueva máquina se crearía de forma similar a lo visto en la sección de despliegue, pero para simplificarlo esta vez no usaremos HTTPS y añadiremos una IP pública para conectarnos directamente.

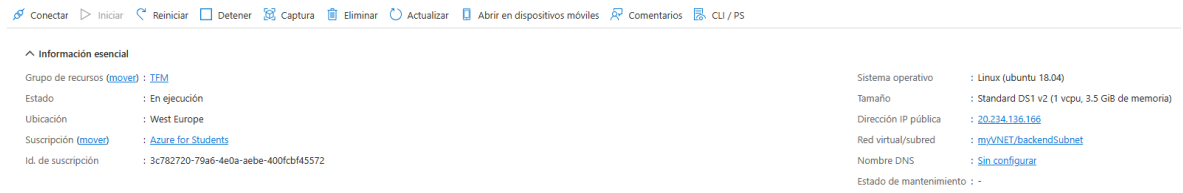


Ilustración 161: Máquina simulación de restauración

Una vez que WordPress está instalado es necesario instalar el plugin UpdraftPlus para poder restaurar las copias de seguridad. Para este experimento no solo restauraremos las copias de WordPress, también usaremos UpdraftPlus para recuperar la base de datos para simplificar el escenario.

Una vez se ha instalado el plugin cargamos las copias desde almacenamiento local. Si este servidor utilizara la misma dirección con la que se generaron las copias, estas se podrían cargar directamente desde Dropbox, lo mismo ocurriría si se hubiera utilizado el almacenamiento de blob de Azure.

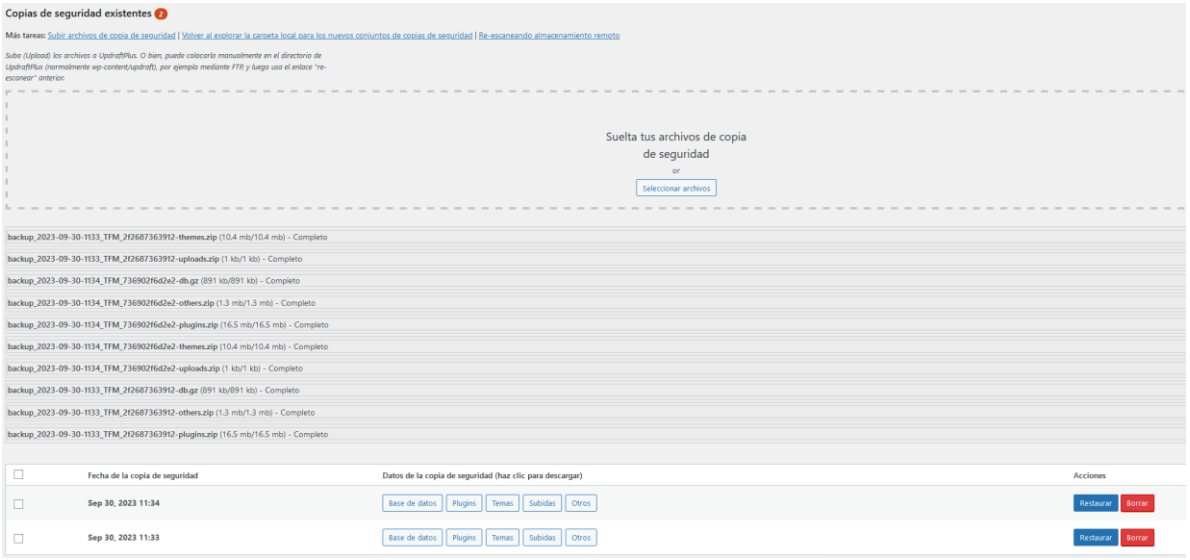


Ilustración 162: Copias de seguridad cargadas

Seleccionamos las copias de seguridad a restaurar.

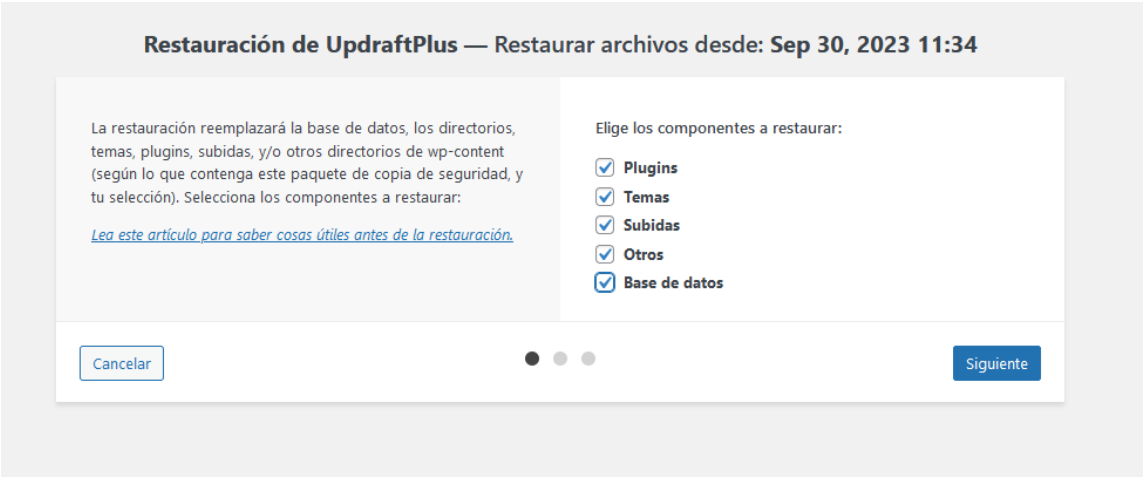


Ilustración 163: Restauración de las copias de seguridad

Esperamos a que el proceso de restauración termine.

Ilustración 164: Proceso de restauración de copias de seguridad

Una vez el proceso termine podemos comprobar que todos los plugins y el contenido de la base de datos se ha cargado correctamente.

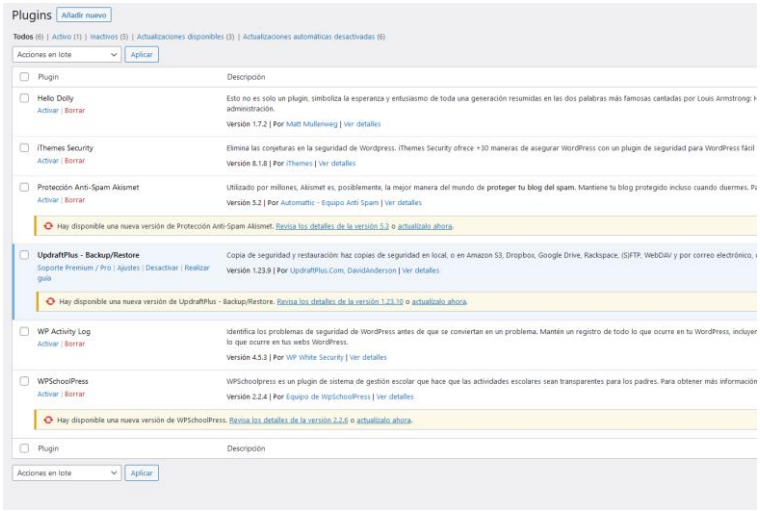


Ilustración 165: Plugins restaurados correctamente

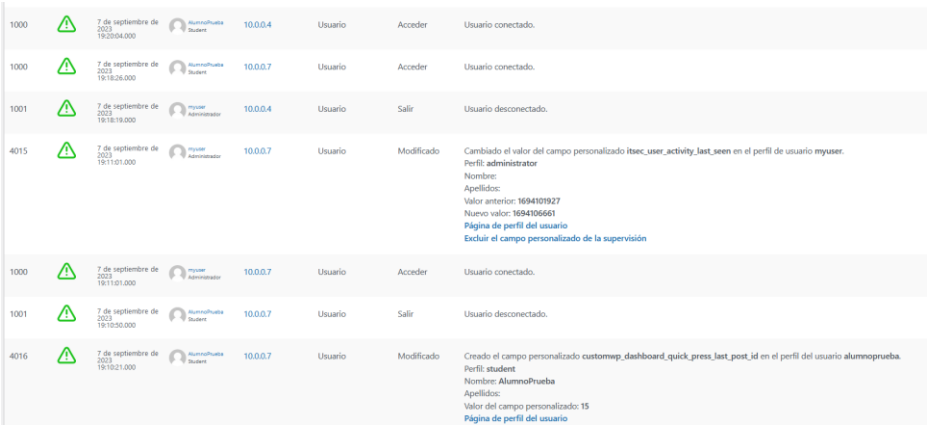


Ilustración 166: Logs restaurados correctamente

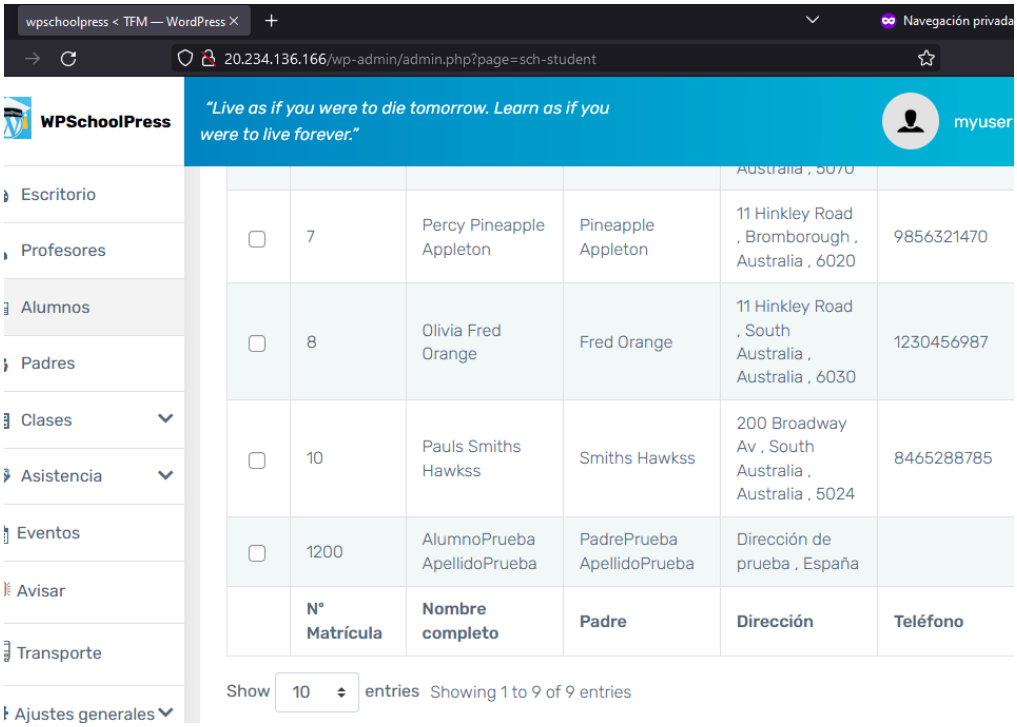


Ilustración 167: Alumnos restaurados correctamente

El proceso completo de restauración del sistema debería ser inferior a media hora.

9.2. Evaluación de seguridad de las contraseñas

En este escenario se simulará que la base de datos ha sido filtrada, se comprobará que solo se almacenan hashes de las contraseñas y que las contraseñas no pueden llegar a recuperarse utilizando para ello la herramienta *Hashcat*, esto indicaría que se ha cumplido el requisito 2.4.1 que se había propuesto anteriormente.

Supondremos que el usuario utiliza una contraseña que se encuentra en alguna de las listas de contraseñas comunes que existen. Para ello pondremos la contraseña del usuario en un archivo de texto donde solo estará esta, agilizando así el proceso y comprobando si podría deshacer el hash de una contraseña común, aunque en este caso se estará usando una creada por un generador de contraseñas.

Lanzamos por lo tanto *Hashcat* con la siguiente configuración:

- -m 400: Indica el tipo de hash de WordPress llamado phpass, el cual a día de hoy es inseguro al ser MD5.
- -a 0: Indica un ataque de diccionario.

Ilustración 168: Ejecución de Hashcat

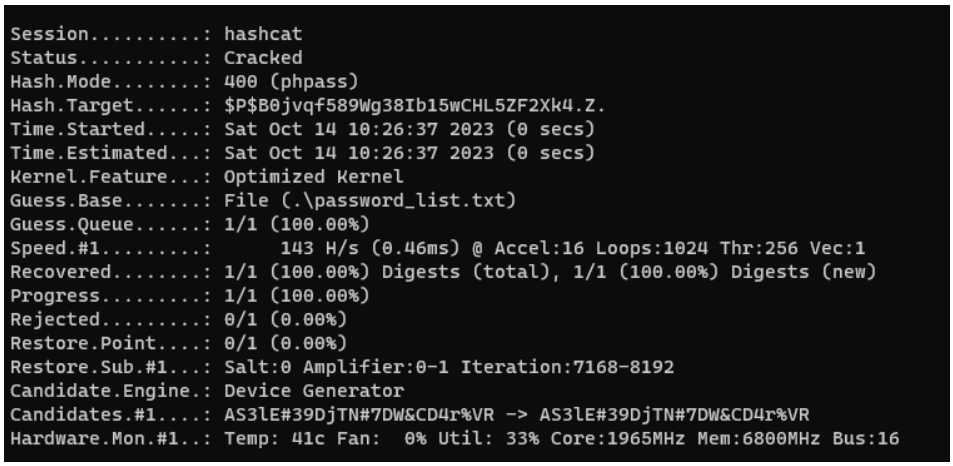


Ilustración 169: Resultado de Hashcat

Vemos que efectivamente consigue obtener la contraseña, con lo que si un usuario del sistema utilizara alguna contraseña que exista en alguna de las listas, el atacante podría obtenerla.

Al seguir utilizando WordPress hashes mediante MD5, la única forma de protegerse ante este tipo de ataque sería utilizar generadores de contraseñas lo cual evitaría que un atacante pudiera utilizar este tipo de ataque de fuerza bruta.

Sin embargo, también se podría utilizar algún plugin para cambiar el modo en el que WordPress genera los hashes, utilizando otro método más seguro como bcrypt. El plugin *Password bcrypt* [4] se encargaría de modificar las funciones password_hash y password_verify de WordPress, estos pasarían a utilizar el método de generación de hashes mencionado.

[4] https://github.com/roots/wp-password-bcrypt

9.3. Evaluación de privilegios mínimos

Se realizarán algunas comprobaciones para ver si un usuario podría realizar acciones que no le corresponden dentro del sistema. Esta evaluación indicaría que se ha cumplido el requisito 4.1.3.

En primer lugar, intentamos ver la lista de alumnos de una clase habiendo iniciado sesión con una cuenta de alumno y utilizando una URL con la que se podrían ver los alumnos desde una cuenta de profesor.

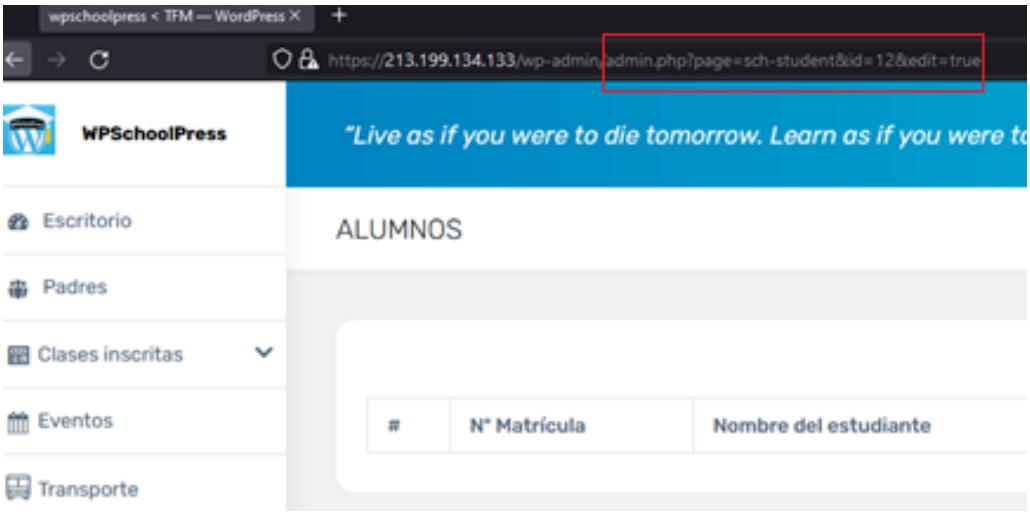


Ilustración 170: Intento de acceso a la lista de alumnos

Vemos que, aunque no muestra ningún error, el sistema no nos devuelve ningún alumno en la lista. A continuación, intentamos obtener la lista de clases.

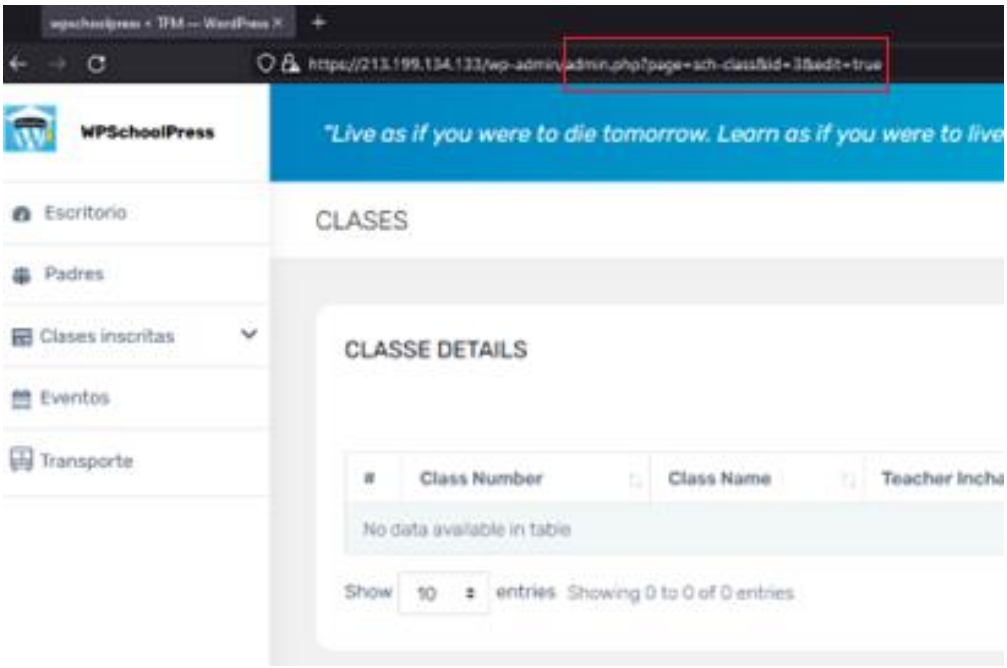


Ilustración 171: Intento de acceso a lista de clases

El acceso a esta URL tampoco nos muestra información en la lista, con lo que el acceso a recursos restringidos desde la aplicación parece funcionar correctamente. Intentamos realizar también un acceso a alguna URL de un recurso restringido dentro del servidor, por ejemplo, de un archivo *readme.txt*.

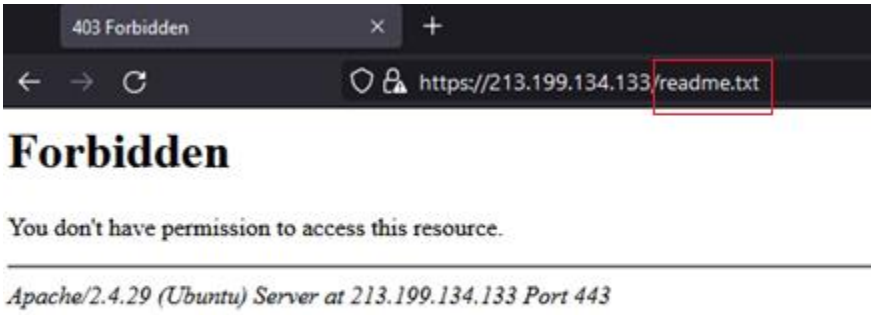


Ilustración 172: Intento de acceso a recurso restringido

Vemos que el servidor nos devuelve un error de acceso restringido al recurso. A continuación, intentamos acceder al panel de administración desde una máquina que no se encuentra en la lista de IP permitidas.

Ilustración 173: Intento de acceso al panel de administración

En este caso también devuelve un error de acceso restringido, aunque esta vez es el *Application Gateway* el que bloquea el acceso al mismo.

9.4. Evaluación de vulnerabilidades

Se realizará un análisis de vulnerabilidades mediante la herramienta OWASP ZAP [5] para evaluar la seguridad del sistema propuesto identificando posibles debilidades y brechas de seguridad. Esta evaluación ayudaría a cumplir el requisito 14.2.1.

[5] https://www.zaproxy.org/

Zed Attack Proxy (ZAP), es una herramienta gratuita y de código abierto utilizada para realizar *pentesting* [42]. Está diseñada específicamente para testear aplicaciones web.

Esta herramienta crea un proxy que se coloca entre un navegador y la aplicación web que se quiere examinar, de manera que la herramienta puede interceptar e inspeccionar los mensajes entre el navegador y la aplicación web, modificando los mensajes en caso de ser necesario.

Ilustración 174: Zed Attack Proxy [42]

La herramienta está incluida en Kali Linux, en caso de no estarlo puede instalarse fácilmente mediante el comando:

```
sudo apt install zaproxy
```

Una vez instalado es necesario configurar el proxy desde Firefox. Para ello, desde los ajustes de conexión, añadimos un proxy HTTP con dirección localhost y puerto 8080.

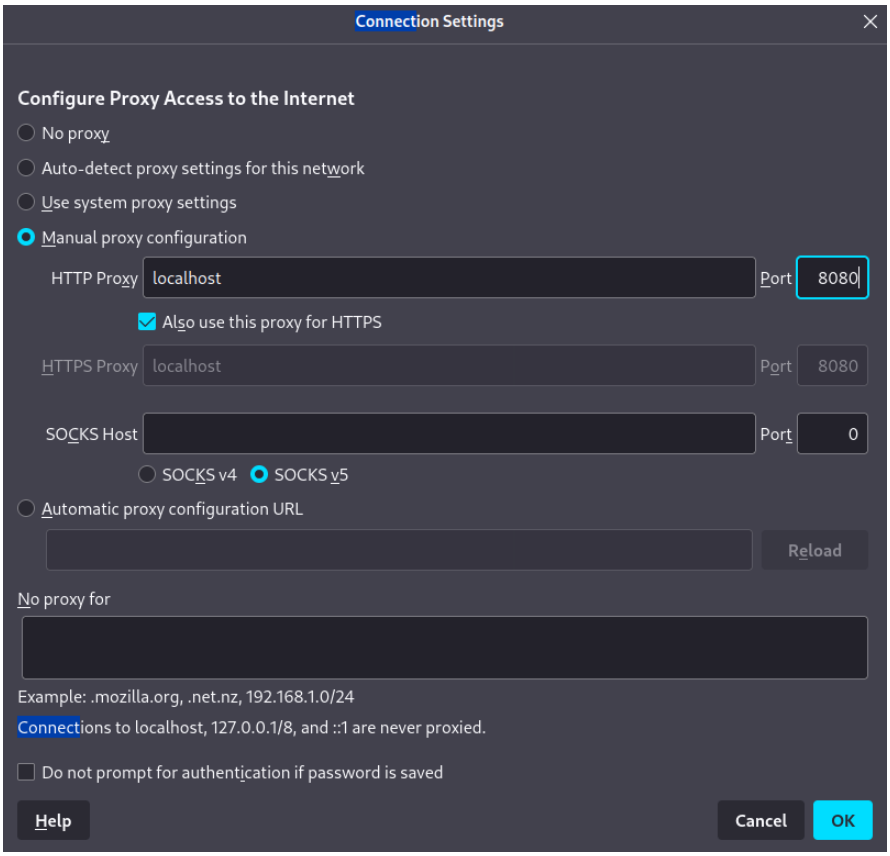


Ilustración 175: Configuración de un proxy en Firefox

Tras configurar el proxy ejecutamos OWASP ZAP y comprobamos que ha podido interceptar el navegador.

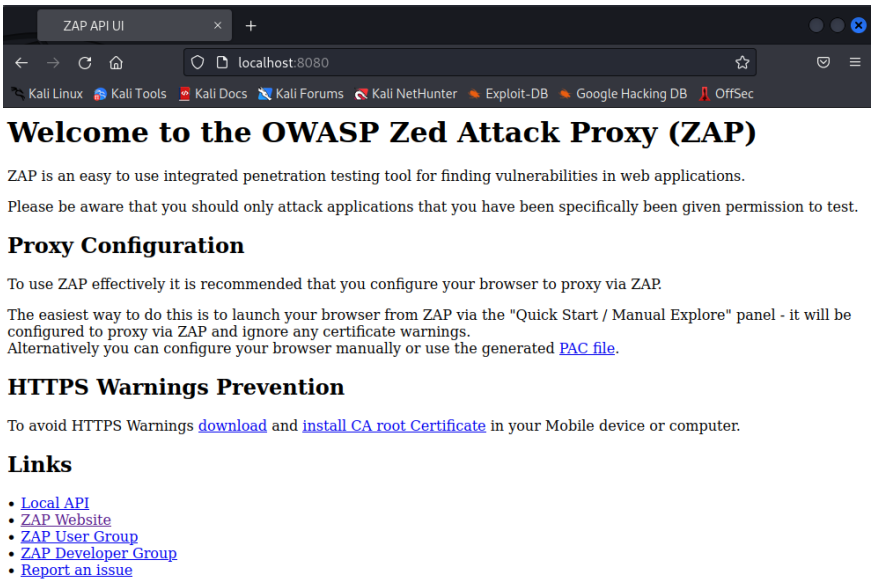


Ilustración 176: Navegador interceptado por OWASP ZAP

A continuación, es necesario configurar un certificado SSL para poder descifrar las conexiones HTTPS que el navegador establezca. Esto se puede realizar desde *Dynamic SSL Certificates* en las opciones de ZAP.

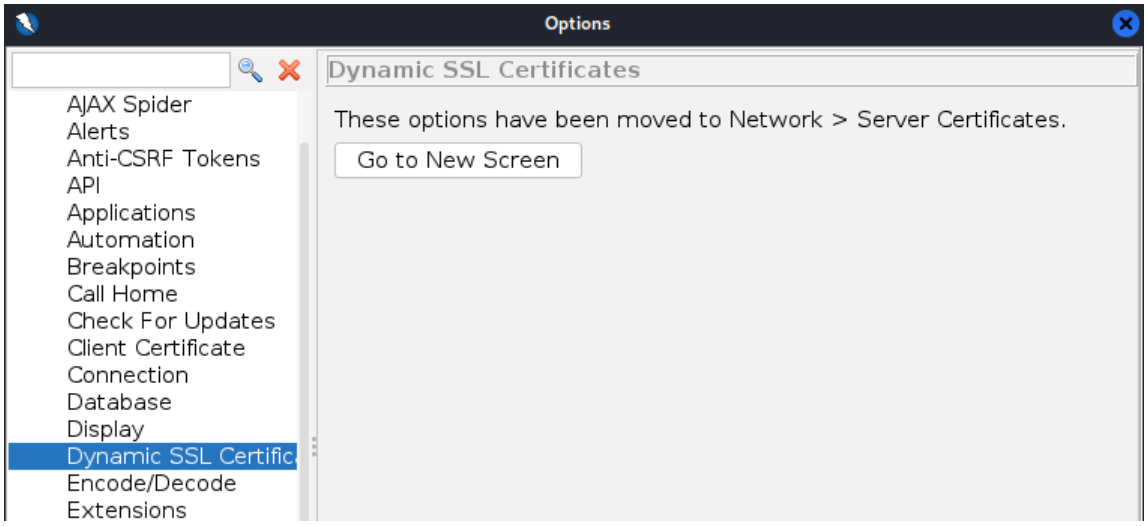


Ilustración 177: Dynamic SSL Certificates en ZAP

Desde la nueva ventana, generamos un nuevo certificado raíz y lo exportamos.

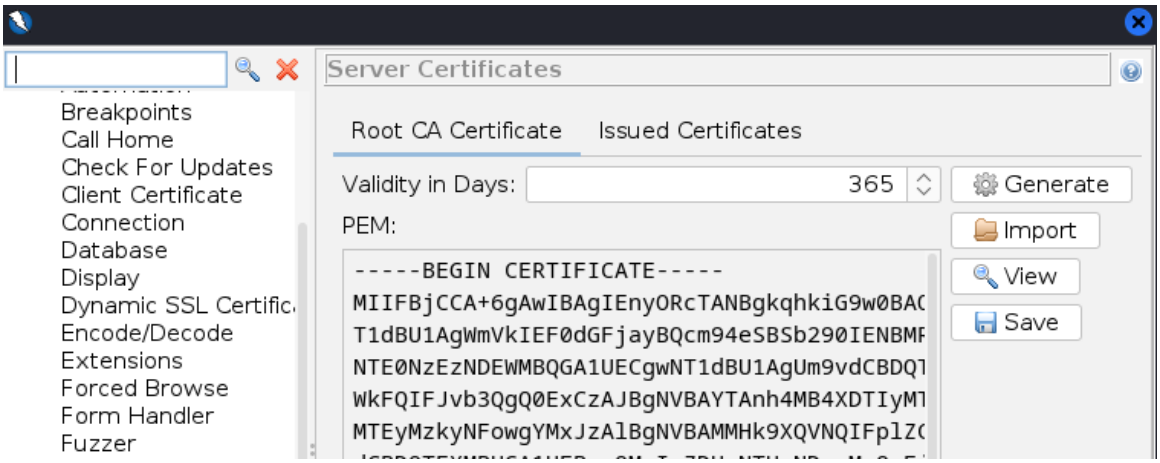


Ilustración 178: Creación de un certificado raíz desde ZAP

A continuación, desde el gestor de certificados de Firefox, importamos una nueva autoridad que será el certificado guardado anteriormente y marcamos que confié en él.

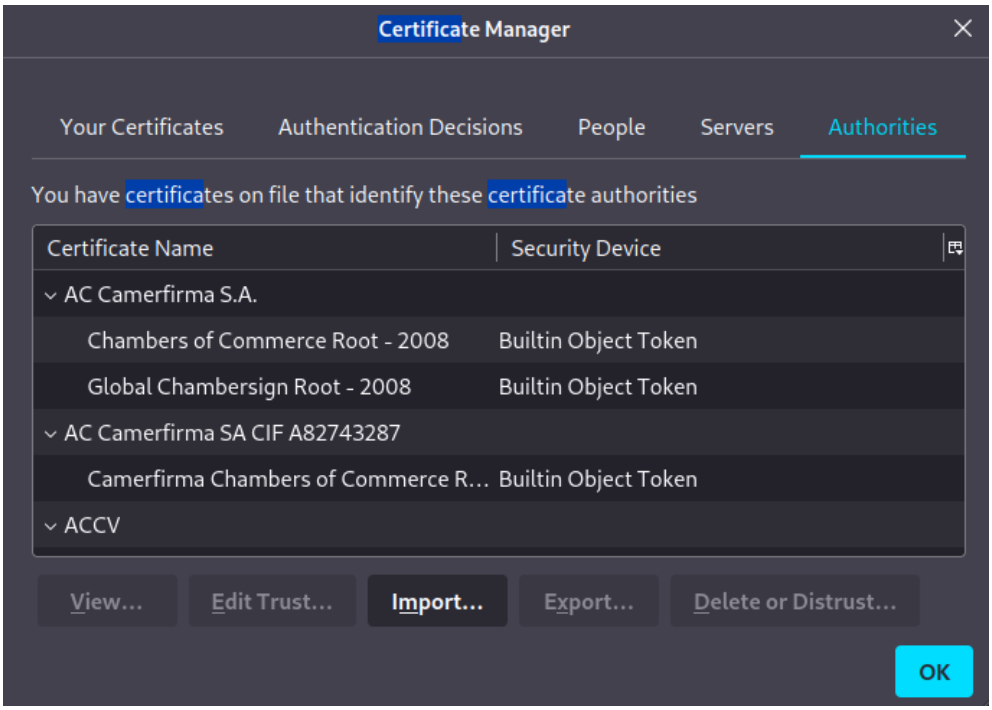


Ilustración 179: Gestor de certificados en Firefox

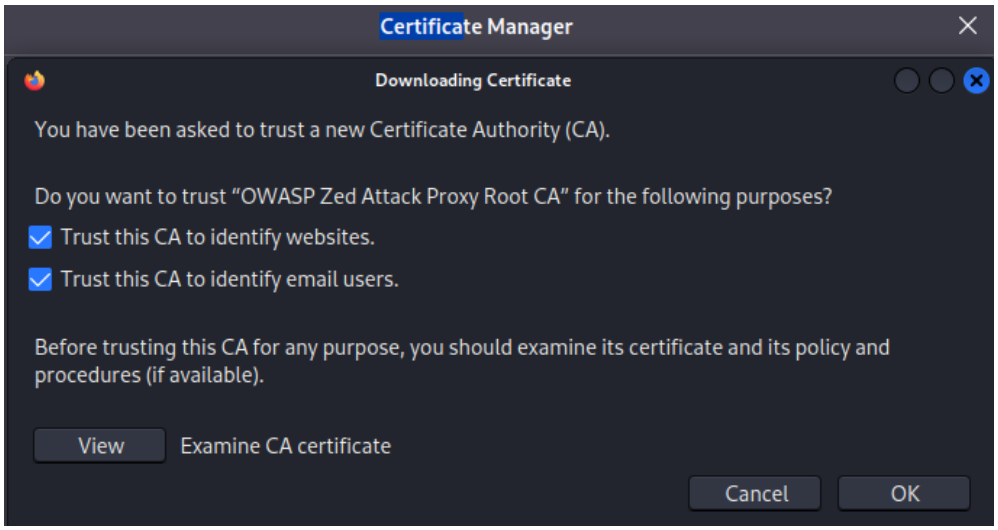


Ilustración 180: Certificado importado en Firefox

Una vez hecho esto, ya podemos realizar la conexión a la web desde el navegador y comprobar que OWASP ZAP lo intercepta.

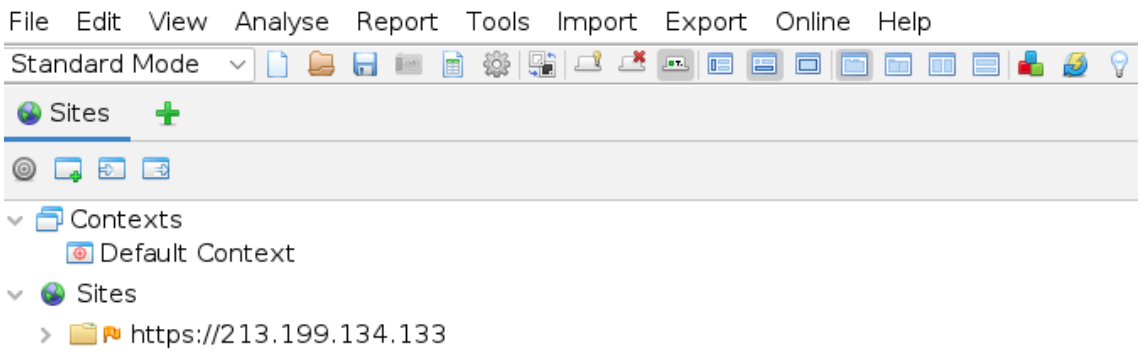


Ilustración 181: Web interceptada por OWASP ZAP

La prueba se realizará iniciando sesión mediante un usuario alumno. En versiones anteriores del plugin WPSchoolPress se incluían plantillas de las páginas, pero esto fue eliminado y el plugin paso a utilizar direcciones de *wp-admin* para acceder a las páginas lo cual presenta un peligro al estar realizando las peticiones a través de la administración. La dirección utilizada por el plugin WPSchoolPress para las páginas son de la forma "/wp-admin/admin.php?page=sch-", con lo que habrá que modificar la regla personalizada del WAF que bloqueaba las direcciones *wp-admin* para que permita en tráfico en esa ruta en específico, separando así la parte del plugin y la de administración.

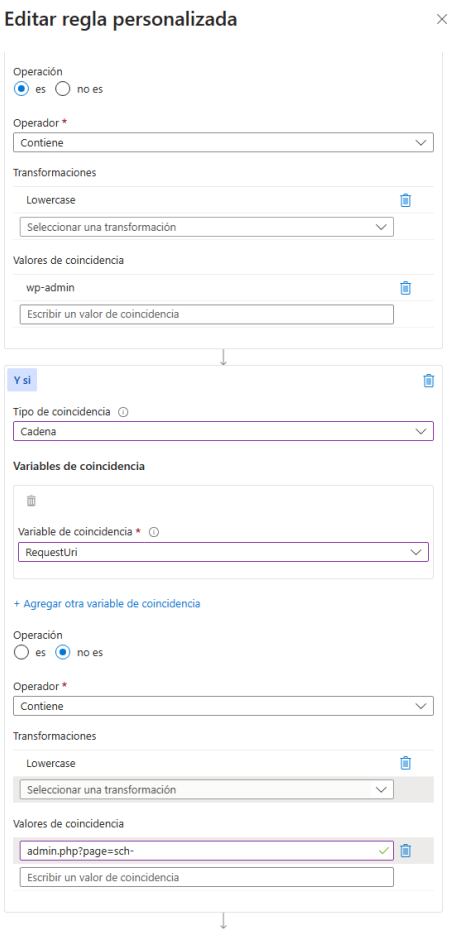


Ilustración 182: Nueva regla personalizada en el WAF

Existen varios modos de escaneo en OWASP ZAP [43]:

- *Safe*: No realiza operaciones peligrosas.
- *Protected*: Solo se realizan operaciones peligrosas en el alcance permitido.
- *Standard*: No se restringe nada.
- *ATTACK*: No se restringe nada y los nuevos nodos se escanean en cuando son descubiertos.

Se utilizará el modo ATTACK puesto que no se trata de un entorno de producción y ya se han realizado copias de seguridad. Creamos un nuevo *Active Scan* y marcamos como punto de inicio el panel de WPSchoolPress.

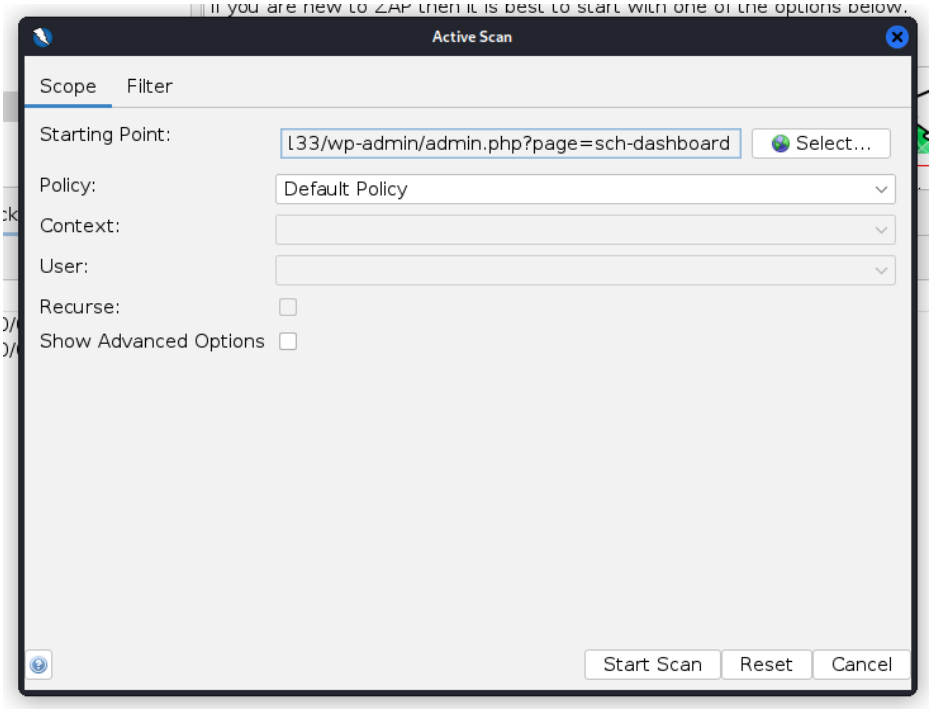


Ilustración 183: Nuevo Escaneo en OWASP ZAP

Podremos realizar un seguimiento del escaneo desde el panel principal de OWASP ZAP.

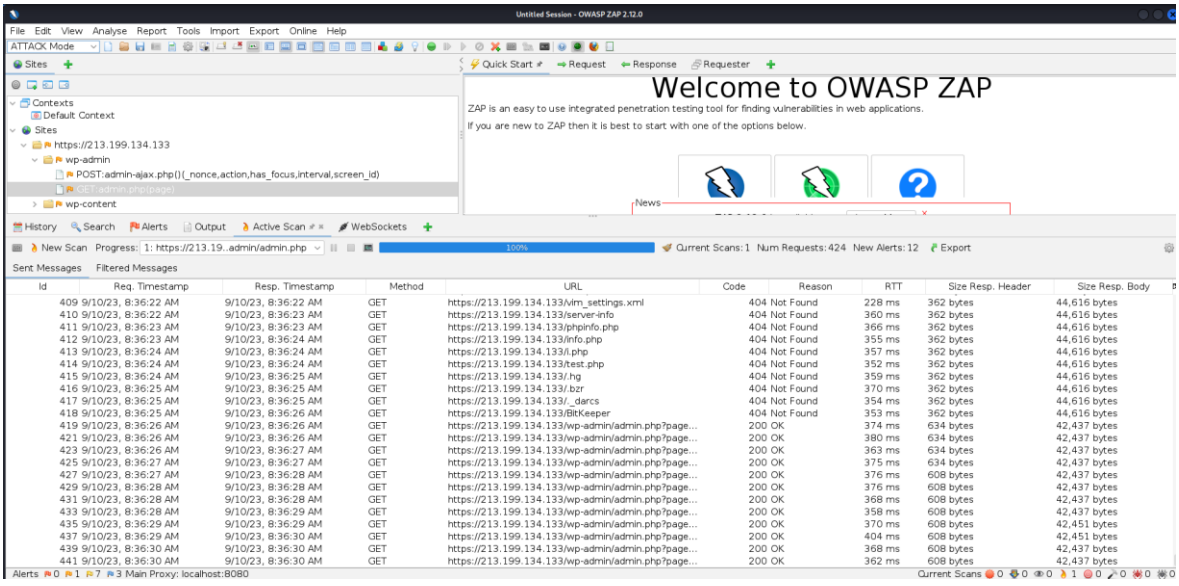


Ilustración 184: Seguimiento del escaneo de OWASP ZAP

Una vez terminado el escaneo podemos ver las alertas que se han generado, estos resultados se utilizaran en la sección de subsanación de errores para mejorar la seguridad del sistema, el reporte al completo puede encontrarse en el apéndice I.

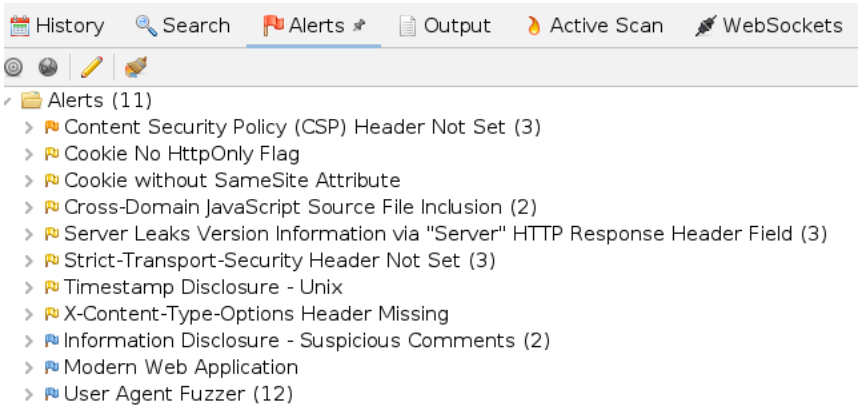


Ilustración 185: Alertas generadas por OWASP ZAP

9.5. Evaluación de logs

Se van a comprobar las dos fuentes de logs principales, desde *Application Gateway* y WP Activity Log, para ver que mediante estas se podría hacer un seguimiento de un ataque, para ello tendrán que dar una escala de tiempo y diferente información de seguridad, también tendrán que aportar información de control de acceso. Esta evaluación indicaría si se han cumplido los requisitos 7.1.4, 7.3.1 y 7.1.3.

Desde Microsoft Sentinel podemos ver que se han aparecido incidentes debido a los escaneos realizados sobre la web, lo que significa que el *Application Gateway* los ha detectado.

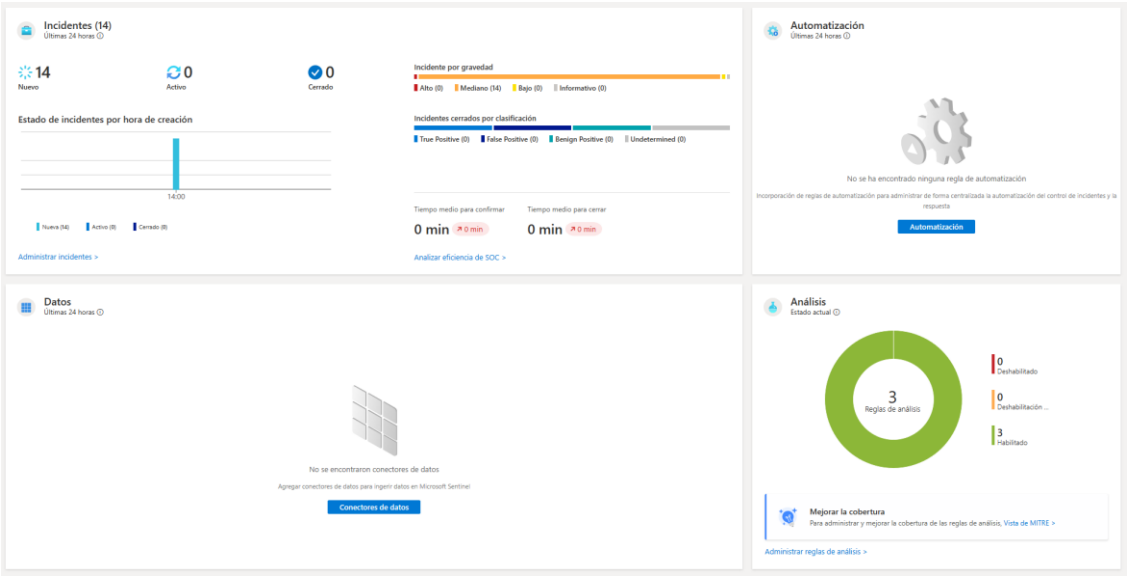


Ilustración 186: Incidentes generados en Microsoft Sentinel

Vemos que se han generado alertas con la regla que se creó anteriormente.

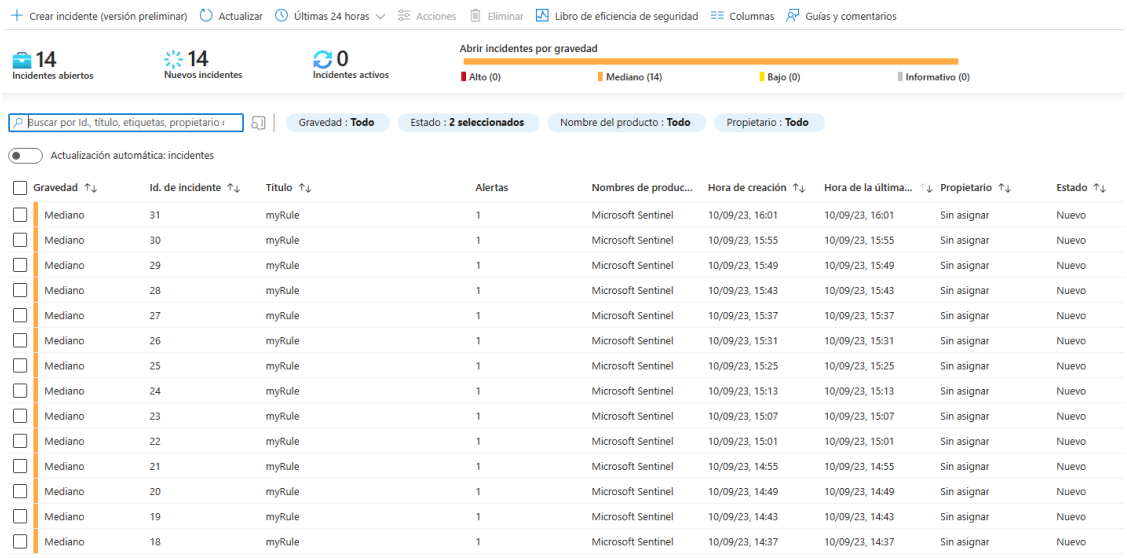


Ilustración 187: Incidentes generados con la regla personalizada

Sobre cada incidente podemos ver más información, incluyendo que regla lo ha generado y el número de eventos detectados.

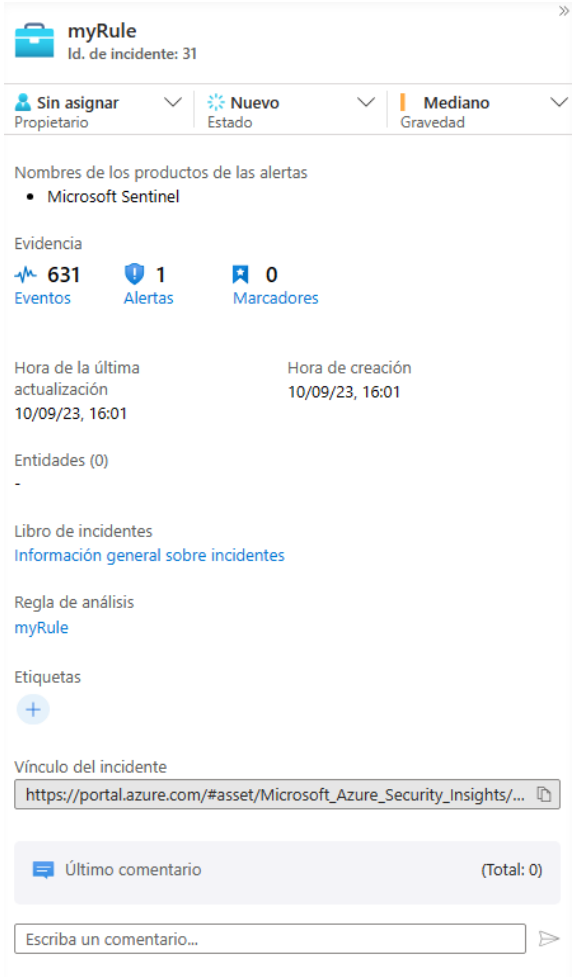


Ilustración 188: Información sobre el incidente en Microsoft Sentinel

A continuación, comprobamos los logs generados por la regla para ver si muestran suficiente información con la que poder hacer un seguimiento de un posible ataque tal y como se había presentado al inicio de la sección.

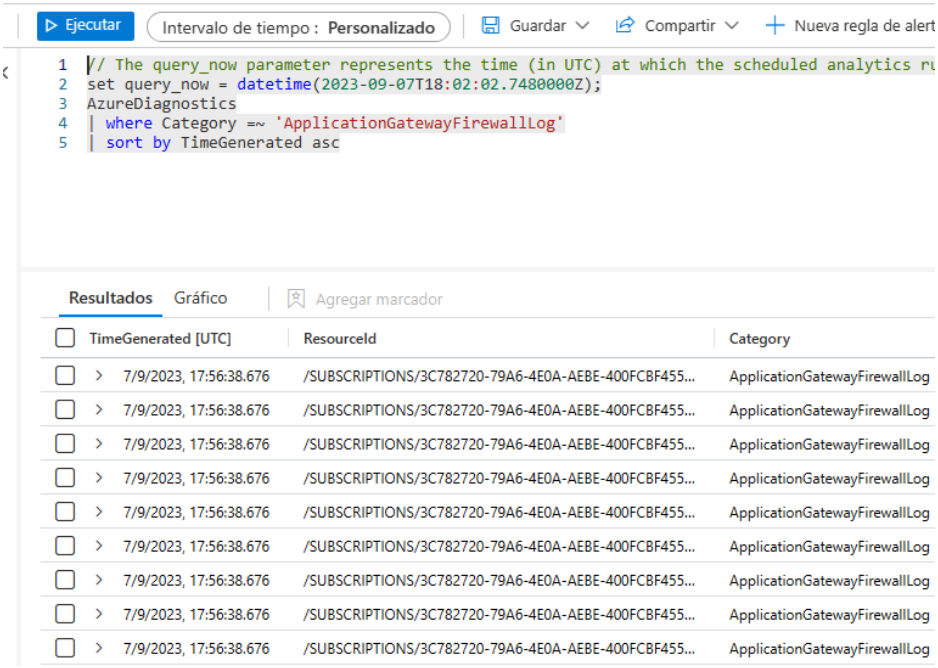


Ilustración 189: Logs generados desde *Application Gateway*

Cada log puede inspeccionarse individualmente para ver toda su información.

TenantId	078ec0be-0b20-4795-b559-0525760fcbe3
TimeGenerated [UTC]	2023-09-10T13:55:56.2560659Z
ResourceId	/SUBSCRIPTIONS/3C782720-79A6-4E0A-AEBE-40
Category	ApplicationGatewayFirewallLog
ResourceGroup	TFM
SubscriptionId	3c782720-79a6-4e0a-aebe-400fcbf45572
ResourceProvider	MICROSOFT.NETWORK
Resource	MYAPPLICATIONGATEWAY
ResourceType	APPLICATIONGATEWAYS
OperationName	ApplicationGatewayFirewall
requestUri_s	/privatekey.key
Message	URL file extension is restricted by policy

Ilustración 190: Ejemplo de log generado por Application Gateway primera parte

instanceId_s	appgw_3
SourceSystem	Azure
clientIp_s	[redacted]
ruleSetType_s	OWASP CRS
ruleSetVersion_s	3.2
ruleId_s	920440
ruleGroup_s	REQUEST-920-PROTOCOL-ENFORCEMENT
action_s	Matched
details_message_s	Pattern match \.([^.]+)$; Within Tx:restricted_extensions at TX:extension.
details_data_s	{.key found within [REQUEST_BASENAME:privatekey.key]} and { found within [TX:extension:.key/]}
details_file_s	REQUEST-920-PROTOCOL-ENFORCEMENT.conf
details_line_s	974
hostname_s	213.199.134.133
policyId_s	135#_subscriptions_3c782720-79a6-4e0a-aebe-400fcbf45572_resourceGroups_TFM_providers_Mi
policyScope_s	Global

Ilustración 191: Ejemplo de log generado por Application Gateway segunda parte

Vemos que para el ejemplo anterior se bloqueó el acceso puesto que se intentó acceder a una URL con la extensión *.key*, la cual se encuentra prohibida.

Los logs generados por *Application Gateway* nos dan por lo tanto una escala de tiempo para poder seguir la investigación de un posible ataque y diferente información de seguridad como:

- URL solicitada.
- IP del cliente.
- Patrón de la regla.
- Descripción del posible ataque.
- IP a la que se dirigía el ataque.

En el caso de los logs de WP Activity Log podemos observar los diferentes accesos que se producen a la aplicación, incluyendo los que han tenido éxito, los intentos y las desconexiones.

1001	⚠	7 de octubre de 2023 10:30:03.000	AlumnoPrueba Student	10.0.0.7	Usuario	Salir	Usuario desconectado.
1000	⚠	7 de octubre de 2023 10:29:18.000	AlumnoPrueba Student	10.0.0.7	Usuario	Acceder	Usuario conectado.
1002	⚠	7 de octubre de 2023 10:29:17.000	AlumnoPrueba Student	10.0.0.7	Usuario	Acceso fallido	2 acceso(s) fallido(s).

Ilustración 192: Logs de acceso en WordPress

Nos fijamos, por ejemplo, en el log de acceso fallido para ver qué información proporciona.

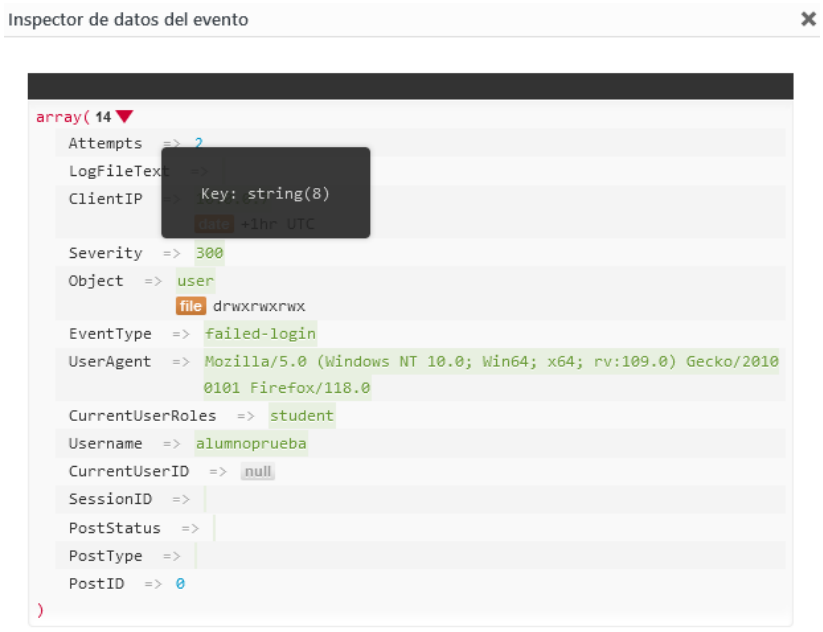


Ilustración 193: Ejemplo de log generado por WP Activity Log

Vemos que muestra diferente información de seguridad como:

- Número de intentos.
- IP del cliente.
- Severidad.
- Evento producido.
- Usuario al que afecta.
- Navegador utilizado.
- Rol del usuario.

Por otro lado, iThemes Security también ofrece una serie de logs que podrían ser útiles para realizar el seguimiento de un ataque, estos ofrecen información sobre los eventos del plugin, como por ejemplo los análisis de vulnerabilidades, las copias de seguridad o las modificaciones de archivos.

Ilustración 194: Ejemplo de eventos de IThemes Security

Se puede ver más información de cada uno de los logs, por ejemplo, de los cambios de archivos.

Ilustración 195: Ejemplo de log en IThemes Security primera parte

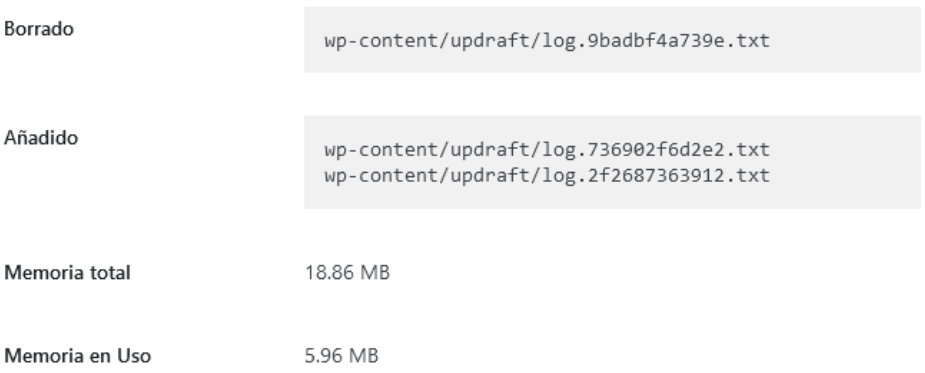


Ilustración 196: Ejemplo de log en IThemes Security segunda parte

Vemos que además de la escala de tiempo aportada información sobre que archivos fueron creados, borrados o modificados, indicando específicamente los archivos afectados, lo cual podría ayudar a realizar un seguimiento de los movimientos de un atacante en el sistema.

9.6. Subsanación de errores

En esta sección se solucionarán algunos de los errores que han sido identificados debido a la evaluación de seguridad.

9.6.1. Subsanación de errores de cabeceras HTTP

Vamos a tratar de solucionar algunas de las alertas que nos propuso la herramienta ZAP. Vemos que muchas de ellas se producen debido a malas configuraciones en las cabeceras HTTP, podemos configurar las mismas desde el *Application Gateway*, para ello vamos a la pestaña de reescrituras.

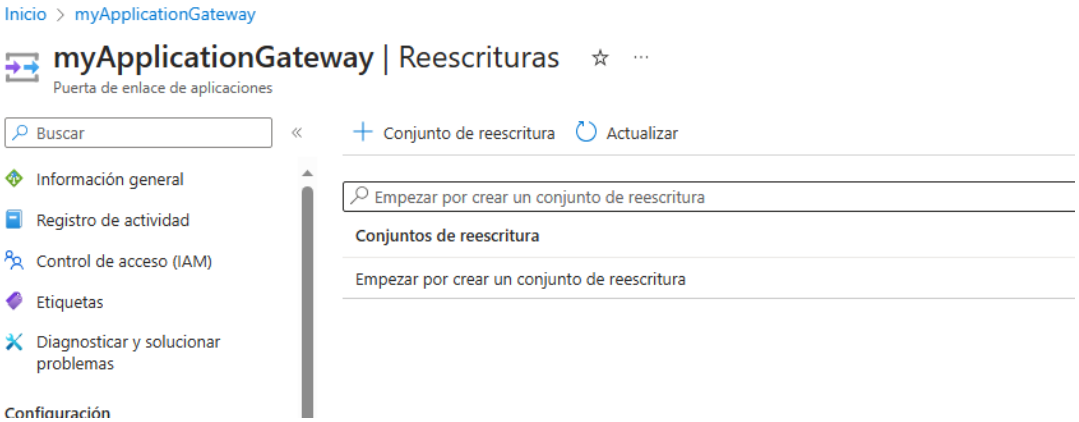


Ilustración 197: Reescrituras en Application Gateway

Creamos un nuevo conjunto de reescritura y lo asociamos con las reglas de enrutamiento del *Application Gateway*.

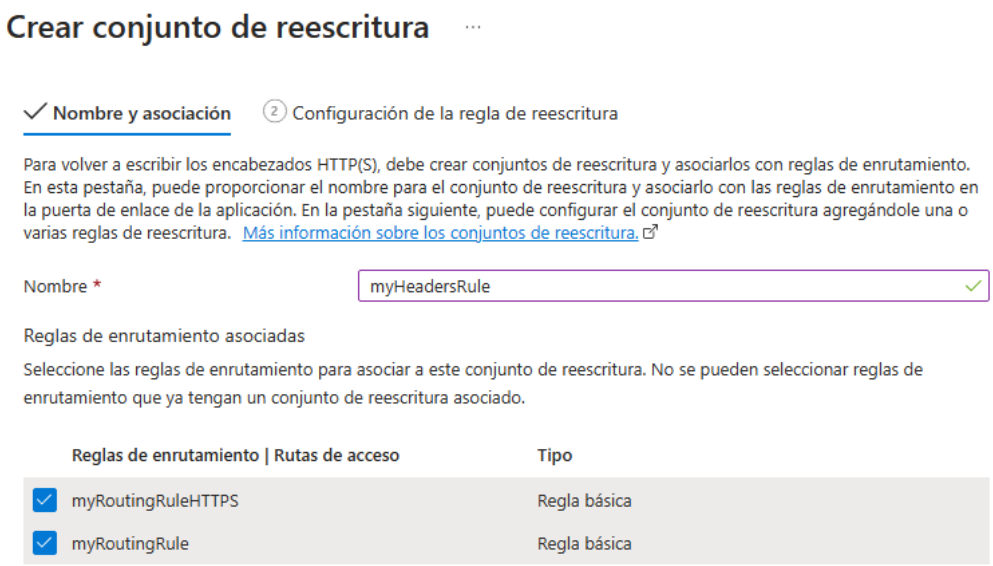


Ilustración 198: Nuevo conjunto de reescritura en Application Gateway

Podemos agregar nuevas reglas de reescritura al conjunto, estas reescribirán las cabeceras HTTP.

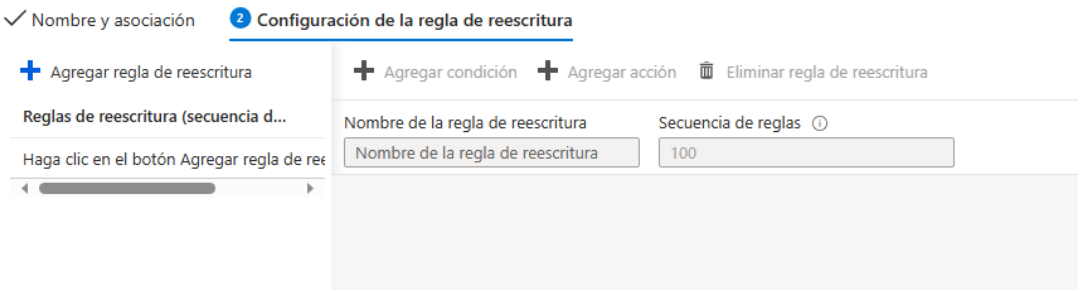


Ilustración 199: Reglas de reescritura en Application Gateway

Se reescribirán las siguientes cabeceras [44]:

- Content-Security-Policy: Aporta protección contra los ataques XSS añadiendo fuentes de contenido aprobado a una *whitelist*.
- X-Content-Type-Options: Hace que el navegador detenga sus intentos de realizar MIME-sniff del contenido, es decir de intentar inspeccionar el contenido para deducir el formato de archivo.
- Server: Revela información sobre el servidor.
- Strict-Transport-Security: Refuerza la implementación del TLS forzando el uso de HTTPS.

- X-Frame-Options: Indica al navegador si el sitio web puede ser renderizado en un *frame* para ser embebido en otro sitio, esto puede provocar ataques de *click-jacking*.
- Referrer-Policy: Permite controlar cuánta información es incluida por el navegador desde fuera de la web.
- X-Powered-By: Indica información del software utilizado.
- X-XSS-Protection: Impide la carga de una página al detectar ataques XSS [45].

Para configurar las cabeceras podemos seguir la guía de seguridad en HTTP publicada por Mozilla [46]. Para configurarlas, se indica que será la cabecera de respuesta, si se establecerá un nuevo valor o se eliminará la cabecera, de qué cabecera se trata y el nuevo valor.

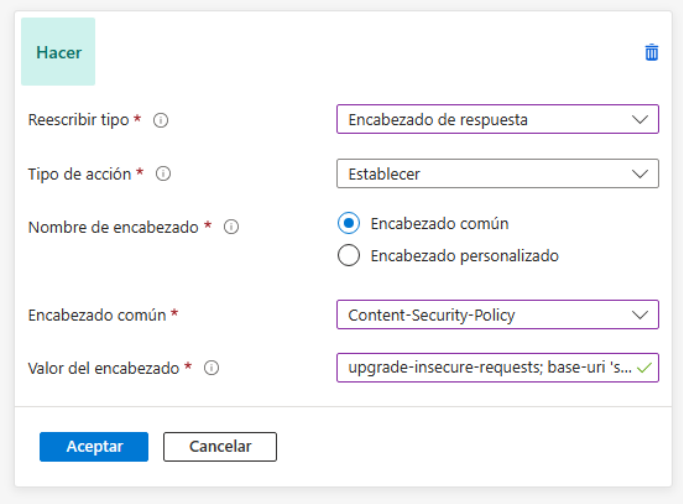


Ilustración 200: Ejemplo de regla de cabecera HTTP

Tras configurarlas podremos guardar el conjunto para que se apliquen las nuevas reglas.

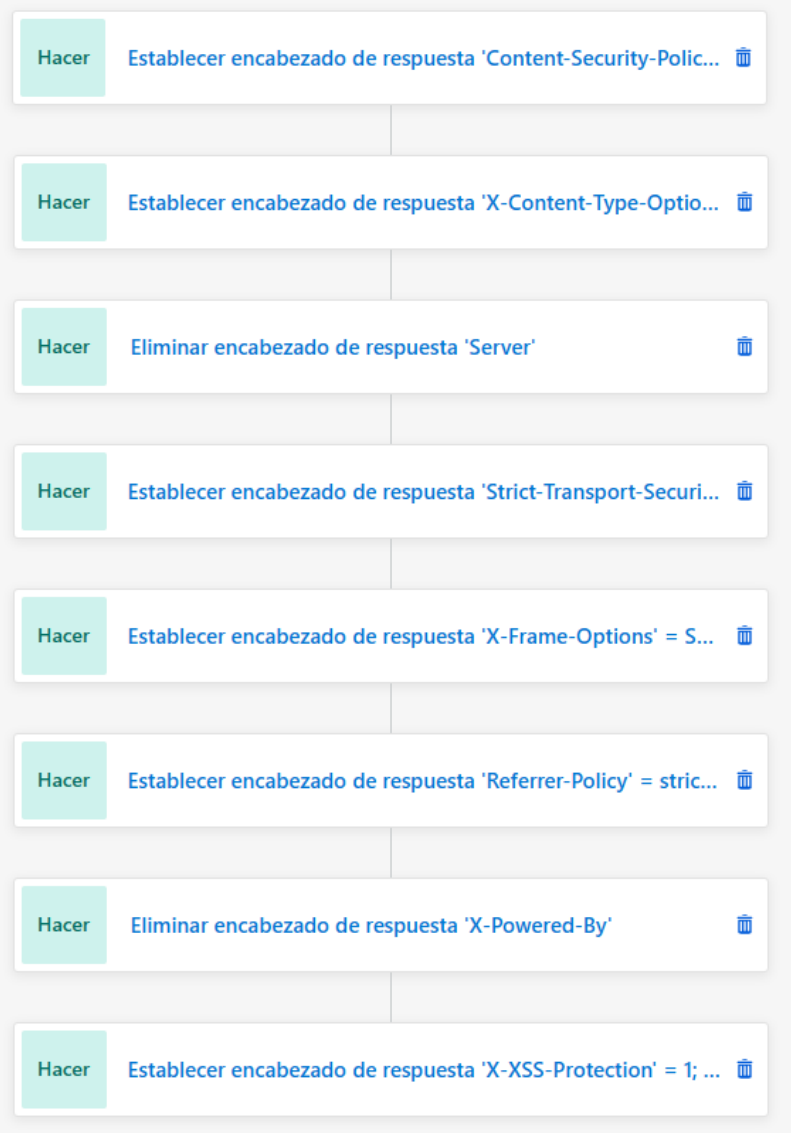


Ilustración 201: Lista de reglas de cabeceras HTTP

Volvemos a escanear la web y vemos que ya no nos muestra las alertas sobre las cabeceras HTTP. El reporte generado puede encontrarse en el apéndice I.

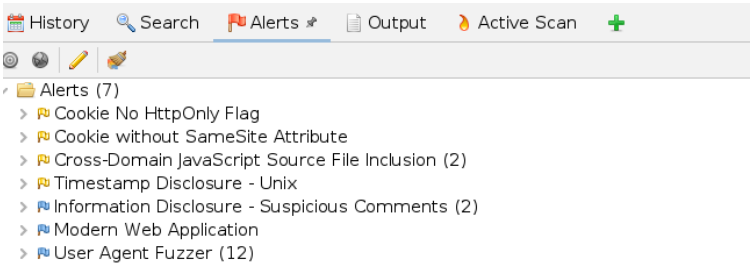


Ilustración 202: Alertas tras los cambios en las cabeceras

9.6.2. Subsanación de seguridad de las contraseñas

Vamos a cambiar el método que utiliza WordPress a la hora de generar el hash de las contraseñas, para ello instalaremos el plugin propuesto en la evaluación, este se puede encontrar en el propio repositorio de WordPress.

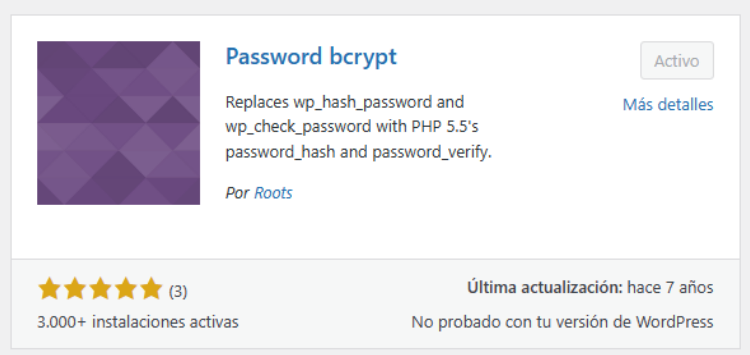


Ilustración 203: Plugin Password bcrypt

Las contraseñas generadas por este plugin quedarían de la siguiente manera frente a las generadas mediante MD5:

- MD5: PBXWL4/IZFGh7LyZrnGzhOy0BODynL00
- bcrypt: 2y10bB31V7.ijogsXiX8CtF8leRa2kHXVSwpxXkOaxaMwb4C5ifNzSW.i

Podemos comprobar cómo de fuerte sería una contraseña cuyo hash haya sido calculado mediante bcrypt frente a un hash calculado con MD5 mediante una calculadora de ataques de fuerza bruta[6]. Para el cálculo haremos uso de una contraseña de 12 caracteres que es lo establecido por la política de *iThemes Security* [47].

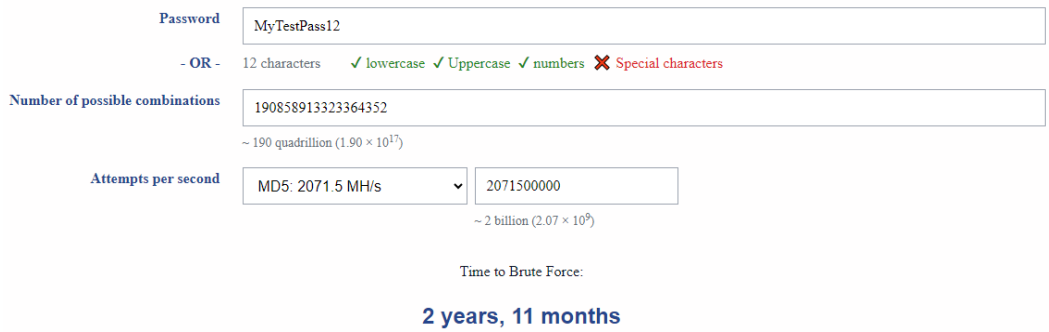


Ilustración 204: Cálculo de fuerza bruta para MD5

[6] https://www.proxynova.com/tools/brute-force-calculator

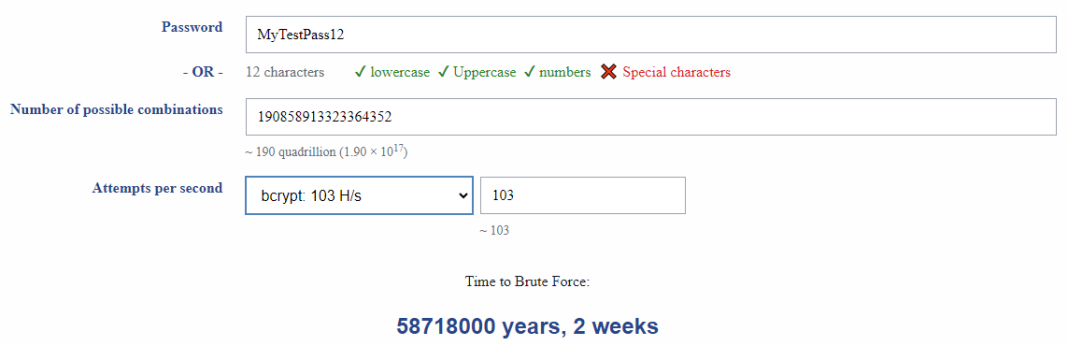


Ilustración 205: Cálculo de fuerza bruta para bcrypt

Vemos que el tiempo requerido para bcrypt sería mucho mayor, sin embargo, es necesario tener en cuenta que ambos tiempos disminuirían notablemente en caso de que se utilizara una lista de contraseñas para realizar el ataque y la contraseña se encontrará en dicha lista.

10. Conclusiones

Este documento ha presentado de forma general un ejemplo de cómo se podría realizar el despliegue seguro de un servicio en la nube.

Es importante analizar el servicio que se pretende desplegar para detectar los diferentes actores que lo utilizaran y la serie de tecnologías que podrían utilizarse para desarrollar el mismo.

Esto también ayuda a identificar los aspectos legales que deberán tenerse en cuenta en el desarrollo.

El siguiente paso debe ser realizar un análisis de riesgos para poder encontrar los principales activos a defender y las amenazas que podrían suponer un riesgo para el sistema. Gracias a esto es posible centrarse en los activos que es necesario defender y en la forma de defender los mismos al saber que los amenaza, basándonos en lo anterior se podrán marcar unos requisitos de seguridad centrados, tanto en los activos que realmente deberíamos proteger, como enfocados en las amenazas más probables al presentar los mayores riesgos para los activos.

Los requisitos obtenidos y las amenazas detectadas han permitido analizar de forma más precisa las medidas de seguridad necesarias para el sistema, tras lo cual es necesario investigar las tecnologías que ayudarán a implementar estas medidas, tanto del proveedor en la nube como de otros terceros.

Tras saber la forma de defender el sistema hay que diseñar su arquitectura con todo lo propuesto y analizar los costes que esta supondría, lo que ayudaría a añadir o retirar ciertas medidas en caso de que el coste se desviara del previsto por una organización, en este caso se tendrían que aceptar ciertos riesgos en el sistema con el objetivo de llegar a los costes propuestos.

Durante el despliegue se ha podido ir viendo si los servicios del proveedor que se habían seleccionado han sido acertados para el sistema o no. En general estos servicios han cubierto lo propuesto, aunque se han encontrado algunos problemas, sobre todo respecto a las copias de seguridad, puesto que no estaban soportadas

para el sistema de almacenamiento compartido propuesto, lo que ha llevado a utilizar un servicio de copias de seguridad de un tercero.

El mayor problema encontrado en el despliegue ha sido debido al plugin de WordPress seleccionado para construir el servicio del instituto. Éste parecía estar bien actualizado y con soporte, pero había algunas funciones que no funcionaban y algunos aspectos de su configuración, como las rutas de sus recursos, eran poco seguras al utilizar el panel de administración, algo de lo que no se informaba en su documentación y que no se realizaba de esa manera en versiones anteriores.

En el documento se han presentado también los costes para el sistema de prueba que ha sido el desplegado. Este sistema ha ayudado a tener una visión más clara del funcionamiento de un servicio en la nube y de su seguridad, también a encontrar posibles fallas en las soluciones propuestas en todo el proceso anterior.

Por último, se ha realizado una evaluación del despliegue realizado para ver si ciertos requisitos se han ido cumpliendo, realizando para ello simulaciones de ataques o analizando algunos de los componentes desplegados.

Este proceso ha llevado a encontrar ciertas fallas en el proceso, por ejemplo, se han tenido que subsanar ciertos problemas detectados durante la evaluación de seguridad. Estos habrían quedado cubiertos si durante el proceso de desarrollo se hubieran añadido requisitos que los cubrieran.

Respecto a posibles mejoras a futuro, sería interesante intentar realizar un análisis de riesgo más completo que ayude no solo a detectar la mayor cantidad de amenazas, también a priorizar las más importantes para el sistema, tras lo que se podrían añadir más requisitos de seguridad para intentar cubrir estas últimas, llevando esto a la investigación de más tecnologías que ayudarán a cubrir los requisitos. Sin embargo, en el caso de una organización, no sería del todo realista, puesto que no siempre es posible cubrir todo lo expuesto en un análisis de riesgo, ya sea por los costes que supondría o por no tener tecnología que pueda cubrirlo al completo.

A nivel personal, este trabajo me ha ayudado a comprender mejor cómo se realizaría el análisis de los aspectos de seguridad en un sistema y cómo se

integraría este en el proceso completo de desarrollo del mismo, pudiendo realizar esto de una forma más realista de la que se podría hacer si solo se realizará el análisis de forma individual.

También me ha permitido aprender a realizar despliegues en Azure y poder hacer uso de las diferentes herramientas que este proporciona para fortalecer la seguridad del sistema.

Por otro lado, me ha servido para repasar varios conceptos de servidores y aprender más sobre WordPress y las diferentes formas mediante las cuales se puede aumentar la seguridad del mismo.

El análisis de costes realizado, me ha permitido tener una mejor idea del coste total que un servicio desplegado en la nube de forma segura podría tener.

Por último, la evaluación de seguridad me ha permitido encontrar errores derivados del proceso anterior, lo que me permitirá poder realizar un mejor trabajo en los diferentes pasos en un futuro. También me ha permitido aprender ciertas vulnerabilidades y formas mediante las que un atacante podría llegar a explotar un sistema.

Bibliografía

[1] Check Point Software Technologies Ltd, «Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most,» 27 04 2023. [En línea]. Available: https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/#:~:text=Global%20weekly%20attacks%20rose%20by,increase%20compared%20to%20Q1%202022.

[2] Agencia Española de Protección de Datos, «Guía del reglamento general de protección de datos,» [En línea]. Available: https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf.

[3] Atico34, «Implantación RGPD: Guía práctica 2023,» 2023. [En línea]. Available: https://protecciondatos-lopd.com/empresas/implantacion-rgpd/.

[4] Agencia Española de Protección de Datos, «Guía para centros educativos,» [En línea]. Available: https://www.aepd.es/es/documento/guia-centros-educativos.pdf.

[5] pilar-tools, «Pilar Micro, Manual de Usuario,» Abril 2022. [En línea]. Available: https://www.pilar-tools.com/doc/manual_micro_es_20221.pdf.

[6] OWASP, «Application Security Verification Standard,» Octubre 2021. [En línea]. Available: https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-es.pdf.

[7] Microsoft, «Documentación de Azure,» 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/.

[8] Microsoft, «¿Qué es Azure Virtual Network?,» 13 05 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/virtual-network/virtual-networks-overview.

[9] Microsoft, «¿Qué es un punto de conexión privado?,» 29 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/private-link/private-endpoint-overview.

[10] Microsoft, «¿Qué es Azure Files?,» 25 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/storage/files/storage-files-introduction.

[11] Microsoft, «Azure Database for MySQL con la opción flexible,» 10 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/mysql/flexible-server/overview.

[12] Microsoft, «Acerca de Azure Key Vault,» 25 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/key-vault/general/overview.

[13] Microsoft, «Autenticación de Azure Key Vault,» 25 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/key-vault/general/authentication.

[14] Microsoft, «¿Qué es Azure VPN Gateway?,» 11 Agosto 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/vpn-gateway/vpn-gateway-about-vpngateways.

[15] Microsoft, «¿Qué es Azure Application Gateway?,» 01 06 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/application-gateway/overview.

[16] Microsoft, «Introducción a Azure Monitor,» 23 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/azure-monitor/overview.

[17] Microsoft, «¿Qué es Microsoft Defender for Cloud?,» 21 05 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/defender-for-cloud/defender-for-cloud-introduction.

[18] Microsoft, «¿Qué es Microsoft Sentinel?,» 11 04 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/sentinel/overview.

[19] Wordpress.org, «Hardening Wordpress,» [En línea]. Available: https://wordpress.org/documentation/article/hardening-wordpress/.

[20] Microsoft, «Diseño de arquitectura de seguridad,» [En línea]. Available: https://learn.microsoft.com/es-es/azure/architecture/guide/security/security-start-here.

[21] Microsoft, «Grupos de reglas y reglas de Web Application Firewall DRS y CRS,» 23 06 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=drs21.

[22] WP White Security, «WP Activity Log,» [En línea]. Available: https://wordpress.org/plugins/wp-security-audit-log/#description.

[23] Microsoft, «Seguridad en las redes,» 20 Abril 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/well-architected/security/design-network.

[24] Microsoft, «Consideraciones sobre la protección de datos,» 20 Abril 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/well-architected/security/design-storage.

[25] Microsoft, «Calculadora de precios,» [En línea]. Available: https://azure.microsoft.com/es-es/pricing/calculator/.

[26] Microsoft, «Crear soluciones en la nube gratis con Azure for Students,» 2023. [En línea]. Available: https://azure.microsoft.com/es-es/free/students.

[27] Microsoft, «Administración de grupos de recursos de Azure con Azure Portal,» 16 08 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/azure-resource-manager/management/manage-resource-groups-portal.

[28] Microsoft, «Inicio rápido: Uso de Azure Portal para crear una red virtual,» 22 08 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/virtual-network/quick-

create-portal.

[29] Microsoft, «Direcciones IP públicas,» 24 08 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/virtual-network/ip-services/public-ip-addresses.

[30] Microsoft, «Inicio rápido: Dirección del tráfico web con Azure Application Gateway: Azure Portal,» 08 06 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/application-gateway/quick-create-portal.

[31] Microsoft, «Creación de una cuenta de Storage,» 02 05 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/storage/common/storage-account-create?tabs=azure-portal.

[32] Microsoft, «Tutorial: Creación de un recurso compartido de archivos NFS de Azure y montaje del mismo en una máquina virtual Linux mediante Azure Portal,» 12 04 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/storage/files/storage-files-quick-create-use-linux.

[33] Microsoft, «Inicio rápido: Uso de Azure Portal para crear un servidor flexible de Azure Database for MySQL,» 18 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/mysql/flexible-server/quickstart-create-server-portal.

[34] Microsoft, «Tutorial: Configuración de una puerta de enlace de aplicaciones con terminación TLS mediante Azure Portal,» 11 Mayo 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/application-gateway/create-ssl-portal.

[35] Microsoft, «Generación de un certificado autofirmado de Azure Application Gateway con una entidad de certificación raíz personalizada,» 28 Abril 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/application-gateway/self-signed-certificates.

[36] Microsoft, «Tutorial: Creación y administración de una instancia de VPN Gateway mediante Azure Portal,» 23 07 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/vpn-gateway/tutorial-create-gateway-portal.

[37] OWASP, «OWASP ModSecurity Core Rule Set,» 2023. [En línea]. Available: https://owasp.org/www-project-modsecurity-core-rule-set/.

[38] iThemes, «iThemes Security Pro,» [En línea]. Available: https://ithemes.com/security/.

[39] iThemes, «Site scan,» 2023. [En línea]. Available: https://ithemes.com/security/site-scan/.

[40] Patchstack, «Detect & manage vulnerabilities in your WordPress sites,» 2023. [En línea]. Available: https://patchstack.com/.

[41] Microsoft, «Uso de Microsoft Sentinel con Azure Web Application Firewall,» 25 06 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/web-application-

firewall/waf-sentinel.

[42] ZAP Dev Team, «ZAP Getting Started,» 2023. [En línea]. Available: https://www.zaproxy.org/getting-started/.

[43] Zap Dev Team, «OWASP ZAP Modes,» 2023. [En línea]. Available: https://www.zaproxy.org/docs/desktop/start/features/modes/.

[44] N. Borghs, «Implement security headers on Azure Application Gateway,» 11 06 2023. [En línea]. Available: https://neelborghs.com/implement-security-headers-on-azure-application-gateway.

[45] Mozilla, «X-XSS-Protection,» 24 07 2023. [En línea]. Available: https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-XSS-Protection.

[46] Mozilla, «HTTP,» 24 07 2023. [En línea]. Available: https://developer.mozilla.org/es/docs/Web/HTTP.

[47] iThemes, «iThemes Security Password Requirements,» 2023. [En línea]. Available: https://help.ithemes.com/hc/en-us/articles/202487714-Solid-Security-Password-Requirements.

[48] M. Toroman y T. Janetscheck, Mastering Azure Security: Keeping your Microsoft Azure workloads safe, 2nd Edition.

[49] «WPSchoolPress,» [En línea]. Available: https://wpschoolpress.com/.

[50] ayudaley, «Guía del RGPD,» [En línea]. Available: https://ayudaleyprotecciondatos.es/guia-rgpd/.

[51] EducaMadrid, «Modelos de protección de datos,» [En línea]. Available: https://dpd.educa2.madrid.org/modelos.

[52] Junta de Andalucía, Consejeria de Educación, «Consentimiento informado,» [En línea]. Available: https://www.juntadeandalucia.es/educacion/portals/delegate/content/f2e0dd09-e0bd-4a95-8a10-ebfef76e9ad3.

[53] Junta de Andalucía, Consejeria de Educación, «Guía de protección de datos de carácter personal para los centros de enseñanza,» [En línea]. Available: https://www.juntadeandalucia.es/educacion/portals/delegate/content/3fecd70c-8fa1-469d-8fb4-d09523f83882/Gu%C3%ADa%20LOPD%20Centros%20Educativos.

[54] Agencia Española de Protección de Datos, «Guía para clientes que contraten servicios de cloud computing,» [En línea]. Available: https://www.aepd.es/es/documento/guia-cloud-clientes.pdf.

[55] National Institute of Standards and Technology, «NIST Cybersecurity Framework,» 20 Septiembre 2022. [En línea]. Available:

https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework.

[56] Cloud Security Alliance, «Cloud Controls Matrix,» 2021. [En línea]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix/.

[57] Cloud Security Alliance, «Top Threats to Cloud Computing,» 2022. [En línea]. Available: https://s3.amazonaws.com/content-production.cloudsecurityalliance/zyaqubn85bt9mfnh5uv6f2n3x6mj?response-content-disposition=inline%3B%20filename%3D%22TopThreatstoCloudComputingPandemicEleven060622.pdf%22%3B%20filename%2A%3DUTF-8%27%27TopThreatstoCloudComp.

[58] Cloud Security Alliance, «Security Guidance,» 2021. [En línea]. Available: https://s3.amazonaws.com/content-production.cloudsecurityalliance/8zux7a24u92d7w49zn0c7cr4txi8?response-content-disposition=inline%3B%20filename%3D%22Security-Guidance-v4.0-9-20-21.pdf%22%3B%20filename%2A%3DUTF-8%27%27Security-Guidance-v4.0-9-20-21.pdf&re.

[59] Microsoft, «Productos de Azure,» [En línea]. Available: https://azure.microsoft.com/es-es/products/.

[60] R. Funchal, «Wordpress Security Checklist,» [En línea]. Available: https://wpsecuritychecklist.org/.

[61] Microsoft, «¿Qué es Azure Bastion?,» 18 05 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/bastion/bastion-overview.

[62] Microsoft, «Información general de App Service,» 18 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/app-service/overview.

[63] Microsoft, «Introducción a Azure Blob Storage,» 29 03 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/storage/blobs/storage-blobs-introduction.

[64] Microsoft, «Generación y exportación de certificados para conexiones de punto a sitio con PowerShell,» 04 08 2023. [En línea]. Available: https://learn.microsoft.com/es-es/azure/vpn-gateway/vpn-gateway-certificates-point-to-site.

Apéndice I: Material complementario

Archivo	Descripción
cloud-init.yml	Contiene un script utilizado para realizar las configuraciones iniciales en las máquinas virtuales.
ZAP-Reporte-1	Contiene el reporte de ZAP con las vulnerabilidades encontradas.
ZAP-Reporte-2	Contiene el reporte de ZAP tras la subsanación de errores.