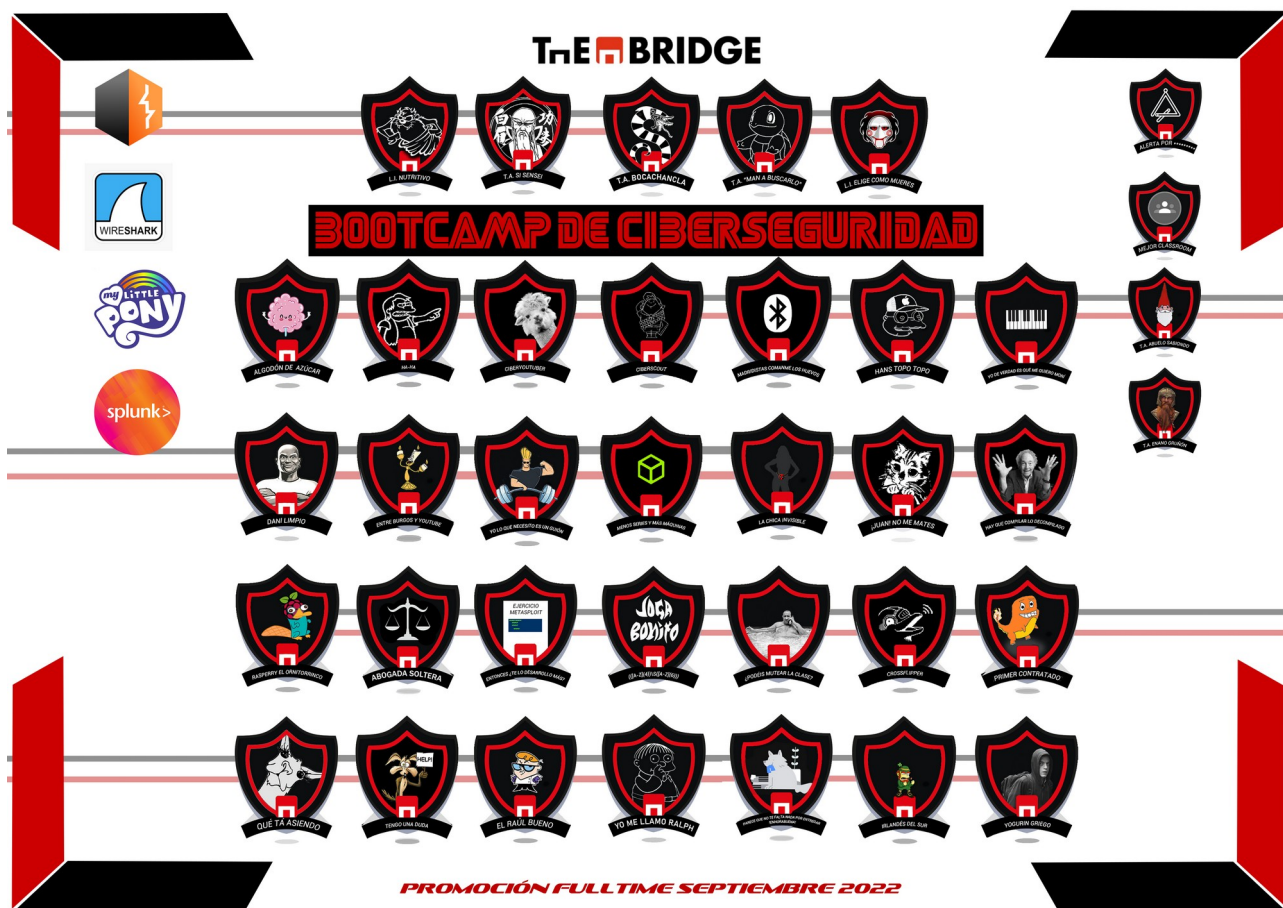


ASEGURANDO LA APLICACIÓN PARA ASISTENCIA A VÍCTIMAS DE VIOLENCIA DE GENERO POR LA CRUZ ROJA ESPAÑOLA

BOOTCAMP DE CIBERSEGURIDAD

PROMOCIÓN SEPTIEMBRE 2022



Raúl Sobrino
Lucía Contreras
Marcos Aceto
Eduardo Martínez
Natalia del Real
Miguel Pascual
Raul Muñoz

1. Política de contraseñas, cookies

En el desarrollo de una aplicación Web, uno de los principales puntos a tener en cuenta es la política de privacidad de los datos que se van a manejar en esa aplicación. Tratándose además, de un tema tan controvertido y personal como es el de la existencia de una situación de maltrato, hemos considerado conveniente dotar de la importancia que merece a este apartado del proyecto.

1.1. Política de privacidad

1ª Capa

CRUZ ROJA ESPAÑOLA tratará sus datos personales para dar respuesta a las solicitudes planteadas a través de este chatbot. Los datos que se recopilen serán tratados con las máximas garantías que prevé la legislación. Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, en la dirección de correo electrónico dpo@cruzroja.es.

Le recomendamos que lea la [política de privacidad](#) antes de proporcionarnos sus datos personales dpo@cruzroja.es.

He leído y acepto las condiciones de la política de privacidad ☐

2ª Capa

POLÍTICA DE PRIVACIDAD

¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE SUS DATOS?

¿CON QUÉ FINALIDAD TRATAMOS SUS DATOS PERSONALES?

¿CUÁL ES LA LEGITIMACIÓN PARA EL TRATAMIENTO DE SUS DATOS?

¿COMPARTIREMOS SUS DATOS CON TERCEROS?

¿QUÉ MEDIDAS DE SEGURIDAD APLICAMOS A LOS DATOS PERSONALES?

¿QUÉ CANALES UTILIZAMOS PARA OBTENER TUS DATOS?

¿QUÉ CATEGORÍAS DE DATOS TRATAMOS?

¿CUÁLES SON TUS DERECHOS?

¿QUÉ PUEDO HACER SI NO QUIERO RECIBIR COMUNICACIONES COMERCIALES?

¿Y QUÉ PASA SI SOY MENOR?

Estas normas rigen para todas las páginas que alberga CRUZ ROJA ESPAÑOLA (en adelante CRE). Para saber cómo se procede con los datos personales, te rogamos leas la siguiente política de privacidad que aconsejamos consultar con regularidad, dado que puede ser actualizada. El visitante se hace responsable y garantiza que los datos personales que facilita a CRE son veraces y cuenta, cuando proceda, con la debida autorización para ello del titular de los mismos.

CRE tratará los datos de carácter personal vinculados a sus espacios webs respetando las exigencias de la legislación vigente, resaltando:

POLÍTICA DE PRIVACIDAD

¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE SUS DATOS?

- **RESPONSABLE DEL TRATAMIENTO** de sus datos es CRUZ ROJA ESPAÑOLA
- **CIF:** Q2866001G
- **Dirección Postal:** C/ Av. Reina Victoria 26-28, 28003 Madrid

El Delegado de Protección de Datos de CRE es la persona encargada de atenderte en cualquier cuestión que pueda plantearse respecto de la protección de tus datos personales y de asegurar el cumplimiento de la legislación en materia de protección de datos. Puedes contactar con él en la siguiente dirección de correo electrónico: dpo@cruzroja.es.

¿CON QUÉ FINALIDAD TRATAMOS SUS DATOS PERSONALES?

Los datos que CRUZ ROJA ESPAÑOLA, recaba por las diferentes vías (página web, correo electrónico, formularios electrónicos o formularios y documentos en papel) dentro de su actividad, son tratados con las siguientes finalidades:

- » Gestionar y tramitar cualquier tipo de solicitud de información, incluidas aquellas dirigidas a hacerse socio, voluntario o donante.
- » Gestión de cursos de formación.
- » Gestionar la asistencia social y prestación de ayudas a personas que lo necesiten, así como a colectivos vulnerables.

»Gestionar y controlar tu colaboración como socio, así como las actividades de voluntariado y de personas físicas y jurídicas que colaboran con nuestra Institución.

»Mantener informados a nuestros socios, voluntarios, alumnos e interesados en colaborar, de las actividades y acciones que llevamos a cabo.

»Controlar y gestionar las aplicaciones y herramientas desarrolladas por CRE, las cuales son necesarias para el desarrollo y gestión de las actividades sociales llevadas a cabo por nuestra Institución.

»Divulgación de nuestras actividades y acciones solidarias. Enviar comunicaciones por cualquier vía (sms, teléfono, e-mail, correo postal) relacionadas con las actividades y acciones sociales que realizamos.

»Llevar a cabo la búsqueda de personas y el restablecimiento de contacto entre familiares.

»Gestionar las suscripciones a nuestras revistas y publicaciones.

»Prestar servicios sanitarios y socio sanitarios.

»Realización de análisis estadísticos y gestión de registro histórico.

»Procesos de selección de personal para un puesto de trabajo.

»Gestión y tramitación de las consultas recibidas a través del chatbot.

¿CUÁL ES LA LEGITIMACIÓN PARA EL TRATAMIENTO DE SUS DATOS?

La base legal que nos permite tratar sus datos personales también depende de la finalidad para la que los tratemos, de este modo encontraremos distintas bases legales en virtud de las siguientes finalidades:

»Tu consentimiento o bien hayan sido suministrados voluntariamente por ti por cualquier medio. En este sentido, la inclusión de datos personales en ficheros es absolutamente voluntaria y su recogida está debidamente anunciada.

»El mantenimiento, desarrollo y ejecución de una relación contractual que mantengamos contigo, en el caso de: (i) prestación de servicios; (ii) relación laboral, mercantil, administrativo, entre otros.

»La gestión, coordinación y control de nuestros: (i) voluntarios, (ii) socios; (iii) Donantes (iv) y de todas las personas que mantienen una relación directa o indirecta con CRE a través de nuestros proyectos solidarios.

»El desarrollo, gestión y ejecución de las acciones solidarias y de ayuda a los colectivos más desfavorecidos que llevamos a cabo.

»Prestaciones sanitarias y sociales.

»Por interés legítimo de CRE, respetando siempre tu derecho a la protección de datos personales, al honor y a la intimidad, para el desarrollo y difusión de nuestras actividades humanitarias y sociales.

¿COMPARTIREMOS SUS DATOS CON TERCEROS?

Tus datos serán conservados bajo estrictas medidas de seguridad que garanticen la confidencialidad y la seguridad de los mismos. Del mismo modo, sólo serán cedidos a las entidades y para las finalidades siguientes:

1. Entidades y proveedores que prestan servicios a CRE para la correcta ejecución de nuestras actividades y proyectos. Dichas entidades y proveedores se encuentran debidamente acreditados y firman con nosotros el correspondiente contrato de tratamiento de datos en cumplimiento de la normativa de protección de datos vigente. Por ponerte ejemplos de los servicios que nos prestan y que pueden implicar el tratamiento de tus datos personales por cuenta de CRE, podemos citarte, a título enunciativo y no limitativo: servicios profesionales multidisciplinares, logística, asesoramiento jurídico, servicios tecnológicos, informáticos, mensajería y reparto, mantenimiento, seguridad y vigilancia, publicidad y marketing, call center etc...
2. Entidades públicas y privadas que colaboran con nosotros, para el control y seguimiento de los proyectos para los que nos otorgan su financiación.
3. Administraciones y organismos públicos correspondientes para cumplimiento de las normativas vigentes o por imperativo legal, así como a las Fuerzas y Cuerpos de Seguridad del Estado, Policía Local o Autonómica en los casos de asistencia a víctimas de violencia de género.
4. A los servicios de emergencia, servicios sociales, sanitarios o asistenciales, con la finalidad de atender correctamente a los usuarios.

Sólo en los casos en que la cesión de los datos venga impuesta por ley o fuera necesaria para hacer frente a una situación de emergencia que exija la cooperación de personas o entidades distintas de las mencionadas anteriormente,

tus datos podrán ser cedidos a terceros en la medida en que resulte necesaria para cumplir la legislación vigente o para hacer frente a la situación de emergencia planteada.

Asimismo, en el ámbito de las relaciones internacionales y en cuanto a transferencias internacionales de datos:

»Intercambio de información entre las Oficinas de CRUZ ROJA INTERNACIONAL y MEDIA LUNA INTERNACIONAL, únicamente cuando es necesario para los proyectos de Cooperación y Ayuda Internacional a los que te hayas inscrito.

¿QUÉ MEDIDAS DE SEGURIDAD APLICAMOS A LOS DATOS PERSONALES?

Aplicamos las medidas de seguridad necesarias para evitar el robo, alteración o acceso no autorizado a los datos, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

- En el caso de contratación de servicios, exigimos y velamos porque el encargado del tratamiento aplique medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos existentes, conforme se recoge en el art. 32 del Reglamento General de Protección de Datos.
- También realizamos Evaluaciones de Impacto sobre aquellas operaciones de tratamiento que consideramos puedan tener un riesgo para los derechos y libertades de las personas, con el objeto de implantar las medidas necesarias y oportunas para evitar una violación de la confidencialidad.

¿QUÉ CANALES UTILIZAMOS PARA OBTENER TUS DATOS?

Cruz Roja Española obtiene los datos de carácter personal a través de los siguientes canales:

»Correo electrónico.

»Formularios y cuestionarios a través de nuestras páginas Web. El tipo y la cantidad de información que CRE recibe y conserva depende de la forma en la utilices los espacios web de CRE. Puedes acceder a casi todas las páginas sin señalar quién eres y sin comunicarnos dato personal alguno.

»Campañas telefónicas. Las llamadas que realizamos en el marco de nuestras campañas son grabadas para mejorar la calidad del servicio.

»Formularios en papel (contactos persona a persona y puerta a puerta por personal de CRE, voluntarios o colaboradores).

»El chatbot incluido en nuestra página web para la recepción de consultas.

»Personalmente, a través de los puntos y oficinas y centros repartidos por todo el territorio nacional.

»Directamente de los interesados.

»A través de acuerdos de colaboración con organismos e instituciones.

¿QUÉ CATEGORÍAS DE DATOS TRATAMOS?

Tratamos las siguientes categorías de datos, según las circunstancias de tu relación con nosotros:

»Datos de identificación, incluida la imagen.

»Dirección postal y direcciones electrónicas.

»Números de teléfonos

»Datos de características generales.

»Datos económicos.

»Circunstancias sociales.

»Académicos y profesionales.

»Datos especialmente protegidos (Arts. 9 y 10 del Reglamento General de Protección de Datos (Reglamento UE 2016/679)).

¿CUÁLES SON TUS DERECHOS?

Toda persona tiene derecho a conocer si CRE realiza tratamientos de sus datos personales. También tienes derecho a:

»Acceder a tus datos personales,

»Solicitar la rectificación de los datos inexactos.

«Solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos,

»Oponerte al tratamiento de tus datos, por motivos relacionados con tu situación particular, solicitando que no sean tratados por CRE.

«En determinadas circunstancias, podrás solicitar la limitación del tratamiento de tus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

»Retirar, siempre que quieras, el consentimiento prestado, sin que ello afecte a la licitud del tratamiento que hayamos realizado con anterioridad a dicha retirada.

»Cuando ejercites tus derechos de supresión, oposición, limitación o nos retires tu consentimiento, CRE dejará de tratar tus datos, salvo por motivos legítimos imperiosos o el ejercicio o la defensa de posibles reclamaciones.

»Todos estos derechos podrás ejercitarlos, dirigiéndote a nosotros en las siguientes direcciones: Cruz Roja Española, Av. Reina Victoria 26-28, 28003 de Madrid (Att. Delegado de Protección de Datos) o, si lo prefieres, a través de correo electrónico a la siguiente dirección: dpo@cruzroja.es.

»Recuerda siempre que ejercites alguno de los derechos que te hemos expuesto, acompañar a tu solicitud una copia de tu DNI o documento equivalente que nos permita comprobar tu identidad.

»Asimismo, si no estás conforme con cómo hemos atendido tus derechos, podrás presentar una reclamación ante la Agencia Española de Protección de Datos, a través de la página Web www.aepd.es.

¿QUÉ PUEDO HACER SI NO QUIERO RECIBIR COMUNICACIONES COMERCIALES?

De conformidad con la Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI) podrás darte de baja de cualquiera de nuestros servicios de suscripción, así como manifestar tu oposición a recibir informaciones publicitarias, enviando la palabra BAJA a las siguientes direcciones: Cruz Roja Española, att/ DPO, Av. Reina Victoria 26-28, 28003 de Madrid, o si lo prefieres, a través de correo electrónico a la siguiente dirección: dpo@cruzroja.es.

¿Y QUÉ PASA SI SOY MENOR?

Si tienes menos de 14 años y deseas ser socio o participar en nuestras redes sociales, tus padres o tu tutor legal tienen que darnos su permiso para darte de alta como usuario, por lo que tienes que pedirles que rellenen con sus datos personales y firmen los formularios correspondientes, contenidos en los sitios Webs de la Institución. Una vez firmados, puedes enviarnoslos a las siguientes direcciones: Cruz Roja Española, att/ DPO, Avenida Reina Victoria, 26-28, 28003 Madrid, o a la dirección de correo electrónico dpo@cruzroja.es, adjuntando al correo electrónico el documento que contiene el formulario firmado por tus padres o tutor legal.

Igualmente, si algún registro revelase que eres menor de edad, CRE, por medio de correo electrónico, notificará a tus padres o tutor legal el contenido de la información recibida y recabará su consentimiento para la recogida y tratamiento de tus datos personales. En cualquier momento, tus padres o el tutor legal podrán revisar, cancelar o denegar la recogida de tus datos personales, dirigiéndote a Cruz Roja Española en las direcciones anteriormente reseñadas.

Procedimiento de generación de copias de respaldo y recuperación de la información

1. OBJETO

1. El objeto del presente documento es la definición del Procedimiento aplicable a la Generación de Copias de Respaldo y Recuperación de la Información manejada por CRUZ ROJA ESPAÑOLA.

Se implantará el presente Procedimiento atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de CRUZ ROJA ESPAÑOLA, que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. ÁMBITO DE APLICACIÓN

1. Este Procedimiento es de aplicación a todo el ámbito de actuación de CRUZ ROJA ESPAÑOLA, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de CRUZ ROJA ESPAÑOLA..
2. El presente Procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios de CRUZ ROJA ESPAÑOLA, especialmente, los responsables de los Servicios de Explotación de los Sistemas de Información de CRUZ ROJA ESPAÑOLA y los propios usuarios, como actores ambos, en sus respectivas competencias, de la generación de copias de respaldo y su ulterior recuperación, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información de CRUZ ROJA ESPAÑOLA..
3. En el ámbito del presente Procedimiento, se entiende por usuario cualquier empleado público perteneciente o ajeno a CRUZ ROJA ESPAÑOLA, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con CRUZ ROJA ESPAÑOLA y que utilice o posea acceso a los Sistemas de Información del <<ORGANISMO>>.

3. VIGENCIA

1. El presente Procedimiento ha sido aprobado por el departamento de informática de CRUZ ROJA ESPAÑOLA, contribuyendo al establecimiento de las directrices generales para el uso adecuado de los recursos de tratamiento de información que CRUZ ROJA ESPAÑOLA pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, cuando proceda, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.
2. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de CRUZ ROJA ESPAÑOLA.
3. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este Procedimiento.

4. REVISIÓN Y EVALUACIÓN

1. La gestión de este Procedimiento corresponde al departamento de tecnología, que es competente para:
 - Interpretar las dudas que puedan surgir en su aplicación.
 - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
 - Verificar su efectividad y grado de cumplimiento.
2. Anualmente (o siempre que existan circunstancias que así lo aconsejen), el departamento de tecnología revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación del departamento de tecnología de CRUZ ROJA ESPAÑOLA.
3. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.
4. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

1. Las referencias tenidas en cuenta para la redacción de este Procedimiento han sido:
 - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
 - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
 - REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
 - Documentos y Guías CCN-STIC.

6. ROLES Y RESPONSABILIDADES

1. Las responsabilidades personales derivadas de las actividades descritas en el presente Procedimiento son las siguientes:

Roles	Responsabilidades
Personal del área de Explotación del Departamento de Sistemas de CRUZ ROJA ESPAÑOLA	Gestionar las copias de respaldo de los activos recogidos en el alcance del Procedimiento, siguiendo las directrices señaladas.
Responsable del área de Explotación del Departamento de Sistemas de CRUZ ROJA ESPAÑOLA	<ul style="list-style-type: none">·Custodiar los soportes de almacenamiento extraíbles donde se almacenan las copias de respaldo de CRUZ ROJA ESPAÑOLA.·Garantizar la correcta ejecución de las operaciones periódicas de copia de respaldo.

CRUZ ROJA ESPAÑOLA	<ul style="list-style-type: none">· Ejecutar las comprobaciones periódicas de los procedimientos de restauración de CRUZ ROJA ESPAÑOLA.
Responsables de los Activos	<ul style="list-style-type: none">·Tramitar las solicitudes de inclusión de activos en la(s) copia(s) de respaldo.·Tramitar las solicitudes de recuperación de activos alterados, dañados o destruidos desde la realización de la(s) copia(s) de respaldo.·Validar las operaciones de restauración de activos gestionadas por el personal del área de Explotación del Departamento de Sistemas de CRUZ ROJA ESPAÑOLA.

El responsable del área de informática	·Aprobar las solicitudes de inclusión de activos en la(s) copia(s) de respaldo solicitadas por los Responsables de los Activos. ·Aprobar las solicitudes de recuperación de activos a partir de copias de respaldo, solicitadas por los Responsables de los Activos.
--	---

7. CUESTIONES GENERALES

Las Copias de Respaldo

1. Toda la información de CRUZ ROJA ESPAÑOLA del ámbito de aplicación del ENS será periódicamente respaldada en soportes de backup.
2. Las copias de respaldo deben abarcar toda la información necesaria para recuperar el servicio en caso de corrupción o pérdida de la información. Tal información puede incluir datos, programas, ficheros de configuración e, incluso, la imagen del sistema operativo.
3. Para todos los sistemas relevantes se definirán los estándares de respaldo, que incluirán, al menos, la siguiente información:
 - Periodicidad de las copias de respaldo.
 - Periodos de retención de las copias.
 - Ubicación de los soportes de respaldo.
 - Procedimientos de recuperación de la información.
 - Procedimientos de restauración y verificación de la integridad de la información respaldada.
 - Procedimientos de inventario y gestión de soportes.

Tipos de Copias de Respaldo

Completa	Se efectúa una copia de seguridad completa de todos los ficheros y bases de datos. Puede consumir bastante tiempo si el volumen de datos a salvaguardar es elevado. La ventaja derivada de este tipo de copia es que se tiene la seguridad de tener una imagen completa de los datos en el momento de la salvaguarda.
Incremental	Se copian los datos modificados desde la anterior copia incremental. Siempre se debe partir de una salvaguarda completa inicial. Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar. Por el contrario, la restauración es lenta, toda vez que requiere restaurar una copia completa y todas las copias incrementales realizadas hasta el momento al que se quiera restaurar el sistema.
Diferencial	Se copian los datos modificados desde la última copia completa. Se ejecutará con mayor o menor rapidez en función de la frecuencia con que se realice. La restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.

Ordenadores Portátiles

1. Todos los usuarios de ordenadores portátiles deberán realizar copias de respaldo de sus datos con la regularidad que se especifique.
2. Para la realización de estas copias de respaldo deberá utilizarse la herramienta que, a tal propósito, se defina a nivel corporativo.

Cifrado de soportes almacenados externamente

3. Toda la información de copias de respaldo que CRUZ ROJA ESPAÑOLA almacene fuera de sus locales debe estar cifrada, según los procedimientos definidos a tal efecto.

4. El procedimiento de envío y recepción de soportes permitirá asegurar que éstos no son extraviados ni han sido manipulados durante su transporte.

Copia de respaldo de información de usuarios

5. Los usuarios son responsables de la realización de copias de respaldo con la frecuencia definida y siempre que haya cambios significativos en la información que manejan, para lo que utilizarán las carpetas de red que a tal efecto les sean habilitadas.
6. En ningún caso se deberán almacenar copias de respaldo en el domicilio del usuario o en dependencias de terceros ajenas a CRUZ ROJA ESPAÑOLA si no existe un acuerdo previamente suscrito con el tercero en el que se prevea tal posibilidad y se explicitan las cautelas debidas respecto de la custodia de la información almacenada.
7. Los responsables de las unidades administrativas de CRUZ ROJA ESPAÑOLA deberán asegurarse de que la información de los empleados a su cargo se salvaguarda de forma satisfactoria.

Retención de información

8. Los documentos originales y los ficheros en formato electrónico deben ser retenidos durante el tiempo que en cada caso el ordenamiento jurídico prescriba.
9. Además de lo anterior, hay que tener en cuenta que puede haber requerimientos para retener datos, tales como “logs para auditorías”, de cara a la realización de acciones administrativas, disciplinarias, civiles o penales, por lo que habrán de definirse los procedimientos pertinentes para custodiar este tipo de información. Además, se implementarán los medios necesarios para poder revisar las actividades de los usuarios que manejan este tipo de información.
10. El Departamento de Asesoría Jurídica de CRUZ ROJA ESPAÑOLA, con la colaboración del resto de Departamentos involucrados de CRUZ ROJA ESPAÑOLA, especialmente los Responsables de la Información, los Servicios y de Seguridad, se encargará de definir los periodos de retención de la información en función de la naturaleza de la misma y del ordenamiento jurídico vigente en cada momento.
11. Cuando la información de CRUZ ROJA ESPAÑOLA deje de ser necesaria, deberá ser destruida o eliminada de manera segura. Para dar soporte a

este requisito, los responsables de las unidades administrativas de CRUZ ROJA ESPAÑOLA deberán revisar, de forma periódica, el valor y la utilidad de la información almacenada.

12. Todos los datos almacenados en soportes de información que se desechen serán eliminados según un procedimiento definido a tal efecto, que asegure los objetivos de seguridad para la información de los citados soportes. En este sentido, se deberá tener especial cuidado con respecto a la información almacenada en servidores o estaciones de trabajo, el software licenciado o desarrollado a medida y los elementos que recibirán mantenimiento dentro de CRUZ ROJA ESPAÑOLA por usuarios que no tengan permiso permanente de acceso a los mismos.

Identificación de información crítica

1. Los responsables de las unidades administrativas de CRUZ ROJA ESPAÑOLA serán los encargados de identificar y mantener una relación actualizada de aquella información que sus departamentos necesitan para recuperar la operativa de sus procesos, durante eventuales operaciones de restauración. Se deberá adoptar especial cuidado con aquella información que proporcione evidencia de la existencia de un hecho, responsabilidad u obligación contractual.

Prueba de Soporte Informático

1. La información del ámbito de aplicación del ENS, almacenada en un medio informático durante un período prolongado de tiempo, deberá ser verificada al menos una vez al año, para asegurar que la información es recuperable.

Periodicidad de las copias de respaldo

1. La realización de copias de respaldo de forma periódica permitirá a CRUZ ROJA ESPAÑOLA disponer de su información en caso de destrucción de los equipos o errores producidos en los datos y/o aplicaciones.
2. Las copias de respaldo de software, ficheros de datos y bases de datos se deberán realizar regularmente. La frecuencia con la que se deben realizar los back-ups se definirá en función de la sensibilidad de las aplicaciones o datos y de su impacto en el adecuado desarrollo de las competencias

atribuidas a CRUZ ROJA ESPAÑOLA. Por ello, tal periodicidad deberá determinarse sobre la base de las consecuencias que la pérdida de la información tendría para CRUZ ROJA ESPAÑOLA. En nuestro caso las copias de seguridad se realizan semanalmente antes del viernes a las 14:00.

3. Respecto de los ficheros que contengan datos de carácter personal, habrá de tenerse en cuenta lo siguiente:

- Se deben crear procedimientos para la realización de, al menos, una copia de respaldo semanal, si en tal periodo se hubiere producido alteración o modificación de los datos.
- Cuando las pruebas anteriores a la implantación o modificación de los sistemas de información, traten ficheros con datos reales de carácter personal, se deberá realizar previamente una copia de seguridad de los datos.

Almacenamiento de las Copias de Respaldo en dependencias externas

1. Suele ser frecuente el almacenamiento de la última copia de seguridad en una ubicación externa, lo que minimiza el riesgo de pérdida de datos en caso de producirse una contingencia.
2. Deberán adoptarse las siguientes cautelas, especialmente cuando se traten ficheros que contengan datos de carácter personal o con información sensible.
 - La última copia de seguridad, junto con los procedimientos de recuperación, deberá ubicarse en edificios distintos de las ubicaciones de los CPD's. A ser posible, en un centro externo.
 - Deberá existir un registro con el contenido de las copias de respaldo, lo que facilitará un control efectivo en su gestión.
 - Deberá llevarse un registro de las copias de respaldo ubicadas, tanto en las dependencias de CRUZ ROJA ESPAÑOLA, como en las sedes de almacenamiento alternativas.

Protección de las Copias de Respaldo

1. La adecuada protección de las copias de respaldo permitirá tanto su correcta conservación, como un control de acceso efectivo a los datos almacenados.

2. La protección de las copias de respaldo alcanzará tanto a archivos de información como a librerías de aplicaciones. El almacenamiento de los soportes se hará efectivo ubicando las copias en armarios ignífugos, bajo llave y restringiendo el acceso a personal previamente autorizado.

Automatización del sistema de Backup

1. La automatización de los procedimientos de backup reducirán la posibilidad de omitir ciclos de respaldo o que éstos sean erróneos.
2. La programación periódica de las copias de respaldo se debe efectuar a través de un sistema de administración de soportes.

Descripción del contenido de las Copias de Respaldo

1. La documentación del contenido de las copias de seguridad facilitará su identificación.
2. En las correspondientes etiquetas se deberá identificar la fecha a que corresponde. En el inventario de copias de respaldo se detallará los archivos de los cuales se hace backup.

Control de entrada y salida de las Copias de Respaldo

1. La existencia de un registro que controle las entradas y salidas de copias de respaldo proporciona fiabilidad al inventario de copias de seguridad.
2. Debe quedar registrado el flujo de entradas y salidas de los soportes fuera de las instalaciones de CRUZ ROJA ESPAÑOLA, dejando constancia del solicitante de cada petición y de los motivos.
3. En cuanto a los ficheros que contengan datos de carácter personal (o especialmente sensibles), se deberá tener en cuenta que las copias de seguridad que contengan datos de carácter personal sólo deberán salir con autorización del Responsable del Fichero y llevándose a cabo bajo su última responsabilidad.

Transporte de las Copias de Respaldo

1. El transporte de las copias de respaldo deberá contar con las adecuadas medidas de seguridad que garanticen la no alteración, robo o destrucción de los datos durante su transporte.

2. El transporte de las copias de respaldo con información sensible se deberá realizar utilizando maletas provistas de mecanismos de apertura operados bajo llave y/o mecanismos de cifrado, y cuyas llaves o claves se encontrarán bajo custodia. La responsabilidad de la destrucción o pérdida de información durante el transporte o almacenamiento recaerá sobre el personal / unidad administrativa / personas jurídicas responsables de su gestión.

Pruebas de realización y restauración de las Copias de Respaldo

1. La realización de las pruebas de restauración de las copias de respaldo confirmará el funcionamiento correcto del proceso de recuperación de copias de datos, y garantizará la integridad de los datos que contienen.
2. Se establecerán pruebas respecto a la restauración de las copias de respaldo, de forma rotativa y con una periodicidad previamente establecida.
3. Las pruebas y los resultados deberán estar convenientemente documentados y, como consecuencia de las mismas, se subsanarán las incidencias que se hayan puesto de manifiesto durante su desarrollo.
4. Además, cuando se traten ficheros que contengan datos de carácter personal, el Responsable del Fichero deberá verificar semestralmente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación.

Periodo de existencia de las Copias de Respaldo y su eventual destrucción

1. El establecimiento de un período de existencia de las copias de respaldo, de acuerdo con el ordenamiento jurídico vigente en cada momento y lo dispuesto en la Política de Seguridad de CRUZ ROJA ESPAÑOLA, facilitará la salvaguarda de las mismas, el cumplimiento legal y el uso eficiente del espacio físico disponible para el almacenamiento.
2. Se deberá establecer el período de existencia para las copias de seguridad y los procedimientos a seguir para proceder a su destrucción definitiva una vez concluido tal período.

8. HERRAMIENTAS PARA LA GENERACIÓN DE COPIAS DE RESPALDO

1. El Departamento de Sistemas de CRUZ ROJA ESPAÑOLA contará con un conjunto de herramientas para la generación de copias de respaldo, que le permitirá realizar copias de seguridad de los activos y sistemas de información de CRUZ ROJA ESPAÑOLA sujetos al ámbito de aplicación del ENS.
2. Estas herramientas de copia se detallan en el registro de herramientas para la generación de copias de respaldo del que se presenta un modelo en el epígrafe 12 del presente Procedimiento.

9. GENERACIÓN DE COPIAS DE RESPALDO

9.1 INCLUSIÓN DE ACTIVOS EN LA COPIA DE RESPALDO

1. La operación de inclusión de activos en la copia de respaldo se iniciará a petición del Responsable del Activo y deberá ser previamente aprobada por el departamento de tecnología competente.
2. Para solicitar la inclusión, el Responsable del Activo abrirá una incidencia en el <<gestor de incidencias>> de CRUZ ROJA ESPAÑOLA, a la que adjuntará la Solicitud de Inclusión de activos en la Copia de Respaldo. Un modelo de este documento se muestra en el epígrafe 13 del presente Procedimiento.
3. El departamento de tecnología competente:
 - Aprobará la petición, y asignará la incidencia al responsable del área de explotación del Departamento de Sistemas de CRUZ ROJA ESPAÑOLA, o
 - Rechazará la petición, cerrando la incidencia y detallando los motivos que provocan tal rechazo.

9.2 PROCEDIMIENTO DE GENERACIÓN DE COPIAS DE RESPALDO

1. La generación de copias de respaldo de los activos de CRUZ ROJA ESPAÑOLA del ámbito de aplicación del ENS se soporta en los procedimientos y

herramientas de copia del Departamento de Sistemas de CRUZ ROJA ESPAÑOLA.

2. Las operaciones de copia de respaldo de los activos de CRUZ ROJA ESPAÑOLA recogidos dentro del alcance del ENS se gestionan de forma programada en fechas y horas concretas, a través de las herramientas de copia del Departamento de Sistemas de CRUZ ROJA ESPAÑOLA.
3. El Departamento de Sistemas de CRUZ ROJA ESPAÑOLA mantendrá un inventario de los activos sobre los que se realiza copia de seguridad en el Registro de Activos sujetos a Copia de Respaldo. Un modelo de este registro se presenta en el epígrafe 12 del presente Procedimiento.

9.3 PROCEDIMIENTO DE VERIFICACIÓN DE COPIAS DE RESPALDO

1. La herramienta de generación de copias de respaldo de CRUZ ROJA ESPAÑOLA contará con un sistema automático de verificación de copias. Este sistema, que se mantendrá permanentemente activado, verificará las copias de respaldo una vez generadas y almacenará el resultado de la operación en el registro del sistema.
2. El Departamento de Sistemas de CRUZ ROJA ESPAÑOLA comprobará diariamente el registro del sistema, al objeto de garantizar la correcta ejecución de las operaciones de copia de respaldo.
3. En caso de detectar un fallo en el proceso de generación, el Departamento de Sistemas de CRUZ ROJA ESPAÑOLA investigará y resolverá la incidencia y relanzará la tarea de copia.

9.4 GESTIÓN DE SOPORTES

1. Las herramientas de gestión de copias de respaldo de CRUZ ROJA ESPAÑOLA contarán con una librería de soportes que permita la inserción de múltiples volúmenes para facilitar la gestión automatizada de las operaciones.
2. Estos soportes se insertarán antes de una operación de copia y se retirarán para su almacenamiento, tras la verificación de la misma.

3. Los soportes de copia se obtendrán situado en [Avenida Reina Victoria, 26-28](#) de las instalaciones del CRUZ ROJA ESPAÑOLA, y se almacenan en discos duros como dispositivo de custodia.
4. La CRUZ ROJA ESPAÑOLA mantendrá un inventario de los soportes empleados en las operaciones de generación de copias de respaldo en el Registro de Soportes Extraíbles. Se presenta un modelo de este Registro en el epígrafe 12 del presente Procedimiento.

10. RECUPERACIÓN DE ACTIVOS A PARTIR DE COPIAS DE RESPALDO

10.1 SOLICITUD DE RECUPERACIÓN DE ACTIVOS

1. La operación de recuperación de activos a partir de copias de respaldo se iniciará a petición del Responsable del Activo y deberá ser previamente aprobada por el departamento de informática competente.
2. Para solicitar una recuperación, el Responsable del Activo abrirá una incidencia en el <<gestor de incidencias>> de CRUZ ROJA ESPAÑOLA, a la que adjuntará la Solicitud de Recuperación de Activos. Un modelo de esta solicitud se presenta en el epígrafe 13 del presente Procedimiento.
3. El departamento de informática competente:
 - Aprobará la petición y señalará la incidencia al Departamento de Sistemas de CRUZ ROJA ESPAÑOLA, o
 - Rechazará la petición, cerrando la incidencia y detallando los motivos que provocan tal rechazo.

10.2 RECUPERACIÓN DE ACTIVOS

1. El Departamento de Sistemas de CRUZ ROJA ESPAÑOLA accederá al soporte físico en el que reside la copia de respaldo del activo a recuperar y lo cargará en la unidad de lectura de la herramienta de generación de copias de respaldo.
2. El personal del área de Explotación del Departamento de Sistemas de CRUZ ROJA ESPAÑOLA responsable de la recuperación del activo, accede al soporte y, empleando las herramientas de copia, restaura el activo en una

ubicación temporal a la que sólo tendrá privilegios de acceso su responsable, y actualizará la incidencia informando de la ubicación donde puede localizar el activo.

3. El Responsable del Activo accederá a la ubicación temporal y:

- Validará la recuperación del activo, expresando su conformidad en el registro de la incidencia, autorizando de esta forma su restauración a partir de la copia en su ubicación original, o
- La rechazará, solicitando en el campo comentarios de la incidencia una nueva recuperación a partir de una copia de respaldo alternativa.

4. Una vez validada la restauración, el Responsable del Activo:

- Recuperará el activo en su ubicación original.
- Eliminará de su ubicación temporal el activo recuperado desde la copia de respaldo.

5. Por su parte, el Departamento de Sistemas de CRUZ ROJA ESPAÑOLA:

- Retirá el soporte físico de la unidad de lectura de la herramienta de generación de copias y lo devolverá al armario ignífugo donde se almacenan los soportes de CRUZ ROJA ESPAÑOLA.
- Almacenará el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de restauración de CRUZ ROJA ESPAÑOLA.
- Cerrará la incidencia.

11. COMPROBACIÓN PERIÓDICA DE LOS PROCEDIMIENTOS DE RESTAURACIÓN

1. Para garantizar la eficacia de los procedimientos de restauración de CRUZ ROJA ESPAÑOLA y la capacidad para recuperar activos desde las copias de respaldo, se establecerá el procedimiento de comprobación periódica que se detalla a continuación.

11.1 PROCEDIMIENTO DE COMPROBACIÓN

78. EL primer día del mes, el Departamento de Sistemas de CRUZ ROJA ESPAÑOLA

- Seleccionará al azar un activo de información 15 almacenado en la copia de respaldo.
- Ejecutará una restauración del activo sobre una ubicación temporal, comprobará la restauración del activo y lo eliminará posteriormente.
- Almacenará el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de comprobación periódicas de CRUZ ROJA ESPAÑOLA.

12. REGISTROS E INDICADORES

Identificador	Nombre	Frecuencia	Archivo	Genera	Custodia
<<x-R01>>	Herramientas de generación de copias de respaldo	Una vez al año	Gestor Documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<x-R02>>	Activos sujetos a copia de respaldo	Dos veces al año	Gestor Documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<x-R03>>	Soportes extraíbles	Una vez al año	Gestor Documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<x-R04>>	Solicitudes de inclusión de activos en la copia de respaldo	No aplicable	Gestor de incidencias	Responsable del activo	Responsable de Gestión de Soportes
<<x-R05>>	Solicitudes de	No aplicable	Gestor de	Responsable	Responsable de

	restauración		incidencias	del activo	Gestión de Soportes
<<x-R06>>	Operaciones de restauración	Una vez al año	Gestor documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<x-R07>>	Operaciones de comprobación periódicas	Una vez al año	Gestor documental	Responsable del área de Explotación	Responsable de Gestión de Soportes

12.2 TABLA DE INDICADORES

Identificador	Rango	Frecuencia	Métrica	Objetivo	Descripción
<<x-I01>>	%	Una vez al año	Operaciones fallidas de recuperación con respecto al total	0%	--

13. SOPORTE Y MODELOS

13.1 SOPORTE

1. A continuación se detallan los elementos de soporte necesarios para la implantación del presente Procedimiento.

- Herramientas de generación de copias de respaldo.
- Soportes de almacenamiento.
- Armario ignífugo.
- Gestor de incidencias.

13.2 MODELOS

2. A continuación se detallan los modelos a emplear para la implantación del presente Procedimiento.

Modelo de solicitud de inclusión de activos en la copia de respaldo

3. Modelo para la solicitud de inclusión de activos en la copia de respaldo.

Activo	Sistema	Periodo Retención	Tipo (A/C)	Contenidos	Comentarios
	(Sistema de información que alberga el activo a incluir en la copia de respaldo.)		(Tipo de activo a incluir en la copia de respaldo: A: Activo de información, C: Sistema de Información completo.)	Únicamente para activos de tipo Activo de información, listado completo con el detalle de contenidos, incluyendo directorios y archivos sobre los que generar copia de respaldo.)	

Modelo de registro de herramientas para la generación de copias de respaldo

1. Modelo para el registro de herramientas para la generación de copias de respaldo.

Nombre	Tipo (HW/SW)	Fabricante	Versión	Responsable
	Tipo de herramienta: HW: Hardware, SW: Software.			

Modelo de registro de soporte extraíbles

1. Modelo para el registro de soportes para la generación de copias de respaldo.

Etiqueta	Contenido	Formato	Capacidad	Responsable

Modelo de solicitud de recuperación de activos

2. Modelo para la solicitud de recuperación de activos desde la copia de respaldo.

Activo a recuperar	Sistema	Tipo (A/C)	Fecha recuperación	Tamaño estimado	Comentarios
	(Sistema de información que alberga el activo a recuperar.)	(Tipo de activo a recuperar desde la copia de respaldo: A: Activo de información, C: Sistema de información completo.)	(Fecha estimada en la que el activo se encontrará disponible.)		

Modelo de registro de activos sujetos a copia de respaldo

Activo	Tipo copia (C/I/D)	Periodicidad (D/S/M/A/BD)	Periodo retención	Contenido	Responsable	Soporte (C/D)	Tipo Activo (A/C)	Comentarios
	(Tipo de copia de respaldo: C: Completa, I: Incremental, D: Diferencial)	(Periodicidad de la copia: D: Diaria, S: Semanal, M: Mensual, A: Anual, BD: Bajo Demanda.)				(Tipo de soporte en el que se almacena la copia: C: Cinta, D: Disco.)	(Tipo de activo: A: Activo de información, C: Sistema de información completo .)	

3.1. Seguridad de las operaciones

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

En todos los equipos y servidores de la organización se han implantado medidas de antivirus que los protegen de software malicioso. Los antivirus se encuentran configurados para actualizar sus bases de datos diariamente o en el momento en el que haya una actualización crítica.

El antivirus implantado en la organización es: _____

COPIAS DE SEGURIDAD

Las copias de seguridad se realizarán con una periodicidad al menos semanal, salvo que en dicho periodo no se hubiera producido ninguna actualización de datos.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

CRUZ ROJA ESPAÑOLA, S.L., o en quién él delegue, verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que necesiten utilizar datos personales, se realizarán previa copia de seguridad, garantizando el nivel correspondiente al tratamiento realizado.

POLITICA DE MESAS LIMPIAS

Al acabar la jornada debe guardarse la documentación que se encuentra a la vista (información de la empresa, clientes, proveedores, etc.). Se debe ser especialmente estricto en los puestos de atención al público.

La documentación que no estemos utilizando en un momento determinado debe estar guardada correctamente.

No puede haber contraseñas, nombres de usuario o datos personales en post-its o similares en los puestos de trabajo.

SALVAPANTALLAS Y BLOQUEO

En los puestos de atención al público, o cuando se comparta espacio con personal que tenga autorizaciones diferentes a las nuestras, debe activarse el salvapantallas.

En cualquier caso, al abandonar el puesto de trabajo, aunque sea de forma momentánea se debe bloquear el mismo. Para ello se puede pulsar Ctrl + Alt + Supr o Windows+L. En los sistemas que es posible, el área de sistemas dispone medidas automáticas para programar el bloqueo automático del mismo tras 5 minutos de inactividad por parte del usuario.

PROGRAMAS Y APLICACIONES

Los puestos de trabajo tienen una configuración fija en sus aplicaciones y sistemas operativos, que sólo puede ser cambiada bajo la autorización del responsable de seguridad o por el administrador del sistema.

No está permitida a los usuarios la instalación de ningún programa o aplicación. Las aplicaciones necesarias serán instaladas exclusivamente por el personal del Departamento de Informática.

Se prohíbe el uso de aplicaciones no relacionadas con la actividad de la organización, por entenderse que pueden comprometer la seguridad de los equipos y permitir de forma no controlada el acceso a datos protegidos.

IMPRESORAS

En el caso de las impresoras debe asegurarse de que no queden documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos, los responsables de cada puesto deben retirar los documentos conforme van siendo impresos.

FICHEROS TEMPORALES

Los ficheros temporales que los usuarios mantengan en sus ordenadores personales deberán ser borrados, una vez haya concluido la finalidad para la que fueron creados (fichero temporal: ficheros de trabajo creados por los usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento).

Se prohíbe la creación de nuevos ficheros que supongan el tratamiento de datos personales, así como la cesión de los mismos sin previa autorización de CRUZ ROJA ESPAÑOLA.

3.2. POLÍTICA PARA PROTECCIÓN Y ADMINISTRACIÓN DE LOS SERVIDORES DE LA RED CORPORATIVA

El buen uso por parte del personal de los servidores de almacenamiento en red es fundamental. Desde CRUZ ROJA ESPAÑOLA hemos optado por un almacenamiento en la nube así como “on premise” de la documentación de nuestros trabajadores, a través de una red tipo NAS (Network Attached Storage), para archivos compartidos. Los puntos a tener en cuenta serán los siguientes:

- Clasificación de la información: el empleado deberá cumplir con la Política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa. De esta forma se almacenará en la forma y lugar correctos.
- Control de acceso: se establecen regla para el acceso a la información dependiendo del rango o rol que los usuarios tengan en CUZ ROJA ESPAÑOLA por lo que el departamento de Márketing no puede acceder a la documentación del departamento de Facturación. Asimismo, los trabajadores más nóveles solo tendrán permisos de lectura sobre aquellos documentos que solo sean consultivos.
- Copias de seguridad: ejecutaremos el plan de copias de seguridad en el que se detalla la información a guardar, cada cuánto tiempo se va a realizar, dónde se va a almacenar y el tiempo de conservación de cada copia.
- Acceso limitado: según lo establecido en la política de clasificación de la información se definen perfiles de acceso (y se asignan a los usuarios) que limitan el uso de la información, de manera que cada usuario acceda solo a los directorios necesarios para el desempeño de su actividad laboral.
- Almacenamiento clasificado: crearemos carpetas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Se asignarán los permisos de acceso pertinentes según el perfil del empleado.
- Cifrado de la información: según la política de clasificación de la información, cifraremos la información crítica que se almacene en la red corporativa.
- Auditoría de servidores: Cada cierto tiempo, que especificaremos, tendremos que revisar el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.

3.3. Política para el uso de software permitido

En esta política se incluyen una serie de controles para verificar el cumplimiento de licencias relativas a las aplicaciones y programas que el departamento de informática y legal han estimado oportunas para el desempeño de la labor de los trabajadores:

- Registro de licencias. Si queremos saber de qué software dispone la organización conviene tener un registro actualizado de licencias. En dicho registro se almacenará al menos la siguiente información:

-Nombre y versión del producto -Autor -Fecha de adquisición -Vigencia de la licencia -Tipo de licencia -Número de usuarios permitidos por licencia - Número de licencias adquiridas por cada software -Facturas o comprobantes de compra -Ubicación física del producto.

- Competencia para la instalación, actualización y borrado: para asegurarnos una configuración óptima en nuestros únicamente el personal técnico puede instalar, actualizar y eliminar software. En ningún caso se permite la instalación ni la actualización de software a través de enlaces de webs o correos cuyo origen no sea completamente seguro. Por último remarcar que el software instalado en los equipos debe estar correctamente actualizado.
- Sanciones por uso de software no autorizado: si se detecta que se utiliza un software ilegal o no autorizado el trabajador será sancionado con 30 horas de formaciones en prevención y seguridad de la información. Además, se notificará la posibilidad de acarrear con responsabilidades civiles y penales según la legislación vigente en cada momento en materia de protección de la propiedad intelectual.
- Repositorio de software: para poder tener acceso al software por parte de los trabajadores se ha implementado un repositorio que se accede con las claves de cada trabajador donde se especifica las licencias y el rol que cada usuario puede hacer de él.
- Auditoria de software instalado: nos reservamos el derecho de auditar o inspeccionar en cualquier momento los equipos de los usuarios para verificar que se cumple esta política.
- Autorización y licencia del software: garantizamos periódicamente que los programas instalados en cualquier dispositivo corporativo (se incluyen los dispositivos BYOD) están debidamente autorizados y que disponen de las licencias necesarias. Así mismo, animamos que los trabajadores lean y comprendan los términos y condiciones de uso de dichas licencias. De este modo podremos cumplir con la Ley de Propiedad Intelectual.
- Política de copias de software: Para garantizar lo especificado en las licencias de uso no se debe permitir que los empleados realicen copias del software disponible sin el debido consentimiento.

3.4. Política de seguridad para dispositivos móviles

El equipo de seguridad de CRUZ ROJA ESPAÑOLA deberá contar con un checklist que cuente con los siguientes puntos clave:

- Asignación de dispositivos: procedimiento de solicitud y asignación de los dispositivos móviles corporativos para mantener un inventario activo y registrar las necesidades de los trabajadores.
- Registro de equipos: mantener un registro de los dispositivos móviles asignados (qué dispositivo y a quién se le asigna).

- Mantenimiento de dispositivos: el mantenimiento de dispositivos queda restringido al departamento responsable de su mantenimiento. Por tanto debe prohibirse que el usuario haga cambios en el hardware, instale software o modifique la configuración del equipo sin autorización del departamento competente.

- Protección de la BIOS: los equipos portátiles corporativos tendrán el acceso a la BIOS protegido con contraseña para evitar modificaciones en la configuración por parte del usuario.

- Software de localización: en el caso de que se considere necesario instalar o activar algún software de localización se comunicará al usuario del dispositivo antes de realizar la entrega del mismo. El usuario que va a estar geolocalizado debe firmar un documento aceptando esta condición.

- Almacenamiento de la información: la información corporativa que no sea estrictamente necesaria para el desarrollo de las tareas del usuario no debe almacenarse en el dispositivo. Si se accede a la información desde varios dispositivos, esta tiene que estar sincronizada para evitar duplicidades y errores en las versiones.

- Tratamiento de la información confidencial: toda la información confidencial debe almacenarse cifrada. Antes de la devolución del dispositivo, la información debe ser eliminada de forma segura o solicitar su eliminación al técnico responsable.

- Conexión a redes: las conexiones a redes ajenas a la organización seguirán las normas establecidas en la política de uso corporativo de redes externas

- Notificación en caso de infección: si se sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal técnico responsable.

- Transporte y custodia: el equipo no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo. En ningún caso se debe descuidar el portátil si se viaja en transporte público. Tampoco se ha de guardar en el coche ni dejarlo visible o fácilmente accesible. Si se trabaja en lugares donde no se garantiza la custodia del equipo, este debe quedar anclado con un candado de seguridad o guardado en un armario de seguridad. En caso de robo o pérdida del equipo se debe notificar de manera inmediata al personal técnico responsable.

- Uso del puesto de trabajo: el usuario aplicará las normas recogidas en la Política de uso del puesto de trabajo que sean relativas al uso de un equipo informático (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, etc.).

- Responsabilidades: el usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones. Por tanto, es el trabajador el que debe garantizar la seguridad tanto del equipo como de la información que contiene. Esta normativa será de obligado cumplimiento y podrá ser objeto de acuerdos que se firmen al aceptar el uso de estos dispositivos.

3.5. Control de acceso

Gestión de acceso de los usuarios

Registro y baja de usuario

Alta de usuarios

El alta de usuario en el sistema de información será realizada por el área de informática de forma que se asegure un mínimo acceso según las necesidades específicas de su puesto de trabajo.

El alta de un usuario únicamente podrá ser solicitado por el área de Recursos Humanos, a través de correo electrónico, teléfono o vía procedimiento de gestión de incidencias, comunicando al área de sistemas el alta de usuario, indicando los datos identificativos del mismo, puesto de trabajo y permisos necesarios.

El usuario se dará de alta con todos los datos facilitados por el área de Recursos Humanos, forzando al cambio de contraseña en su primer inicio de sesión en el Directorio Activo. El usuario se creará con los siguientes parámetros:

Nombre de usuario

Contraseña

Unidad organizativa

Grupos de usuario

Baja de usuarios

La baja de usuario deberá ser comunicada por el área de Recursos Humanos, a través de correo electrónico, teléfono o vía procedimiento de gestión de incidencias. Siempre que sea posible, esta comunicación deberá ser realizada días antes de la baja real para garantizar el correcto bloqueo de la cuenta del usuario. Implicará el bloqueo del mismo en el LDAP de la organización, y la baja específica de todas las aplicaciones que implicaban el perfil y puesto asignado al mismo.

Modificación de los usuarios

La modificación de los derechos o permisos de acceso de un usuario deberá ser comunicada por el área de Recursos Humanos o por el responsable del área donde el usuario está asignado.

Cuando la solicitud se realice a través de correo electrónico o teléfono, el área de sistemas generará una solicitud en la herramienta de gestión de incidencias con la parametrización solicitada.

La comunicación debe contener los nuevos permisos concedidos o permisos denegados y la justificación de los mismos.

Política de control de acceso

Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. Cada aplicativo dispone de un listado de usuarios y perfiles de usuario, donde se definen los permisos específicos para la misma.

El responsable del tratamiento ha establecido mecanismos para evitar que los usuarios puedan acceder a recursos distintos de los autorizados mediante la asignación y comunicación de perfiles a los usuarios.

Exclusivamente CRUZ ROJA ESPAÑOLA podrán conceder, alterar o anular el acceso autorizado a los datos o recursos por parte de un usuario.

El acceso físico a las instalaciones está controlado, por lo que cualquier persona no autorizada precisa estar acompañada de personal autorizado.

Control de acceso físico

El acceso a las oficinas en el horario laboral se encuentra controlado por personal de la organización. Sólo está permitido el acceso a las oficinas al personal de la organización. El personal ajeno CRUZ ROJA ESPAÑOLA que deba acceder a las instalaciones, deberá ir siempre acompañado por personal de la organización autorizado. Fuera de horario laboral las oficinas permanecerán cerradas.

El acceso a las oficinas dispone de los siguientes medios para impedir y controlar el acceso:

- Control de acceso

- Con cerradura electrónica. (Acceso con tarjeta magnética...)

- Con cerradura manual. La llave se encuentra custodiada por el área de sistemas.

- Registro de accesos

- Automático, en la herramienta de control de acceso.

- Cámaras de seguridad y videovigilancia que se encuentra debidamente notificada a la entrada de las instalaciones

Identificación y autenticación

El responsable del tratamiento adoptará las medidas necesarias para garantizar la correcta identificación y autenticación de los usuarios con acceso a datos personales automatizados. La identificación de usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización (la identificación pertenecerá a un solo usuario).

El mecanismo de autenticación de la organización se basa en la existencia de contraseñas, de esta forma todos los usuarios con acceso autorizado tienen un código de usuario que es único y que está asociado a la contraseña correspondiente que sólo será conocida por el propio usuario.

Las contraseñas son personales e intransferibles. Una vez asignada, el usuario es responsable de la confidencialidad de las contraseñas, prohibiéndose expresamente el acceso al sistema utilizando el identificador y la contraseña de otro usuario. En todo caso, la responsabilidad sobre el acceso realizado recaerá siempre sobre el usuario que tuviera asignado el identificador y la contraseña utilizada.

Las aplicaciones específicas con acceso restringido requerirán, asimismo, la introducción del identificador y la contraseña para verificar la autorización del usuario.

Procedimiento de asignación y distribución de contraseñas

A cada uno de los usuarios autorizados para el tratamiento de datos personales de manera automatizada se le asignará un identificador y una contraseña.

Estos mecanismos servirán para controlar las autorizaciones del personal.

CRUZ ROJA ESPAÑOLA o persona en la que él delegue, será el que decida el perfil de usuario al que se da acceso mediante un determinado nombre de usuario y contraseña.

Las contraseñas se distribuirán de forma que se garantice su confidencialidad, debiendo almacenarse de forma ininteligible.

Las modificaciones de contraseña se realizan a petición del usuario, cuando sea necesario por motivos de mantenimiento del sistema o por pérdida u olvido.

Las contraseñas caducan y, por tanto, se cambiarán en un periodo máximo de un año. El área de sistemas deberá implantar, siempre que sea posible por la tecnología utilizada, medidas que requieran a los usuarios dicho cambio.

Se tendrán en cuenta las siguientes normas en la asignación de identificadores:

- No se reutilizará un identificador, estos deberán ser personalizados.

- Utilizar al menos cinco caracteres en la composición del identificador del usuario.
- Se debe mantener únicamente aquellos nombres de usuario propios de los sistemas operativos y de las aplicaciones de software que no puedan ser modificados.

El formato de las contraseñas de usuario utilizadas cumple los siguientes requerimientos:

- La longitud mínima será de doce caracteres.
- Será mediante combinación de letras, números y se aconseja la utilización, si es posible, caracteres especiales (¡@#~€%&/()=-_ ...).
- Se evitarán nombres comunes, números de matrículas de vehículos, teléfonos, nombres de familiares, amigos, etc.
- No utilizar una contraseña que se corresponda con el identificador del usuario.

Cuando se extinga la necesidad de acceder a los datos o al sistema de información por parte de un

Usuario, o cuando CRUZ ROJA ESPAÑOLA, S.L. considere que ya no es necesario su acceso a los datos del mismo para el desarrollo de su trabajo, se procede a la cancelación de los derechos de acceso de dicho Usuario al sistema de información por parte del Administrador del Sistema o en su caso el Responsable de Seguridad. Se almacenará información descriptiva sobre los perfiles de acceso de los usuarios que se den de baja, durante el tiempo requerido para cumplir obligaciones legales y para auditoría.

Criptografía

El envío de información confidencial se realizará utilizando mecanismos de cifrado que permita el acceso únicamente a su receptor.

Para el envío a través de portales web, el usuario debe garantizar que la información se envía de forma cifrada, validando al acceder que se encuentra bajo protocolo https.

Para el envío a través de correo electrónico u otros medios de comunicación directa como mensajería instantánea (WhatsApp, Telegrama, etc.) el usuario deberá enviar los archivos cifrados con una contraseña, de la cual habrá informado al receptor a través de otro medio de comunicación.

Política de seguridad del desempeño del teletrabajo

El teletrabajo permite llevar a cabo la actividad laboral desde una ubicación distinta de las sedes que

CRUZ ROJA ESPAÑOLA tiene asignada para que los trabajadores desempeñen sus funciones. Para

todos aquellos trabajadores que opten por un sistema híbrido de teletrabajo y presencialidad se deberá tener en cuenta los siguientes puntos para que el desempeño de sus tareas sea seguro:

Relación de usuarios que disponen de la opción de trabajar en remoto. será necesario llevar un control de las personas que tengan régimen de semi-presencialidad

Periodo de implantación y pruebas: se precisará valorar diferentes escenarios y configuraciones antes de comenzar a teletrabajar ya que la implementación demasiado rápida del teletrabajo, sin valorar los riesgos de seguridad, puede poner en peligro la información confidencial de la empresa.

Realizar pruebas de carga en escenarios simulados: si existe un volumen considerable de empleados que vayan a teletrabajar al mismo tiempo, será necesario valorarse la carga que esto ocasiona en los sistemas internos de la empresa.

Aplicaciones y recursos a los que tiene acceso cada usuario: cada empleado tendrá acceso solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo de su perfil dentro de la organización. En el caso de que el empleado necesitase la instalación y uso de un nuevo software, este tendrá que ser previamente aprobado por el departamento informático de CRUZ ROJA ESPAÑOLA.

Acceso seguro: para las credenciales de acceso se utilizarán contraseñas robustas y el doble factor de autenticación siempre que sea posible, forzando su cambio periódicamente. El mecanismo de gestión de credenciales estará controlado por el departamento informático a través de servicios de directorio LDAP, utilizando implementaciones comerciales de Windows Active Directory. Los dispositivos utilizados por el empleado para teletrabajar serán previamente configurados por los técnicos de la organización (sistema operativo, antivirus, control de actualizaciones , etc.), tanto si son corporativos como si son aportados por el trabajador.

Cifrado de los soportes de información: todos los dispositivos almacenarán la información cifrada, tanto para proteger los datos de la empresa de posibles accesos malintencionados, como para garantizar su confidencialidad e integridad.

Uso de conexiones seguras a través de una red privada virtual o VPN: la conexión a la red de CRUZ ROJA ESPAÑOLA se realizará a través de VPN para facilitar el teletrabajo manteniendo el sistema operativo y las herramientas de conexión VPN actualizadas, empleando una cuenta de usuario específica para trabajar con la VPN y sin privilegios de administrador, disponer de un software antivirus y antimalware actualizados. Así mismo, se recomienda conectarse por cable Ethernet para reforzar la seguridad y persistencia de la red VPN. Finalmente, se ruega que ante cualquier incidencia o comportamiento extraño, contactar inmediatamente con el Departamento Informático de CRUZ ROJA ESPAÑOLA.

Conexión a Internet. Cuando no sea posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utiliza la red de datos móvil 4G o 5G quedan prohibidas la conexión a redes públicas.

Aplicaciones de teleconferencia y colaborativas: toda aplicación para efectuar trabajo colaborativo serán revisadas por el equipo técnico y legal de CRUZ ROJA ESPAÑOLA quedando prohibido el uso de aplicaciones no validadas por la organización.

Política de privacidad

1ª capa

CRUZ ROJA ESPAÑOLA tratará sus datos personales para dar respuesta a las solicitudes planteadas a través de este chatbot. Los datos que se recopilen serán tratados con las máximas garantías que prevé la legislación. Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, en la dirección de correo electrónico dpo@cruzroja.es.

Le recomendamos que lea la política de privacidad antes de proporcionarnos sus datos personales dpo@cruzroja.es.

He leído y acepto las condiciones de la política de privacidad ☐

2ª capa

Estas normas rigen para todas las páginas que alberga CRUZ ROJA ESPAÑOLA (en adelante CRE). Para saber cómo se procede con los datos personales, te rogamos leas la siguiente política de privacidad que aconsejamos consultar con regularidad, dado que puede ser actualizada. El visitante se hace responsable y garantiza que los datos personales que facilita a CRE son veraces y cuenta, cuando proceda, con la debida autorización para ello del titular de los mismos.

CRE tratará los datos de carácter personal vinculados a sus espacios webs respetando las exigencias de la legislación vigente, resaltando:

(terminar porque lucia esta modificando cosas)

2. Pentesting

El pentesting consiste en simular un ataque real de amenazas persistentes avanzadas (APT) contra una organización mediante la combinación de diferentes vectores de ataque. El objetivo es identificar el nivel de seguridad global de la empresa y evaluar su capacidad de prevención, protección y respuesta ante amenazas dirigidas.

El equipo Red Team está formado por expertos en seguridad digital y se enfoca en replicar técnicas, tácticas y procedimientos de intrusión que podrían ser utilizados por un atacante real. El objetivo final es mejorar las capacidades técnicas y de detección del equipo de defensa o Blue Team.

Antes de comenzar a explicar con mayor profundidad cuáles serían los pasos a seguir en la realización de un pentesting y, en concreto, en la realización de un pentesting a Azure, se ha considerado oportuno aclarar los conceptos de **Red Team, pentesting y auditoría de seguridad:**

- **Red team:** ejercicio de intrusión real donde se simulan todos los posibles vectores de entrada y se busca tomar el control de los principales activos de la organización para evaluar su capacidad de protección y respuesta ante ataques dirigidos.
- **Pentesting:** consiste en demostrar mediante una pequeña intrusión controlada, la capacidad de un atacante para comprometer un sistema o aplicación. Se buscan vulnerabilidades críticas y su duración es de varias semanas.
- **Auditoría de seguridad:** las auditorías de seguridad buscan encontrar todas las vulnerabilidades conocidas en un activo o conjunto de activos.

A continuación, se procederá a detallar los pasos a seguir para la realización de un pentesting en Azure:

1. Recopilación de información: es importante recolectar información sobre la infraestructura y los sistemas y aplicaciones que se van a probar. Esto incluye, por ejemplo, el tipo de máquinas, la configuración de seguridad, los servicios de red y almacenamiento, y los servicios y aplicaciones instaladas.
2. Escaneo de puertos y servicios: esto se realiza para identificar posibles vulnerabilidades. Se pueden utilizar herramientas de escaneo automatizadas (que las veremos más adelante) para agilizar el proceso.
3. Análisis de vulnerabilidades: una vez se han identificado algunas vulnerabilidades, se deben analizar en detalle para determinar su gravedad y cómo se podrían explotar.
4. Explotación: en el caso de encontrar algunas vulnerabilidades críticas, se pueden intentar explotar para comprobar la efectividad de la explotación y la capacidad de acceso a los sistemas y aplicaciones.
5. Análisis post-explotación: una vez se ha obtenido acceso a los sistemas, se debe analizar para determinar el alcance del acceso y la información que se ha obtenido.
6. Informe: finalmente, se debe elaborar un informe detallado con los resultados obtenidos, las vulnerabilidades encontradas y las recomendaciones para su corrección.

Pentesting en Azure

El pentesting en Azure es el proceso de realizar pruebas de intrusión en una infraestructura alojada en el cloud de Microsoft, Azure. El objetivo es identificar vulnerabilidades y debilidades en los sistemas y aplicaciones alojadas en Azure, con el fin de mejorar la seguridad de la infraestructura. Durante un pentesting en Azure, se utilizan técnicas y herramientas similares a las utilizadas en un pentesting tradicional, pero se adaptan a las características y configuraciones específicas de Azure. El alcance de las pruebas puede variar, pero generalmente incluyen la verificación de la configuración de seguridad, el análisis de los servicios de red y almacenamiento, y la comprobación de las aplicaciones y servicios. El resultado final es un informe detallado que incluye las vulnerabilidades encontradas y recomendaciones para su corrección.

El proceso de pentesting en una máquina de Azure se divide en varios pasos:

1. Configurar un entorno de prueba: Es importante tener un entorno de prueba separado del entorno de producción, donde se puedan realizar pruebas de seguridad sin causar daños al sistema.

2. Obtener permisos: Es necesario obtener permisos para realizar pruebas de seguridad en el sistema, ya que el pentesting de un sistema sin autorización puede tener consecuencias legales graves.

3. Escaneo de puertos: Utilice herramientas como Nmap para escanear los puertos abiertos en la máquina virtual y buscar posibles vulnerabilidades.

4. Análisis de vulnerabilidades: Utilice herramientas como Nessus o OpenVAS para analizar las vulnerabilidades encontradas en el escaneo de puertos.

5. Explotación: Utilice herramientas como Metasploit para explotar las vulnerabilidades encontradas en el análisis de vulnerabilidades.

6. Escalada de privilegios: Una vez que se ha comprometido una máquina, el siguiente paso es escalar los privilegios para obtener acceso completo al sistema.

7. Recopilación de información: Utilice herramientas como LinEnum para recopilar información adicional sobre el sistema comprometido.

8. Limpieza: Una vez completado el pentest, asegurarse de limpiar cualquier archivo o configuración creada durante el proceso.

Es importante recordar que el pentesting de un sistema en producción puede causar daños y deben tener permiso para realizarlo.

Para la realización del Pentesting es necesario contar los permisos pertinentes por parte de la fundación Azure. De esta forma, las pruebas de penetración sólo se pueden realizar si se obtiene el approval al llenar la forma en Azure Customer:
Enlace formulario: Support. <https://security-forms.azure.com/penetration-testing>

Un aspecto muy importante a tener en cuenta es que la petición debe hacerse con mínimo 7 días de antelación al momento en el que se quiere comenzar a trabajar.

En concreto, el proceso de aprobación es el siguiente:

1. Una vez enviada la forma el equipo de Azure responderá en 3 días laborales, si necesitan más información contactarán al correo anotado en la solicitud.

Uno le puede dar seguimiento a través del número de referencia recibido al enviar la forma.

2. Sólo se pueden ejecutar pruebas autorizadas por Azure, en caso de requerir más tiempo se debe hacer una solicitud nueva.

En caso de que durante o al finalizar las pruebas se encuentre una vulnerabilidad de Azure, se deberá reportar a la mayor brevedad posible para poder encontrarle solución.

Además, la realización de estas pruebas, están sujetas a una serie de **términos y condiciones**:

1. La prueba es sólo sobre tu app, nada de terceros u otros.
2. Sólo pruebas permitidas.
3. Ninguna prueba que exceda la cuota de ancho de banda para la suscripción.
4. Se ejecutaran sólo pruebas autorizadas en el email que envía Microsoft en el tiempo y duración que Microsoft especifica. Tu acataras cualquier otra restricción.
5. Eres responsable por daño a Azure o a otros clientes de Azure que son causadas por falta de cumplimiento de este acuerdo.

Las siguientes pruebas serán sujetas a revisión acelerada:

- 1.-Prueba de endpoint para descubrir el top 10 vulnerabilidades web de OWASP.
- 2.-Fuzz testing en los endpoints.
- 3.-Escaneo de puertos en los endpoints.

También existen algunas pruebas que está prohibido realizarlas como son cualquier Denegación de Servicios o cualquiera que determine, demuestre o simule la existencia de cualquier tipo de Denegación de Servicio (DoS).

Solo puede simular ataques mediante partners de prueba aprobados por Microsoft:

- BreakingPoint Cloud: un generador de tráfico de autoservicio donde los clientes pueden generar tráfico destinado a los puntos de conexión públicos que tengan habilitado el servicio DDoS Protection con fines de simulación.
- Red Button: trabaje con un equipo dedicado de expertos para simular escenarios de ataque DDoS reales en un entorno controlado.

Como información adicional, en la página oficial de Azure, se nos comunica lo siguiente:

“No realizamos pruebas de penetración de su aplicación, pero sabemos que quiere y necesita realizar dichas pruebas en sus propias aplicaciones. Eso es bueno, ya que al mejorar la seguridad de sus aplicaciones, ayuda a hacer que todo el ecosistema de Azure sea más seguro.

Desde el 15 de junio de 2017, Microsoft ya no requiere la aprobación previa para llevar a cabo pruebas de penetración con recursos de Azure. Este proceso solo está relacionado con Microsoft Azure y no es aplicable ningún otro servicio de Microsoft Cloud”.

Pentesting en un chatbot

Una de las características con la que va a contar la página web desarrollada, es la existencia de un Chatbot o asistente virtual por lo que se ha incluido un apartado específico sobre cómo realizar un pentesting a este tipo de funcionalidad. Esta herramienta cada vez es más utilizada en una gran variedad de aplicaciones, desde la atención al cliente hasta la automatización en procesos de negocio. Sin embargo, también están sujetos a la posibilidad de sufrir ataques cibernéticos:

1. Recopilación de información: como hemos dicho antes, el primer paso a realizar en cualquier pentesting es la recopilación de información (tecnología utilizada, servicios y aplicaciones conectadas y las políticas de seguridad existentes).
2. Análisis de la arquitectura: se debe entender cómo está construido el chatbot y cómo se comunica con otras aplicaciones y servicios.
3. Análisis de lógica: se debe analizar la lógica y el comportamiento del chatbot para identificar posibles vulnerabilidades.
4. Pruebas de seguridad: se deben llevar a cabo pruebas de seguridad para identificar posibles vulnerabilidades en el chatbot, como inyección de código, ataques de phishing o robo de sesión.
5. Evaluación de la respuesta: se debe evaluar cómo el chatbot maneja las situaciones de seguridad y cómo se comunica la existencia de una vulnerabilidad o un ataque.
6. Informe: Finalmente, se debe elaborar un informe detallado con los resultados obtenidos, las vulnerabilidades encontradas y las recomendaciones para su corrección.

OWASP Top 10:

El conocido OWASP Top 10 es una lista de los principales riesgos de seguridad para una aplicación web. La mayoría de los chatbots están disponibles en una interfaz de web pública y, como tal, todos los riesgos de seguridad de OWASP también se aplican a esos chatbots. De estos riesgos, hay dos especialmente importantes contra los cuales defenderse, ya que en contraste con los otros riesgos, esos dos son casi siempre una amenaza grave — XSS (secuencias de comandos entre sitios) e inyección SQL.

Además, para los chatbots habilitados para inteligencia artificial, existe un mayor riesgo de Denegación de servicio ataques, debido a la mayor cantidad de recursos informáticos involucrados.

Vulnerabilidad 1: XSS – Guión entre sitios

Es una técnica utilizada para inyectar código malicioso en un sitio web mediante una entrada no validada.

Una implementación típica de una interfaz de usuario de chatbot:

- Hay una ventana de chat con un cuadro de entrada.
- Todo lo que el usuario ingresa en el cuadro de entrada se refleja en la ventana de chat.
- La respuesta de Chatbot se muestra en la ventana de chat.

La vulnerabilidad XSS está en el segundo paso — al ingresar texto, incluido el código Javascript malicioso, el ataque XSS se cumple cuando el navegador web ejecuta el código inyectado:

```
< script > alert ( document.cookie ) < / script >
```

Posible vector de ataque

Para explotar una vulnerabilidad XSS, el atacante tiene que engañar a la víctima para que envíe texto de entrada malicioso.

1. Un atacante engaña a la víctima para que haga clic en un hipervínculo que apunta al chatbot, incluido algún código malicioso en el hipervínculo
2. El código malicioso se inyecta en el sitio web, lee las cookies de la víctima y se lo envía al atacante sin que la víctima se dé cuenta
3. El atacante puede usar esas cookies para obtener acceso a la cuenta de la víctima en el sitio web de la compañía.

Herramientas específicas

Algunas herramientas comunes utilizadas para llevar a cabo una inyección XSS incluyen:

- Burp Suite: una herramienta de seguridad web que incluye un escáner de inyección XSS automatizado.
- OWASP ZAP: una herramienta de seguridad web de código abierto que incluye un escáner de inyección XSS automatizado.
- XSSer: una herramienta de línea de comando automatizada para la inyección XSS.
- XSSStrike: Un escaner de XSS avanzado y generador de payloads.
- XSpear: Una herramienta para automatizar pruebas de inyección XSS

Vulnerabilidad 2: Inyección SQL

Una implementación típica de un backend de chatbot orientado a tareas:

- El usuario le dice al chatbot algún elemento de información.
- El backend de chatbot consulta una fuente de datos para este elemento de información.
- Según el resultado, se genera y presenta una respuesta del lenguaje natural al usuario.

Con SQL Injection, el atacante engaña al backend de chatbot para considerar contenido malicioso como parte del elemento de información:

```
mi número de pedido es " 1234; BORRAR DE PEDIDOS "  
'OR 1=1 --'
```

Posible vector de ataque:

Cuando el atacante tiene acceso personal al chatbot, el atacante explota directamente una inyección SQL (, consulte el ejemplo anterior), haciendo todo tipo de consultas SQL (o no-SQL).

Herramientas específicas

Algunas herramientas comunes utilizadas para llevar a cabo una inyección SQL

incluyen:

- sqlmap: una herramienta de línea de comando automatizada que detecta y explota

vulnerabilidades de inyección SQL.

- Havij: una herramienta gráfica de usuario (GUI) para la inyección SQL automatizada.

- SQLNinja: una herramienta de inyección SQL especializada en el sistema operativo

Windows.

- SQL injection scanner: una extensión de navegador que busca automáticamente

vulnerabilidades de inyección SQL en un sitio web.

Vulnerabilidad 3: Denegación de servicio

La inteligencia artificial requiere una alta potencia informática, especialmente cuando se trata de un aprendizaje profundo como la comprensión del lenguaje natural de última generación (NLU). El ataque de denegación de servicio (DoS) se centra en hacer que un recurso no esté disponible para el propósito fue diseñado, y no es difícil imaginar que los chatbots sean más vulnerables a los ataques de Denegación de servicio (DoS) que los backends habituales basados en sistemas de bases de datos altamente optimizados. Si un chatbot recibe una gran cantidad de solicitudes, puede dejar de estar disponible para usuarios legítimos. Estos ataques introducen grandes retrasos en la respuesta, pérdidas excesivas e interrupciones en el servicio, lo que resulta en un impacto directo en la disponibilidad.

Posible vector de ataque

Un ataque típico de DoS envía una gran cantidad de grandes solicitudes al chatbot para agotar intencionalmente los recursos disponibles. Sucederá que el recursos informáticos ya no están disponibles para usuarios legítimos.

Pero hay un riesgo adicional a considerar: es bastante común que lo usen los desarrolladores de chatbot servicios basados en la nube como IBM Watson o Google Dialogflow. Dependiendo del plan elegido, existen límites de uso y / o cuotas vigentes que pueden ser agotado bastante rápido – por ejemplo, Google Dialogflow Essential límites de plan gratis acceso a 180 solicitudes por minuto, todas las demás solicitudes serán denegadas. Para un plan basado en el uso sin límites, un ataque DoS puede costar fácilmente una fortuna debido al mayor número de solicitudes.

Herramientas

Algunas herramientas comunes utilizadas para llevar a cabo ataques DoS o DDoS incluyen:

- LOIC (Low Orbit Ion Cannon): una herramienta de código abierto utilizada para enviar un gran volumen de solicitudes a un objetivo específico.
- HOIC (High Orbit Ion Cannon): una herramienta de ataque similar a LOIC, pero con una mayor capacidad de ataque.
- Botnets: una red de dispositivos comprometidos que pueden ser utilizados para llevar a cabo ataques DDoS de manera distribuida.
- R-U-Dead-Yet (RUDY): una herramienta de código abierto para ataques DDoS HTTP.

Es importante tener en cuenta que un pentesting de un chatbot no solo debe evaluar la seguridad del chatbot en sí mismo, sino también la seguridad de las aplicaciones y servicios con los que se comunica. Además, se deben seguir las políticas y regulaciones legales y de la compañía.

En conclusión, el pentesting de un chatbot es esencial para garantizar la seguridad de los chatbot y protegerlos de ataques cibernéticos. Es importante llevar a cabo pruebas de intrusión periódicas para asegurar que los chatbot están protegidos contra posibles vulnerabilidades y debilidades. Es recomendable que el pentesting sea realizado por profesionales capacitados y con experiencia en seguridad informática, siguiendo las regulaciones legales y de la compañía.

3. Política de backups

Azure BackUp es una herramienta de Azure para la gestión de backups. Es escalable en función de las necesidades de almacenamiento y cuenta con una interfaz que facilita la definición de directivas de copias de seguridad y la protección de BBDD como SAP y SQL.

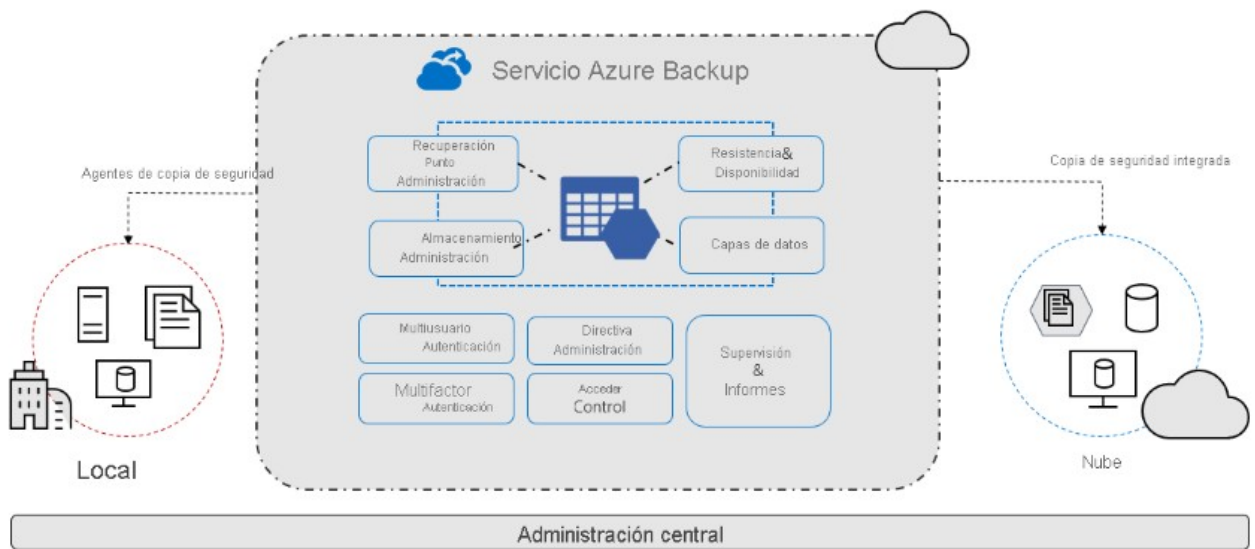
Algunas de las principales características de este servicio son las siguientes:

- Administración centralizada.
- Coherencia de aplicaciones: Con el Servicio de Instantáneas de Volumen (VSS) que permiten realizar copias de seguridad mientras las aplicaciones del sistema siguen escribiendo en esos volúmenes.

- Compatibilidad: Azure VM, servidores de entorno local, SQL Server, SAP HANA en instancias de Azure Virtual Machines, Azure Files y Azure Database for PostgreSQL
- Posibilidad de realizar informes de los backups.
- API, PowerShell y CLI de Azure para automatizar la configuración las directivas de copia de seguridad.
- Exporta datos de las copias de seguridad de la nube a tus propios sistemas de supervisión.

Con Azure Backup puedes hacer copia de:

- Entorno local: realice una copia de seguridad tanto de los archivos, como de las carpetas y del estado del sistema mediante el agente de Microsoft Azure Recovery Services (MARS). O bien, use el agente de DPM o de Azure Backup Server (MABS) para proteger las máquinas virtuales locales (Hyper-V y VMware) y otras cargas de trabajo locales.
- Máquinas virtuales de Azure realice copias de seguridad de máquinas virtuales Windows o Linux completas (mediante extensiones de copia de seguridad), o bien realice copias de seguridad de archivos, carpetas y estados del sistema mediante el agente de MARS.
- Azure Managed Disks Copia de seguridad de Azure Managed Disks.
- Recursos compartidos Azure Files Copia de seguridad de recursos compartidos de archivos de Azure en una cuenta de almacenamiento.
- SQL Server en máquinas virtuales de Azure haga copias de seguridad de las bases de datos de SQL Server que se ejecutan en las máquinas virtuales de Azure.
- Bases de datos de SAP HANA en máquinas virtuales de Azure_haga copias de seguridad de las bases de datos de SAP HANA que se ejecutan en las máquinas virtuales de Azure.
- Servidores de Azure Database for PostgreSQL - Copia de seguridad de bases de datos de Azure Database for PostgreSQL y conservación de estas durante un máximo de 10 años.
- Blobs de Azure



Opciones de almacenamiento duradero

- LRS (Almacenamiento de redundancia local) que copia los datos de forma sincrónica 3 veces dentro de una única ubicación física en la región primaria. Opción poco costosa pero no recomendable para alta disponibilidad o durabilidad.
- GRS los datos copiados de forma síncrona a través de LRS son copiados de forma asincrónica en una única ubicación física de una región secundaria que se encuentra a miles de kilómetros de distancia de la región primaria.

Protección Copias de Seguridad

- Control de acceso basado en rol (RBAC).
- Eliminación temporal que conserva las copias de seguridad hasta 14 días después de ser eliminadas.
- Protege los datos de ransomware habilitando la autenticación multiusuario.
- Claves administradas por clientes con cifrado AES de 256 bits.
- Puntos de conexión privados para la transferencia segura de copias de seguridad.

Reducción de costes

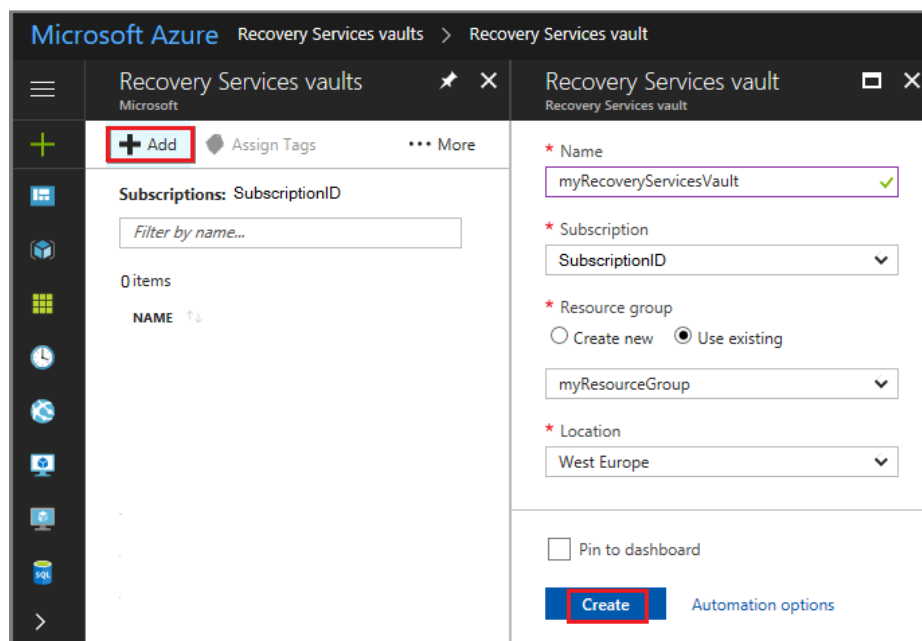
- Elimina los costes adicional de la infraestructura de copia de seguridad adicional y la carga de escalar y administrar el almacenamiento.

- informes de Backup para determinar el tamaño adecuado del almacenamiento de copia de seguridad.
- Puntos de recuperación al nivel de archivo para obtener un ahorro considerable en los costes de almacenamiento.
- Calculadora de precios para calcular los costes exactos.

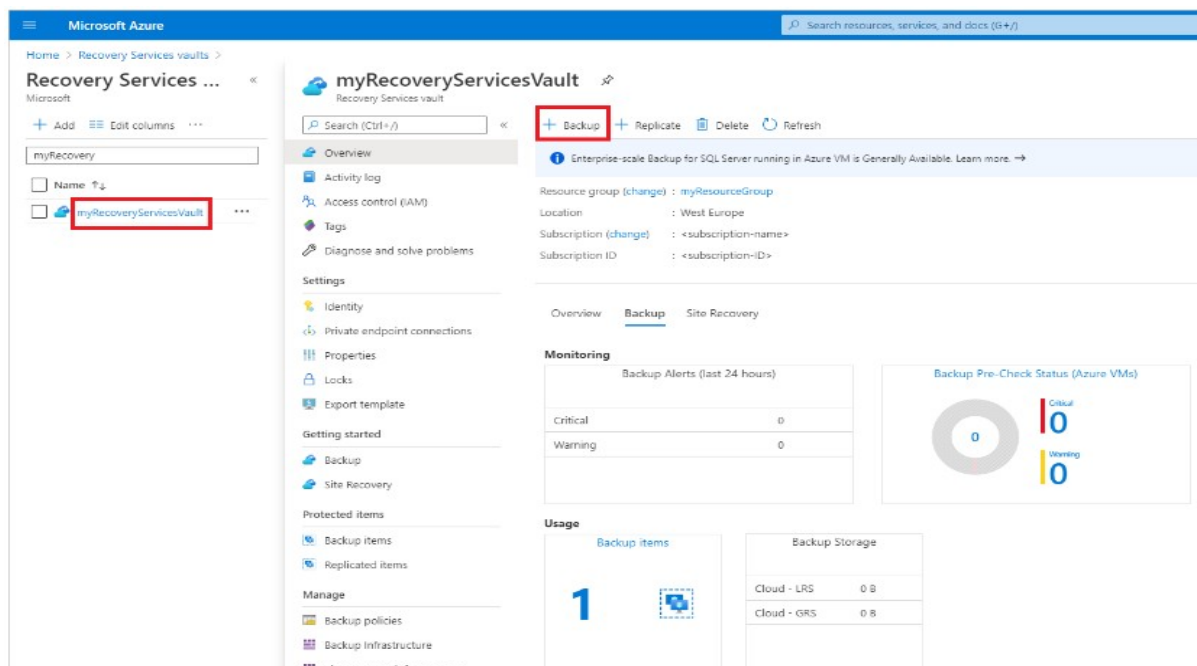
Ejemplo de creacion de un almacén de Recovery Services

Un almacén de Recovery Services contiene los datos y la directiva de la copia de seguridad.

Accedemos a través del menú a los servicios de recovery (podemos usar el buscador) y pulsamos +ADD y CREATE.

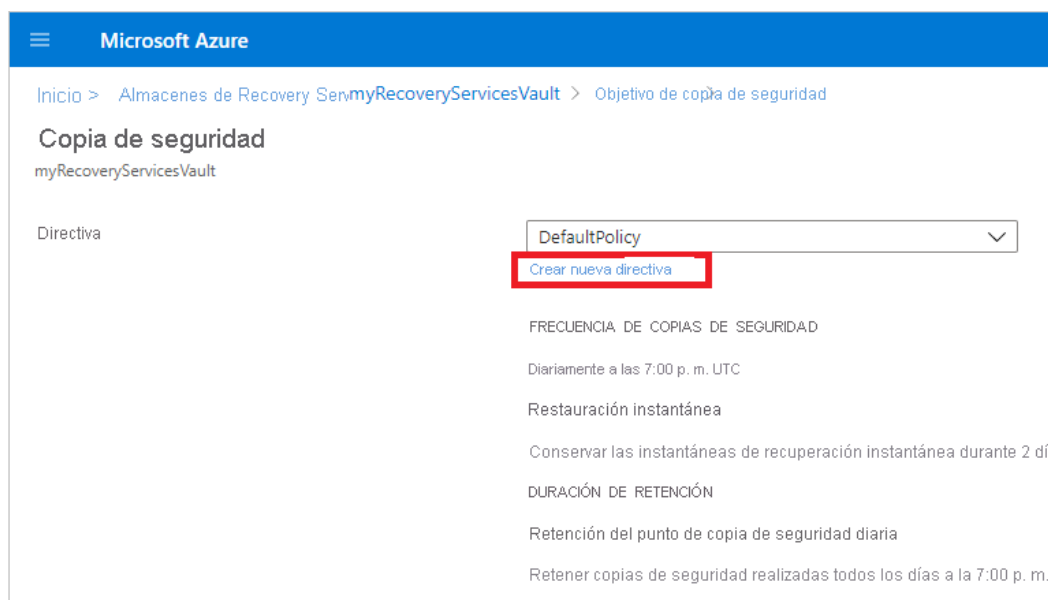


Posteriormente hay que establecer la directiva de copia de seguridad para proteger las máquinas virtuales. Esta directiva es la programación de la frecuencia y el momento de captura de los puntos de recuperación. La directiva también incluye el intervalo de retención de los puntos de recuperación:



Debemos de elegir dónde se ejecuta la carga de trabajo, en este caso Azure, y también de qué deseamos hacer la copia de seguridad. Los almacenes de Recovery Services tienen una directiva predeterminada que crea un punto de restauración al día y conserva los puntos de restauración durante 30 días.

A continuación elegimos crear una nueva directiva en el menú de copias de seguridad:



Tras esto, debemos dar valor a:

- Frecuencia de copia de seguridad
- Retención de punto de copia de seguridad diario
- Retención de punto de copia de seguridad semanal
- Retención de punto de seguridad anual

Backup policy

Policy name * ⓘ

Finance ✓

Backup schedule

Frequency *

Time *

Timezone *

Daily

3:30 AM

(UTC-06:00) Central Time (US & ...

Instant Restore ⓘ

Retain instant recovery snapshot(s) for

2 ✓

 Day(s) ⓘ

Retention range

☒ Retention of daily backup point.

At

For

3:30 AM

90 ✓

 Day(s)

☒ Retention of weekly backup point.

On *

At

For

Monday

3:30 AM

52 ✓

 Week(s)

☒ Retention of monthly backup point.

Week Based

Day Based

On *

Day *

At

For

First

Sunday

3:30 AM

36 ✓

 Month(s)

☐ Retention of yearly backup point.

Not Configured

Tras esto, una práctica conveniente sería realizar nuestra primera copia de seguridad:

Microsoft Azure

Search resources, services, and docs (G+/)

[Home](#) > [All resources](#) > [myRecoveryServicesVault | Backup items](#) >

Backup Items (Azure Virtual Machine)

myRecoveryServicesVault

Refresh

Add

Filter

i

Fetching data from service completed.

Filter items ...

Name	↑↓	Resource Group	↑↓	Backup Pre-Check	Last Backup Status	↑↓	Latest restore point	↑↓
myVM		myResourceGroup		✓ Passed	⚠ Warning(Initial back...			...
myVMH1		myResourceGroup		✓ Passed	⚠ Warning(Initial back...			...
myVMR1		myResourceGroup		✓ Passed	⚠ Warning(Initial back...			...

Seleccionamos Backup Now en el menú desplegable y esperamos que se complete el trabajo y nos muestra una fila como esta:

Inicio myRecoveryServicesVault | Elementos de copia de seguridad

Elementos de copia de seguridad (máquina virtual de Azure)

Almacén myRecoveryServices

Actualizar + Agregar Filtrar

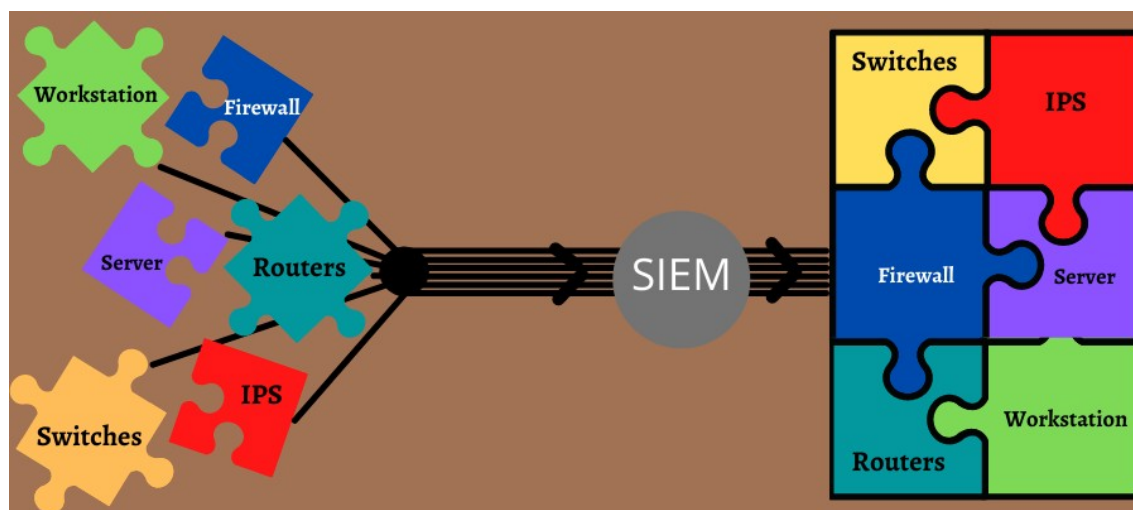
Se completó la captura de datos del servicio.

Filtrar elementos ...

Nombre	Grupo de recursos	Comprobación previa a la copia de seguridad	Estado de la última copia de seguridad	Punto de restauración	
myVlv	myResourceGroup	✓ Superado	✓ Correcto	7/26/2020, 4:23:25 PM	***

SIEM (en el Cloud de AZURE)

SIEM = Security Information and Event Manager



Es un software (conjunto de herramientas) que nos permite visualizar, de manera completa, la monitorización de las amenazas que afectan la seguridad informática de un Sistema. Permite centralizar toda la información con el fin de agilizar los protocolos de respuestas ante un ciberataque.

Azure tiene un Elastic SIEM, lo que significa que dispone de una herramienta de detección, investigación y respuesta a amenazas cambiantes. Aprovecha los datos a la escala y velocidad del Cloud. Aumenta el control y la visibilidad del host. Moderniza la seguridad con una solución de SIEM unificada y abierta.

Como primera aproximación, podríamos decir, que un SIEM debe realizar los siguientes controles críticos (definidos por la SANS.org) para que el funcionamiento del mismo sea efectivo:

1. Inventario de Autorizados y no autorizados en dispositivos: El SIEM debe utilizarse como base de datos de inventario de información sobre autorizaciones en activos. Pueden usar el conocimiento de la información de los

activos (ubicación, regulaciones, criticidad de los datos, etc.) para detectar y priorizar amenazas.

2. Inventario de Autorizados y no autorizados en aplicaciones: Al igual que en el control anterior, el SIEM debe usarse como base de datos de inventario de autorizados en aplicaciones, para la correlación con la red y la actividad de las mismas.

3. Configuraciones seguras: Las vulnerabilidades conocidas siguen siendo una vía principal para exploits exitosos. Si una herramienta automatizada de escaneo de dispositivos descubre un sistema de red mal configurado durante un escaneo de Enumeración de configuración común (CCE), ese error de configuración debe informarse o reflejarse en el SIEM, poniendo un mayor foco en dicho activo. Esto, nos ayudará a solucionar incidentes y a mejorar la postura de seguridad general.

4. Configuraciones seguras para dispositivos de red: Al igual que con el control 3, cualquier error de configuración en los dispositivos de red también debe reflejarse en el SIEM.

5. Defensa de fronteras: Las violaciones de las reglas de red, también deben informarse al SIEM para su correlación con los datos de inventario de autorizados anteriormente indicada, con el fin de controlar nuestros accesos.

6. Análisis de registros de auditoría: Es básicamente un control sobre los SIEM, que son el motor de análisis central que puede analizar los eventos de registro a medida que ocurren.

7. Seguridad del software de aplicación: Las vulnerabilidades que se descubren en las aplicaciones de software también se deben trasladar a los SIEM, con ello, podremos correlacionar la información con los datos de la red, capturados a través de registros, para determinar si las vulnerabilidades se están explotando en tiempo real.

8. Uso controlado de privilegios administrativos: Cuando no se cumplen los principios de este control, el SIEM puede correlacionar los registros de acceso para detectar la infracción y generar una alerta.

9. Acceso controlado según la necesidad de saber: El SIEM puede correlacionar la actividad del usuario con los derechos y los roles del usuario para detectar violaciones de mínimo privilegio en aplicaciones.

10. Evaluación y corrección continua de vulnerabilidades: El SIEM puede correlacionar el contexto de la vulnerabilidad con la actividad real del sistema para determinar si se están explotando las vulnerabilidades.

11. Seguimiento y control de cuentas: La actividad anormal de la cuenta solo se puede detectar cuando se compara con una línea de base de buena actividad conocida. El SIEM debe registrar la línea de base para cumplir con este control; y, a medida que se registren instantáneas o líneas de base futuras, se pueden comparar con la línea de base aprobada en el SIEM.

12. Defensa contra Malware: El malware que se descubra debe registrarse de acuerdo con este control. Las herramientas anti-malware centralizadas deben informar sus hallazgos al SIEM, quien correlacionará con los datos del sistema y las vulnerabilidades para determinar qué sistemas presentan un mayor riesgo debido al malware descubierto en ese sistema.

13. Limitación y control de puertos, protocolos y servicios de red: Los SIEM pueden monitorear los datos de registro para detectar el tráfico a través de puertos, protocolos y servicios restringidos. Las organizaciones pueden usar estos controles para determinar qué puertos y servicios son útiles para las empresas, cuáles no, y qué tipos de tráfico y puertos limitar.

14. Control de dispositivos inalámbricos: Las configuraciones erróneas del dispositivo y las intrusiones inalámbricas deben informarse a una base de datos central. Un SIEM consolida esta información y la utiliza para la correlación o detección de amenazas a la infraestructura inalámbrica.

15. Data Loss Prevention (DLP): Al igual que con el control 5, las violaciones de las reglas de pérdida de datos, también deben informarse a una fuente central, como un SIEM, que puede correlacionar los eventos de pérdida de datos con la información de inventario o activos, así como con otras actividades del sistema y del usuario para detectar violaciones complejas de datos sensibles.

Esquema de actuación del SIEM

El proceso se divide en 4 fases principales:

1. Fase de Recolección.
2. Fase de correlación.
3. Fase de almacenamiento.
4. Fase de reporting.

1. Fase de recolección

Empezaremos analizando los **INPUTS** que serán entre otros:

- 1. LOGS = registro oficial de eventos durante un rango de tiempo, que se emplea para registrar los datos o información sobre quién, qué, cuándo, dónde y por qué ocurre un evento. Para ello, vamos a utilizar Syslog** que es un estándar que utiliza los **puertos 514 TCP y UDP** (en caso de que esté cifrado usará puertos más altos) y que tiene diferentes partes que nos serán útiles (**prioridad; cabecera y texto**);
- 2. DLLs = archivos de bibliotecas: Contienen los recursos que una aplicación necesita para ejecutarse correctamente**, lo que puede incluir imágenes y/o una biblioteca de funciones ejecutables.)
- 3. DLPs (Data Loss Prevention) (principalmente para datos bancarios).**
- 4. SYSMON (para sistemas operativos Windows):** El monitor de sistema (SYSMON) es un servicio del sistema de Windows y un controlador de dispositivo que, una vez instalado en un sistema, permanece residente en los reinicios del sistema para supervisar y registrar la actividad del mismo, en el registro de evento de Windows, por lo que nos será útil a la hora de detectar posibles conexiones sospechosas o para malwares.

De estos inputs analizaremos los que nos puedan servir, de entre los muchos que tenemos. Los que nos van a ser útiles son los que tienen relación con:

- Los **datos de eventos**. Que se dividen en los siguientes:
 - Sistemas operativos.
 - Aplicaciones
 - BBDD (bases de datos)
 - Dispositivos
- Los **datos de contexto**.
 - Escáner de vulnerabilidades
 - Información de usuarios
 - Información de assets (activos, bienes)
 - Feeds de la inteligencia artificial.

Una vez analizados dichos “inputs”, los pasaremos al SIEM, que arrojará los siguientes “outputs”:

- Análisis
- Informes
- Monitorización

Para llevar a cabo la **recolección** de todos los datos necesarios para la securización, lo vamos a realizar de dos formas: **activa y pasiva**. Para no extendernos demasiado, elijo una opción en cada apartado. **Activa: Consultas BBDD. Pasiva: SYSLOG.**

En este apartado de la recolección, van a ser de suma importancia los Agentes = *pequeñas piezas de software que se van a poder instalar dentro de las propias fuentes o en las máquinas intermedias y son importantes para el SIEM porque realizan 5 tareas fundamentales que son:*

- **Parseo.**

Vamos a realizar un ***análisis del log*** teniendo en cuenta su:

- Timestamp
- IP de origen
- IP de destino
- Puerto de origen
- Puerto de destino, etc

Con ello vamos a interpretar los datos a través de las ***expresiones regulares***.

- **Normalización.**

En esta parte vamos a estandarizar los diferentes campos teniendo en cuenta: el fabricante, el formato y el campo “custom” de los diferentes fabricantes.

- **Categorización = poner una etiqueta a los logs.**

- **Agregación**

Por cuestiones económicas (principalmente) las empresas suelen agrupar los logs por eventos iguales (ej Timestamp).

- **Filtrado**

Muy importante hacer una selección de los logs para optimizar el rendimiento del SIEM y no sobrecargarlo con trabajo innecesario, así como para no colapsar el almacenamiento del servidor.

2. Fase de Correlación.

Aquí es donde se recogen los eventos de la etapa anterior.

Es un ***almacenamiento temporal (suele ser online)*** lo que significa que tiene ***un rotado muy rápido de logs***, para poder optimizar todas las búsquedas que haya que hacer en los análisis. También ***se generan*** los ***eventos de correlación (alarmas / notificaciones)***.

3. Fase de Almacenamiento.

Es donde se van a guardar los logs durante más tiempo y se va a encargar de toda la parte de Backups y de control de datos (sujetas a las diferentes normativas existentes que tenga que cumplir nuestro producto, en este caso la página web). Para hacernos una idea, a grandes rasgos debemos tener en cuenta:

- Tiempo determinado
- Rotado de logs a largo plazo (no debemos guardar cosas “antiguas” si no son necesarias).
- Accesibilidad
- Centralización
- Logs consultables (búsquedas y Reportes)
- Integridad de los datos almacenados.

Otras ***FUNCIONES ADICIONALES*** del SIEM van a ser:

- Análisis de fallos y simulación de exploits.
- Priorización de vulnerabilidades.
- Análisis y tipologías de red.
- Detección de anomalías de red.
- Gestión de incidentes.
- Control de usuarios.
- Normativa (SOX, PCI, HIPAA, RGDP, 27001)

4. Fase de Reporting centralizado (informes ejecutivos), que es muy importante ya que se trata demostrar nuestro trabajo, a nuestros “jefes” para que ellos entiendan el trabajo realizado, sin usar un lenguaje técnico.

En Recursos CRITICOS, nos vamos a centrar en aquellos sistemas a los que deberemos prestar especial atención (como por ejemplo cuando tratamos con ***datos médicos, datos bancarios, contenidos sexuales***, etc) que son entre otros, los siguientes:

- Servidores Legacy
- Sistemas SWITF (para los sistemas bancarios)

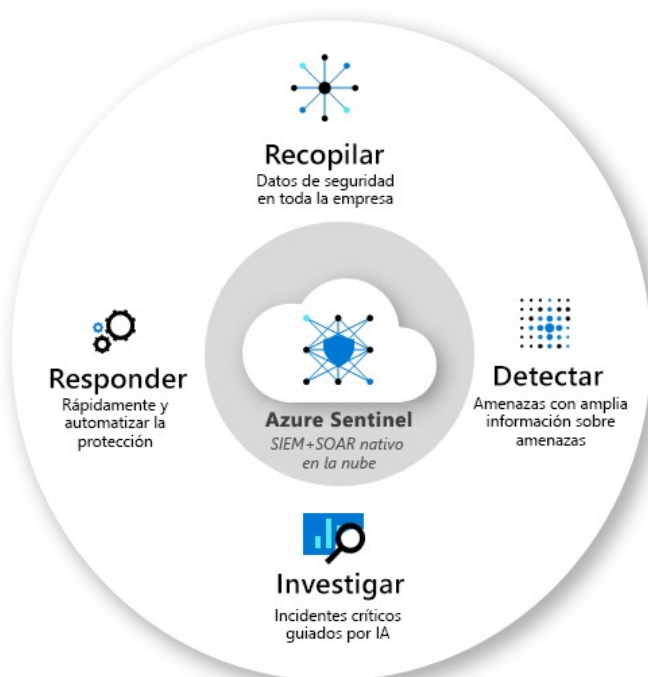
En concreto, Azure utiliza la herramienta **Azure Microsoft Sentinel**:

Es una solución escalable y nativa de la nube que proporciona:

- Administración de eventos e información de seguridad (SIEM).
- Respuesta automatizada de orquestación de seguridad (SOAR).

Microsoft Sentinel permite obtener una vista general de toda la empresa, lo que suaviza la tensión de ataques cada vez más sofisticados, volúmenes de alertas cada vez mayores y plazos de resolución largos.

- **Recopila datos a escala de nube** de todos los usuarios, dispositivos, aplicaciones y de toda la infraestructura, tanto en el entorno local como en diversas nubes.
- **Detecta amenazas que antes no se detectaban** y minimiza los falsos positivos mediante el análisis y la inteligencia sobre amenazas sin precedentes de Microsoft.
- **Investiga amenazas con inteligencia artificial** y busca actividades sospechosas a escala, aprovechando el trabajo de ciberseguridad que ha llevado a cabo Microsoft durante décadas.
- **Responde a los incidentes con rapidez** con la orquestación y la automatización de tareas comunes integradas.



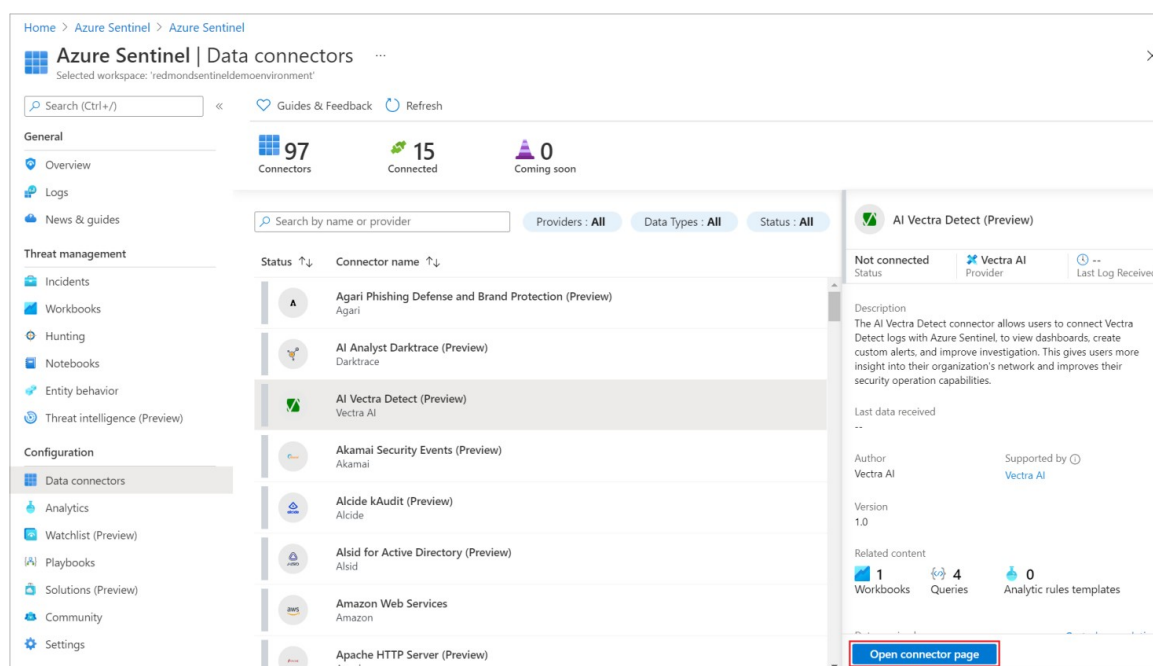
Microsoft Azure Sentinel incorpora de forma nativa servicios Azure contrastados, como Log Analytics y Logic Apps. Microsoft Sentinel enriquece la investigación y la detección con IA. Proporciona el flujo de inteligencia de amenazas de Microsoft y le permite usar su propia información sobre amenazas.

Recopilación de datos mediante conectores de datos

Para incorporar Microsoft Azure Sentinel, **primero debe conectarse a sus orígenes de datos**. Microsoft Sentinel incluye **varios conectores** para soluciones de Microsoft, que están disponibles inmediatamente y proporcionan integración en tiempo real. Algunos de estos conectores son:

- **Orígenes de Microsoft como Microsoft 365 Defender, Microsoft Defender for Cloud, Office 365, Microsoft Defender para IoT, etc.**
- **Orígenes de servicio de Azure, como Azure Active Directory, Actividad de Azure, Azure Storage, Azure Key Vault, Azure Kubernetes Service, etc.**

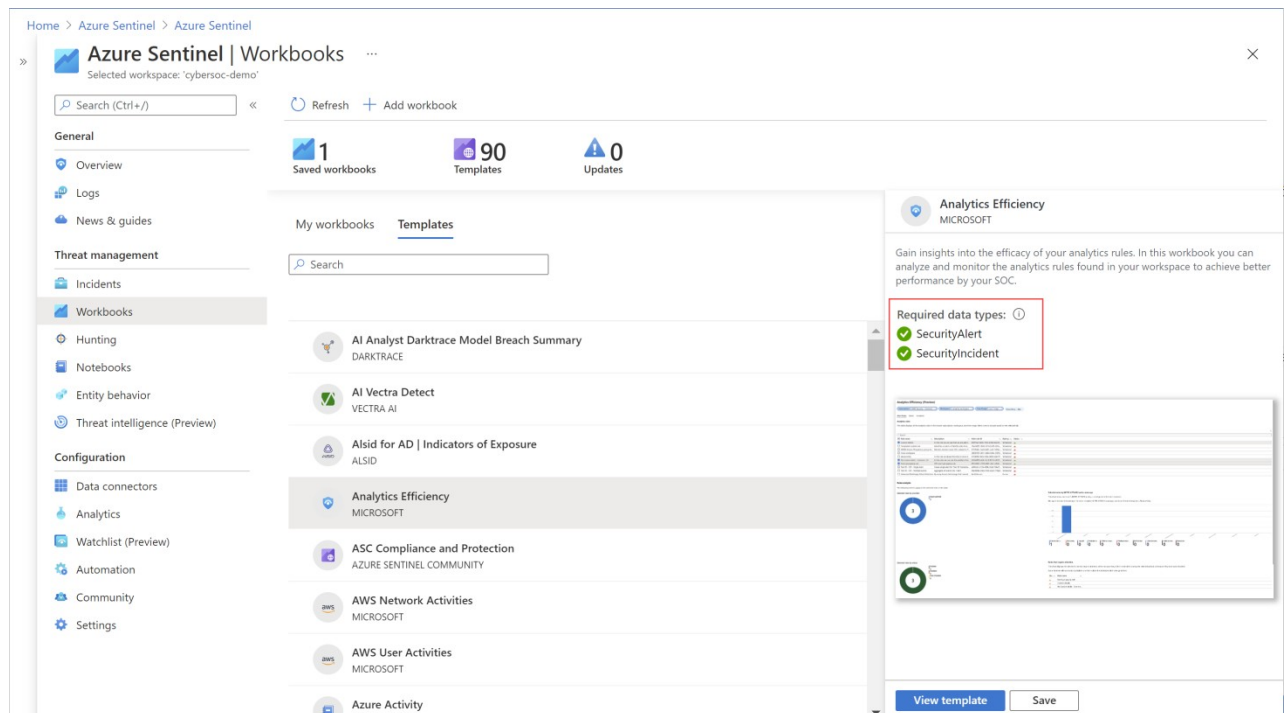
Microsoft Sentinel tiene conectores integrados para los ecosistemas de seguridad y aplicaciones más amplios para soluciones que no sean de Microsoft. También puede usar el formato de evento común, Syslog o la API de REST para conectar los orígenes de datos con Microsoft Sentinel.



Creación de informes interactivos mediante libros

Después de incorporarse a Microsoft Sentinel, supervise los datos mediante la integración con los libros de Azure Monitor.

Los libros se muestran de forma diferente en Microsoft Sentinel que en Azure Monitor. Pero puede resultar útil ver cómo crear un libro en Azure Monitor. Microsoft Sentinel le permite crear libros personalizados de todos los datos. Microsoft Sentinel también incluye plantillas de libro integradas que le permiten obtener rápidamente conclusiones sobre los datos en cuanto usted conecta un origen de datos.

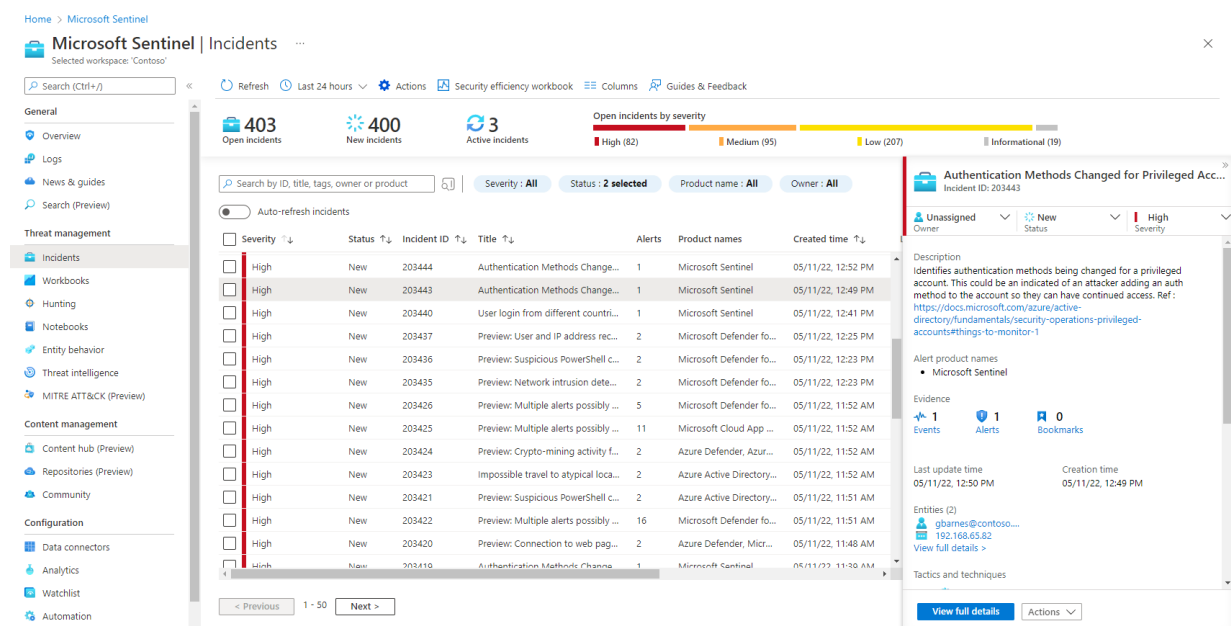


Los libros están diseñados para que los ingenieros y analistas de SOC de todos los niveles **visualicen los datos**. Los libros se usan mejor para vistas de alto nivel de datos Azure Sentinel y **no requieren ningún conocimiento de codificación**. Pero no se pueden integrar libros con datos externos.

Correlación de alertas en incidentes mediante reglas de análisis

Para reducir el ruido y minimizar el número de alertas que tiene que revisar e investigar, Microsoft Azure Sentinel usa **análisis para correlacionar las alertas con los incidentes**. Los incidentes son grupos de alertas relacionadas que, juntas, indican una posible amenaza procesable que se puede investigar y resolver. **Use las reglas de correlación integrada tal cual, o úselas como punto de partida para crear las suyas propias**. Microsoft Azure Sentinel también proporciona reglas de aprendizaje automático para asignar el comportamiento de red y buscar luego anomalías en los recursos. Estos análisis

conectan los puntos, al combinar alertas de baja fidelidad sobre distintas entidades en posibles incidentes de seguridad de alta fidelidad.



Automatización y orquestación de tareas comunes mediante cuadernos de estrategias

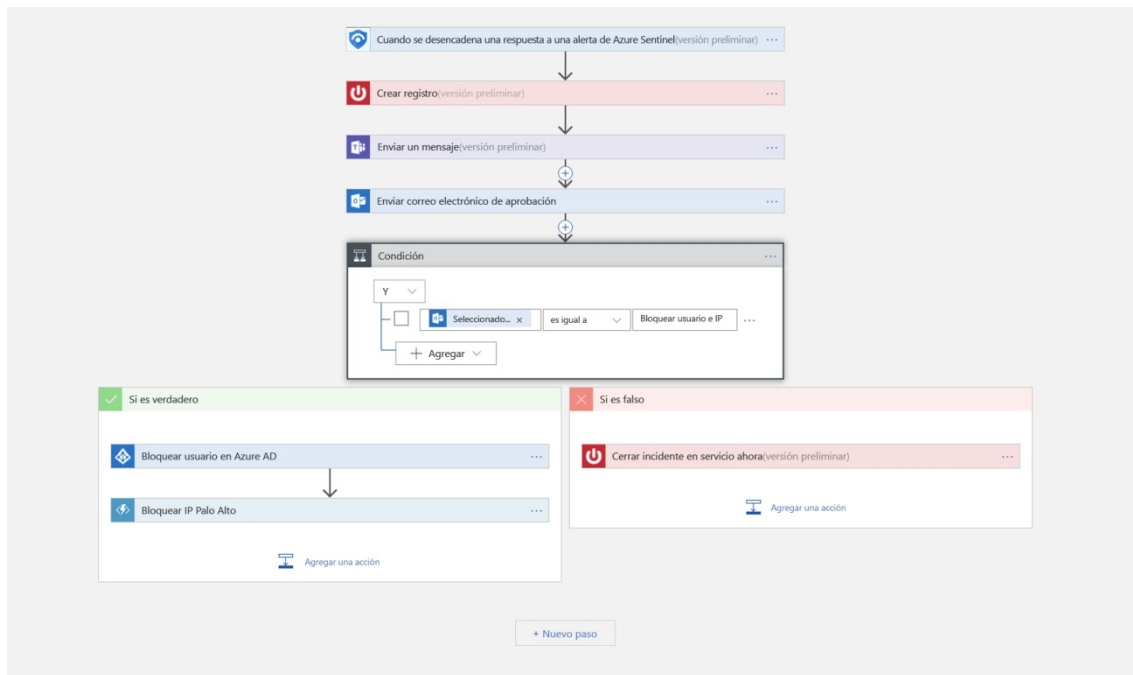
Automatice las tareas comunes y simplifique la orquestación de la seguridad con cuadernos de estrategias que se integran con los servicios de Azure y las herramientas existentes.

La solución de automatización y orquestación de Microsoft Azure Sentinel proporciona una arquitectura muy extensible que permite una **automatización escalable a medida que emergen nuevas tecnologías y amenazas**. Para crear cuadernos de estrategias con **Azure Logic Apps**, puede elegir de una galería creciente de cuadernos de estrategias integrados. Estos incluyen más de 200 conectores para servicios, como Azure Functions. Los conectores permiten aplicar cualquier lógica personalizada en código como:

- ServiceNow
- Jira
- Zendesk
- Solicitudes HTTP
- Microsoft Teams

- Slack
- ATP de Windows Defender
- Defender para aplicaciones en la nube

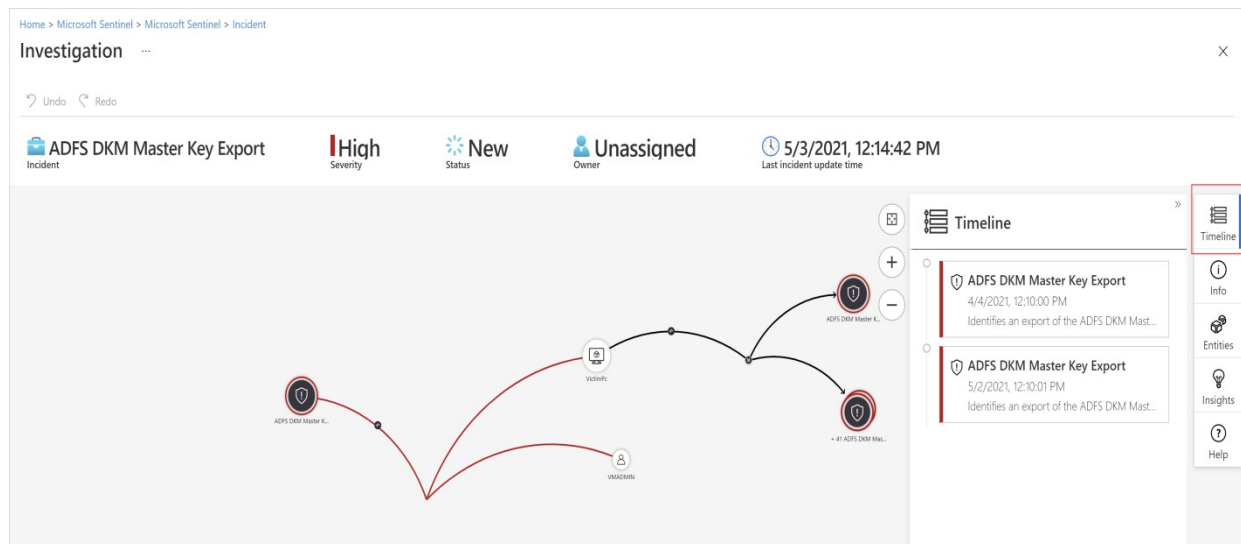
Por ejemplo, si usa el sistema de vales de ServiceNow, use Azure Logic Apps para automatizar los flujos de trabajo y abrir un vale en ServiceNow cada vez que se genera una alerta o incidente determinados.



Los cuadernos de estrategias son más adecuados para tareas únicas y repetibles, y no requieren ningún conocimiento de codificación. Los cuadernos de reproducción no son adecuados para cadenas de tareas ad hoc o complejas, ni para documentar y compartir evidencias.

Investigar el ámbito y la causa principal de las amenazas de seguridad

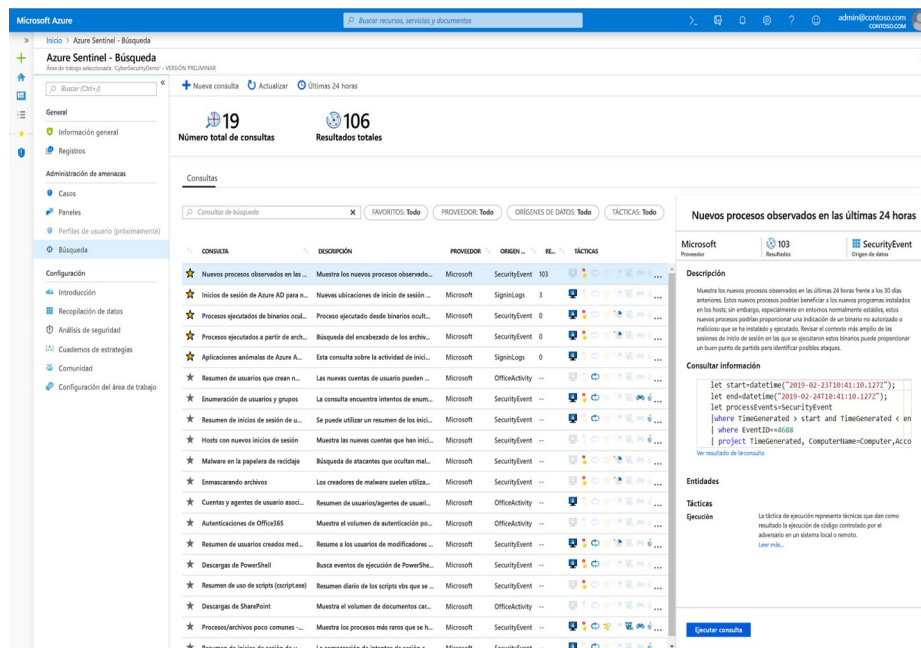
Las herramientas de investigación profunda de Microsoft Sentinel le ayudan a comprender el ámbito y a encontrar la causa principal de una posible amenaza de seguridad. Puede elegir una entidad en el gráfico interactivo para hacer preguntas interesantes sobre ella y explorar en profundidad esa entidad y sus conexiones para llegar a la causa principal de la amenaza.



Búsqueda de amenazas de seguridad mediante consultas integradas

Use las eficaces **herramientas de búsqueda y consulta** de Microsoft Azure Sentinel, **basadas en el marco MITRE**, que le permiten buscar de forma proactiva amenazas de seguridad en todos los orígenes de datos de la organización, antes de que se desencadene una alerta. **Cree reglas de detección personalizadas** basadas en la consulta de búsqueda. A continuación, **muestre esas conclusiones como alertas a los responsables de incidentes de seguridad**.

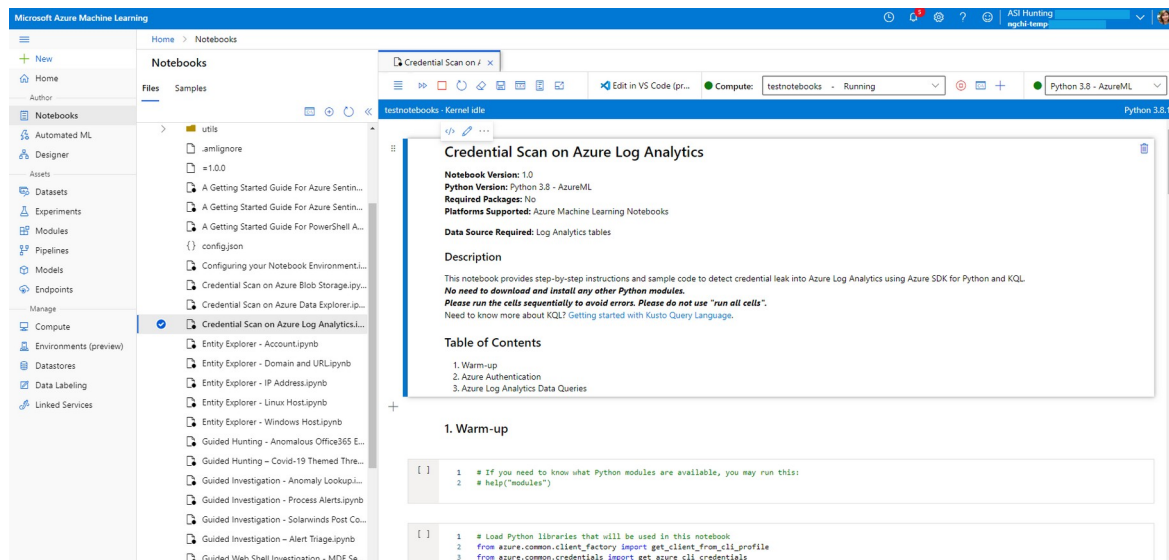
Durante la búsqueda, **cree marcadores para volver a eventos interesantes** más adelante. Use un marcador para compartir un evento con otros usuarios. O bien, **agrupe eventos** con otros eventos relacionados para crear un incidente atractivo para la investigación.



Mejora de la búsqueda de amenazas con cuadernos

Microsoft Azure Sentinel admite cuadernos de Jupyter en áreas de trabajo de Azure Machine Learning, incluidas las bibliotecas completas para el aprendizaje automático, la visualización y el análisis de datos. Use cuadernos en Microsoft Azure Sentinel para ampliar el ámbito de lo que puede hacer con los datos de Microsoft Azure Sentinel. Por ejemplo:

- Realizar análisis que no están integrados en Microsoft Sentinel, como algunas características de aprendizaje automático de Python.
- Crear visualizaciones de datos que no están integradas en Microsoft Sentinel, como escalas de tiempo personalizadas y árboles de proceso.
- Integrar orígenes de datos fuera de Microsoft Sentinel, como un conjunto de datos local.



Los cuadernos están destinados a buscadores de amenazas o analistas de nivel 2 y 3, investigadores de incidentes, científicos de datos e investigadores de seguridad. **Requieren una curva de aprendizaje más alta y conocimientos de codificación.** Tienen compatibilidad limitada con la automatización.

Los cuadernos de Microsoft Sentinel proporcionan:

- **Consultas tanto a Microsoft Sentinel como a datos externos.**
- **Características para el enriquecimiento de datos, la investigación, la visualización, la búsqueda, el aprendizaje automático y el análisis de macrodatos.**

Los cuadernos son los más adecuados para:

- Cadenas de tareas repetibles más complejas
- Controles de procedimientos ad hoc
- Aprendizaje automático y análisis personalizado

Los cuadernos admiten bibliotecas enriquecidas de Python para manipular y visualizar datos. Son útiles para documentar y compartir evidencias de análisis.

[Descarga del contenido de seguridad de la comunidad](#)

La comunidad Microsoft Azure Sentinel es un recurso muy eficaz para la detección y la automatización de amenazas. Nuestros analistas de seguridad de Microsoft crean y agregan nuevos libros, cuadernos de estrategias, consultas de búsqueda,

etc. Publican estos elementos de contenido en la comunidad para que los use en su entorno. Puede descargar contenido de ejemplo del repositorio de GitHub privado de la comunidad con el fin de crear libros, consultas de búsqueda, cuadernos y cuadernos de estrategias personalizados para Microsoft Sentinel.

Buscar o saltar a...

Solicitudes de incorporación de cambios Problemas Marketplace Explorar

Azure / Azure Sentinel

Sin inspección 27 Estrella 15 Bifurcación 4

Código Problemas 0 Solicitudes de incorporación de cambios 2 Proyectos 0 Wiki Insights Configuración

Sin descripción o sitio web proporcionado. Editar

sample-code cybersecurity Administrar temas

299 confirmaciones 67 ramas 0 versiones 19 colaboradores MIT

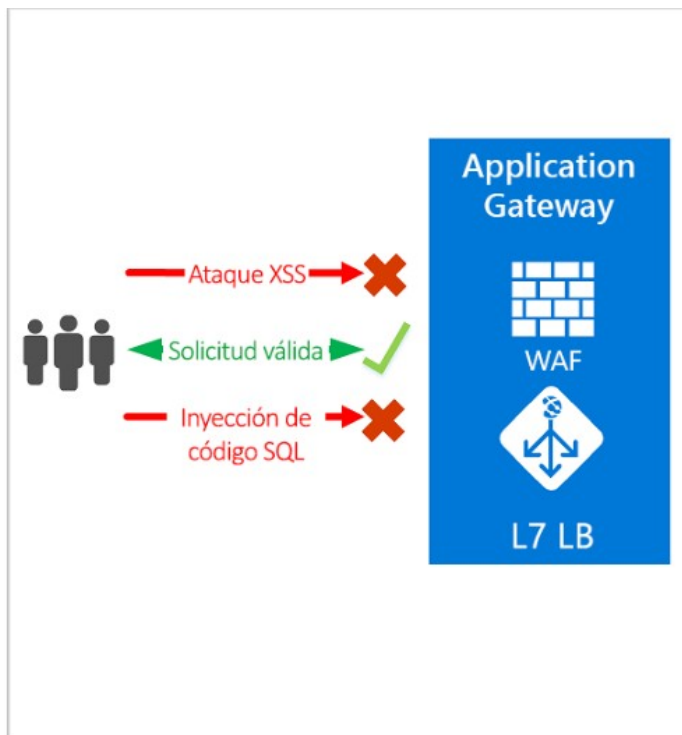
Rama: principal Nueva solicitud de incorporación de cambios Crear archivo Cargar archivos Buscar archivo Clonar o descargar

File	Commit	Time
zhzhao8888 Title font	Latest commit e76986d	2 days ago
.github/ISSUE_TEMPLATE	Update issue templates	2 months ago
Alert Rules	Add files via upload	6 months ago
Dashboards	exchange logo path	3 days ago
Detections	Merge pull request #41 from Azure/SignInLogs_Aprakash_Feb11	3 days ago
Exploration Queries	Committing File entities	5 days ago
Functions	folder restructure for hunting queries, exploration queries, and build...	a month ago
Hunting Queries	updated hunting script	2 days ago
Notebooks	Title font	2 days ago
Parsers	Create Readme	6 months ago
Playbooks	Create ReadMe	5 days ago
QueryLanguageSamples	Adding current items (#11)	a month ago
docs	Adding current items (#11)	a month ago
.gitignore	Initial commit	6 months ago
CODEOWNERS	Add files via upload	2 months ago

WAF UTILIZADO PARA AZURE

Un WAF es un firewall diseñado específicamente para aplicaciones web. Se encarga de analizar las peticiones enviadas al servidor, y en el caso de que no cumplan con las reglas establecidas por el administrador, corta el tráfico. El principal objetivo es protegerse contra los ataques más comunes, como el SQL Injection y el XSS entre otros.

En concreto, Azure dispone de un servicio de WAF nativo de la nube que ofrece protección para los 10 riesgos de seguridad principales recogido en OWASP top 10 (explicado anteriormente). La herramienta se puede activar fácilmente y se basa en un modelo de pago por uso:



Reglas y directiva de WAF

La herramienta posee una serie de reglas pre configuradas y administradas por Azure, pero también pone a la disposición del usuario la creación de reglas personalizadas que se aplican antes (tienen una prioridad superior a las preestablecidas).

Una regla está formada por una condición de coincidencia, una prioridad y una acción. Los tipos de acción que se admiten son los siguientes: PERMITIR, BLOQUEAR y REGISTRAR. Puede crear una directiva totalmente personalizada que cumpla sus requisitos específicos de protección de aplicaciones combinando reglas personalizadas y administradas.

El orden de prioridad se establece a través de un número entero de la misma forma que se hace en otros WAF. Se evalúan los criterios de coincidencia según el orden, y al coincidir se aplica la acción (los siguientes criterios quedarían sin evaluar).

En el siguiente enlace se pueden ver los distintos conjuntos de reglas que se le pueden aplicar a la herramienta:

<https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=owasp32>

En cuanto a los precios del servicio, vemos que se cobra un valor fijo en función de las horas que tenemos el WAF activo:

Azure WAF con Application Gateway v1

Cobramos por las puertas de enlace de aplicaciones en función de la cantidad de tiempo que la puerta de enlace esté aprovisionada y disponible para las puertas de enlace de aplicaciones. Consulte la página de [precios](#) de Azure Application Gateway para obtener más información sobre WAF.

Tipo de Application Gateway	Application Gateway de firewall de aplicaciones web
Pequeña	No disponible
Mediana	\$0,126 por hora de puerta de enlace (~\$91,98/mes)
Grande	\$0,448 por hora de puerta de enlace (~\$327,04/mes)

Azure WAF con Application Gateway v2

Azure Application Gateway SKU de WAF v2 ofrece compatibilidad con el escalado automático, la redundancia de zona y la VIP estática. Estas puertas ofrecen rendimiento optimizado, mejor aprovisionamiento y tiempo de actualización de la configuración, reescrituras de encabezados y reglas personalizadas. Consulte [precios](#) de Azure Application Gateway para más detalles sobre SKU que no sean WAF y la [documentación](#) para más detalles sobre el producto. Consulte a continuación para obtener información sobre precios y facturación.

	Application Gateway de firewall de aplicaciones web
Fijo	\$0,443 por hora de puerta de enlace
Unidad de capacidad ¹	\$0,0144 por hora de unidad de capacidad

Así como otras cantidades variables en función de la cantidad de datos procesados:

Procesamiento de datos

El procesamiento de datos se factura por la cantidad de datos que las instancias de Application Gateway procesan.

Procesamiento de datos	Precio
Pequeña	
Ilimitado	\$0,008 por GB al mes

Si los datos no superan los 10 TB al mes, no se considera una cantidad elevada de datos, y se cobra a 0,008\$ el GB, que dado las características de la web, y que está destinada a una región geográfica específica, es bastante probable que no se

alcance ese volumen de datos. Cada paquete procesado se considera que tiene un tamaño de 2KB aunque realmente sea de tamaño inferior.

Teniendo en cuenta todo esto y en función de si se utiliza Application Gateway V1 o V2, el coste por tener el WAF activo todos los días sería de entre 150\$ y 350\$ al mes.

Como alternativa, se podría implementar un WAF de código abierto como ModSecurity en una máquina virtual y desplegarla en Azure.

MFA (MULTIFACTOR AUTHENTICATION) AUTENTICACIÓN DE MÚLTIPLES FACTORES

Hay muchos métodos que se pueden usar para la autenticación de segundo factor. Hay una gran variedad donde seleccionar, por ello los escogeremos según: nivel de seguridad, facilidad de uso y disponibilidad.

Los distintos métodos de autenticación son:

- Microsoft Authenticator Configuración MFA o política de método de autenticación.
- Claves de seguridad FIDO2 Directiva de métodos de autenticación.
- Tokens OATH de software o hardware Configuración de MFA
- Verificación de SMS Configuración de MFA, administrar el inicio de sesión de SMS para la autenticación principal en la política de autenticación.
- Políticas de llamadas de voz Métodos de autenticación.

La autenticación multifactor de Azure AD se aplica mediante políticas de acceso condicional. Estas políticas le permiten solicitar MFA a los usuarios cuando sea necesario por razones de seguridad y permanecer inactivas cuando no sea necesario.

En Azure Portal, se pueden configurar las políticas de acceso condicional en Azure Active Directory > Security > Access Conditional.

Políticas comunes para la autenticación multifactor de Azure AD:

Los casos de uso comunes que requieren la autenticación multifactor de Azure AD incluyen:

- Para administradores
- Para aplicaciones específicas
- A todos los usuarios

- Para la administración de Azure
- Desde ubicaciones de red que no son de confianza

Hay algunos campos, en los que se puede planificar la duración de los usuarios. Al planificar la implementación de la autenticación multifactor, es importante pensar en la frecuencia con la que desea solicitar a los usuarios. Solicitar a los usuarios las credenciales a menudo parece algo sensato, pero puede tener sus inconvenientes. Si los usuarios están capacitados para escribir sus credenciales sin pensar, es posible que las proporcionen sin darse cuenta ante una solicitud de credenciales maliciosa. Azure AD tiene varias configuraciones que determinan la frecuencia con la que necesita autenticarse. Sea consciente de las necesidades tanto del negocio como de los usuarios y realice las configuraciones que proporcionen el mejor equilibrio para su entorno.

Recomendamos usar dispositivos con tokens de actualización primaria (PRT) para mejorar la experiencia del usuario final y reducir la duración de la sesión con la política de frecuencia de inicio de sesión solo para casos de uso comercial específicos.

Sanitizar entradas

Una de los principales ataques que podría sufrir nuestra aplicación, sería la inyección de código, como hemos visto anteriormente. Una forma de intentar evitar este tipo de ataques, sería a través de la sanitización de los posibles caracteres de entrada que son permitidos:

Sanitizar es el proceso de limpiar o filtrar los datos de entrada para evitar ataques maliciosos. Cuando rellenamos un formulario en una web, los datos que ingresamos pueden ser recolectados y procesados por el servidor. Sin embargo, si no se toman medidas de seguridad adecuadas, es posible que los datos recolectados sean vulnerables a ataques como la inyección SQL, la inyección de scripts, command and control o la suplantación de identidad.

Para securizar un formulario en una web, se deben tomar varias medidas de seguridad. Algunas de las medidas más importantes incluyen:

- Validación de entrada: validar los datos de entrada en el lado del cliente y en el lado del servidor para asegurarse de que los datos cumplen con los requisitos esperados.
- Sanitización de entrada: limpiar los datos de entrada para eliminar cualquier caracteres no deseados o peligrosos.
- Uso de protocolos seguros: utilizar HTTPS para asegurar que la información transmitida entre el cliente y el servidor está encriptada.
- Autenticación y autorización: asegurar que solo los usuarios autorizados con un captcha puedan enviar datos al formulario.
- Límite de intentos: limitar el número de intentos que un usuario puede realizar para enviar el formulario.
- No guardar datos sensibles: No guardar datos sensibles en el servidor.

Hay varias formas de sanitizar la entrada de caracteres en un chatbot. Una forma es utilizando librerías de sanitización de entrada como OWASP, las cuales proporcionan métodos para limpiar y validar los datos de entrada. Otra forma es usar expresiones regulares para filtrar caracteres no deseados o peligrosos. También es importante validar la entrada del usuario para asegurar que solo se permiten caracteres esperados y de acuerdo al contexto. Además, se pueden aplicar medidas de seguridad adicionales como la autenticación y autorización de usuarios para evitar ataques maliciosos.

Al sanitizar un formulario de correo, es recomendable evitar los siguientes caracteres:

- Caracteres de nueva línea (`\r`, `\n`): estos caracteres pueden ser utilizados para insertar un salto de línea en el cuerpo del correo, lo cual podría dar lugar a un ataque de inyección de código.
- Caracteres de separación de línea (`\r\n`): estos caracteres pueden ser utilizados para insertar un salto de línea en el encabezado del correo, lo cual podría dar lugar a un ataque de inyección de encabezado.
- Caracteres especiales como `<`, `>`, `/`, `,`, `(`, `)`, `&`, `#`, `%`, `;`, `:`, `"`: estos caracteres pueden ser utilizados para inyectar código malicioso en el formulario.

- Caracteres de scripts como <script>, <iframe>, <object> : estos caracteres pueden ser utilizados para insertar scripts maliciosos en el cuerpo del correo.
- También es recomendable sanitizar cualquier otro caracter que no sea alfanumerico y que no sea necesario para el envio del correo.

Hasta ahora, la información que se ha facilitado y recabado ha sido basada en la utilización de Microsoft Azure para desplegar la aplicación que hemos desarrollado, pero, viendo que desde Ciberseguridad no teníamos acceso a la aplicación para realizar ningún tipo de comprobaciones prácticas, se ha decidido ejemplificar la creación del entorno en el que se desplegaría la aplicación en el caso de realizarlo de forma local.

En este caso, se ha decidido utilizar una máquina Ubuntu Server. Se ha realizado la instalación y se ha comenzado a realizar el hardening y configuración de la misma.

El enlace desde el que se ha descargado es el siguiente:
<https://ubuntu.com/download/server>

Get Ubuntu Server

Option 1: Manual server installation

USB or DVD image based physical install

- ✓ OS security guaranteed until April 2027
- ✓ Extended security maintenance until April 2032
- ✓ Commercial support for enterprise customers

[Download Ubuntu Server 22.04.1 LTS](#)

[Alternative downloads ›](#)

[Alternative architectures ›](#)

Utilizaremos una Ubuntu Server 22.04.1 LTS (para asegurarnos el soporte hasta abril de 2027) descargada de la página web oficial.

En un primer paso verificamos el hash del archivo descargado para comprobar la integridad del mismo utilizando el algoritmo SHA256:

Run this command in your terminal in the directory the iso was downloaded to verify the SHA256 checksum:

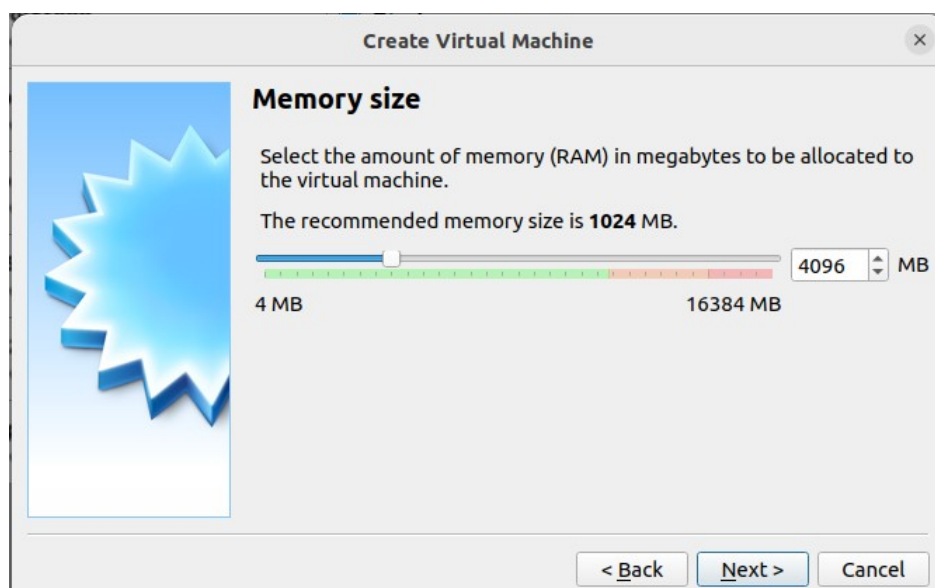
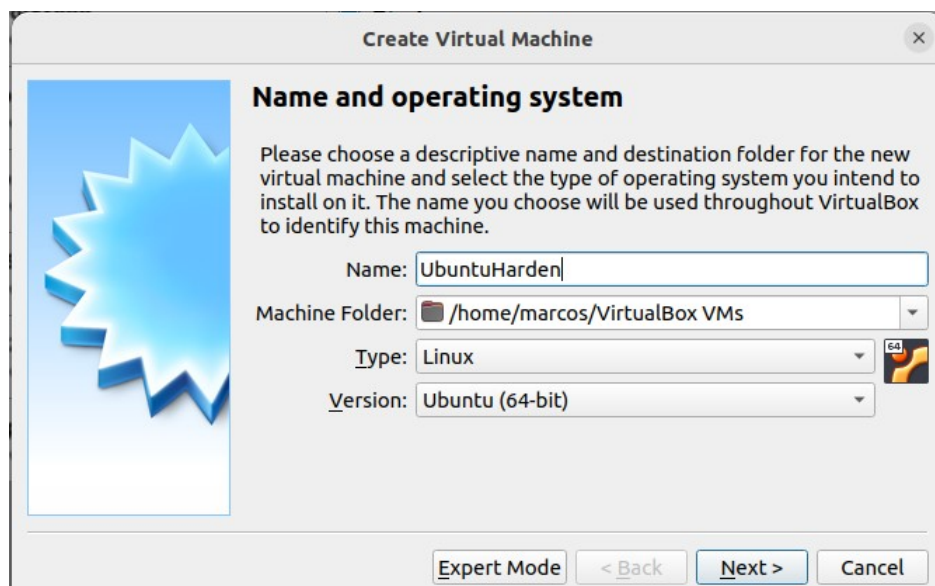
```
echo
"10f19c5b2b8d6db711582e0e27f5116296c34fe4b313ba45f9b201a50070
56cb *ubuntu-22.04.1-live-server-amd64.iso" | shasum -a 256 -
-check
```

You should get the following output:

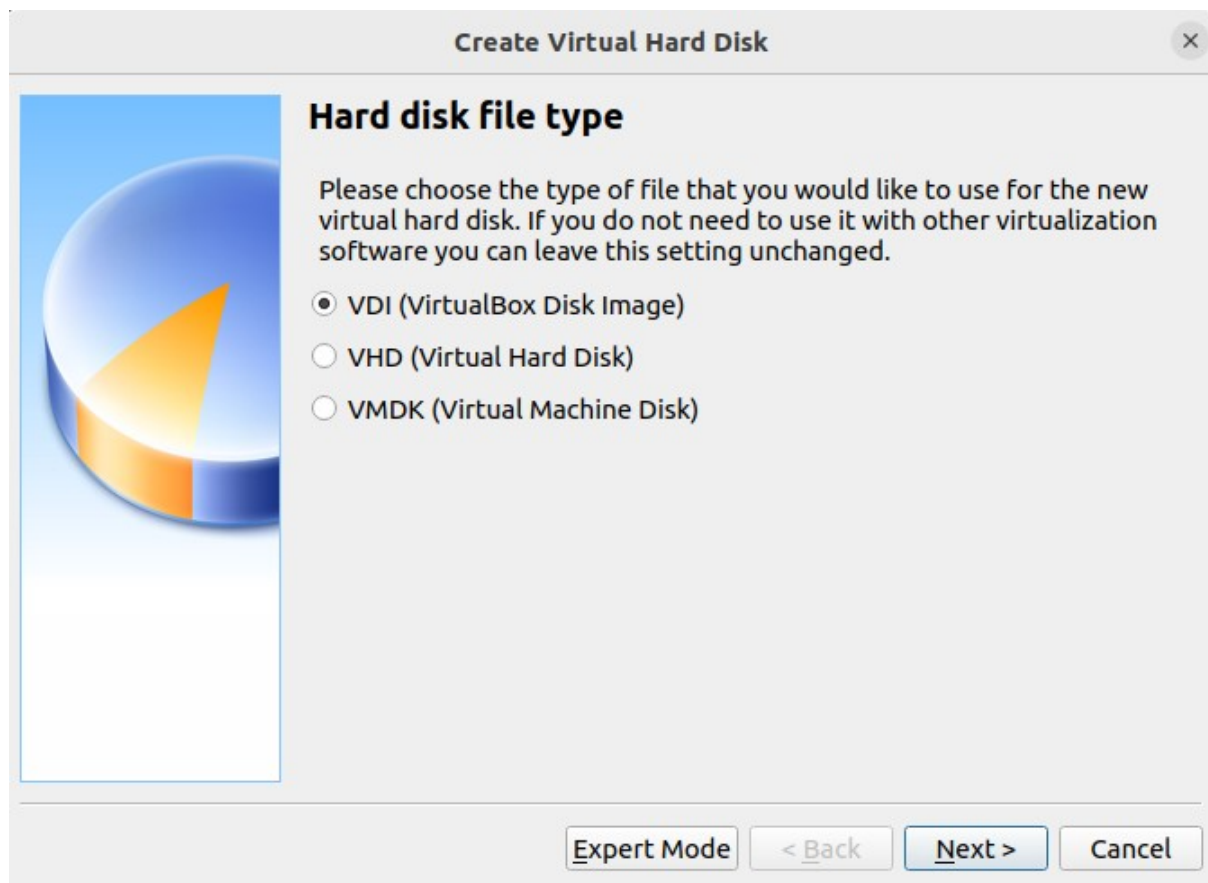
```
ubuntu-22.04.1-live-server-amd64.iso: OK
```

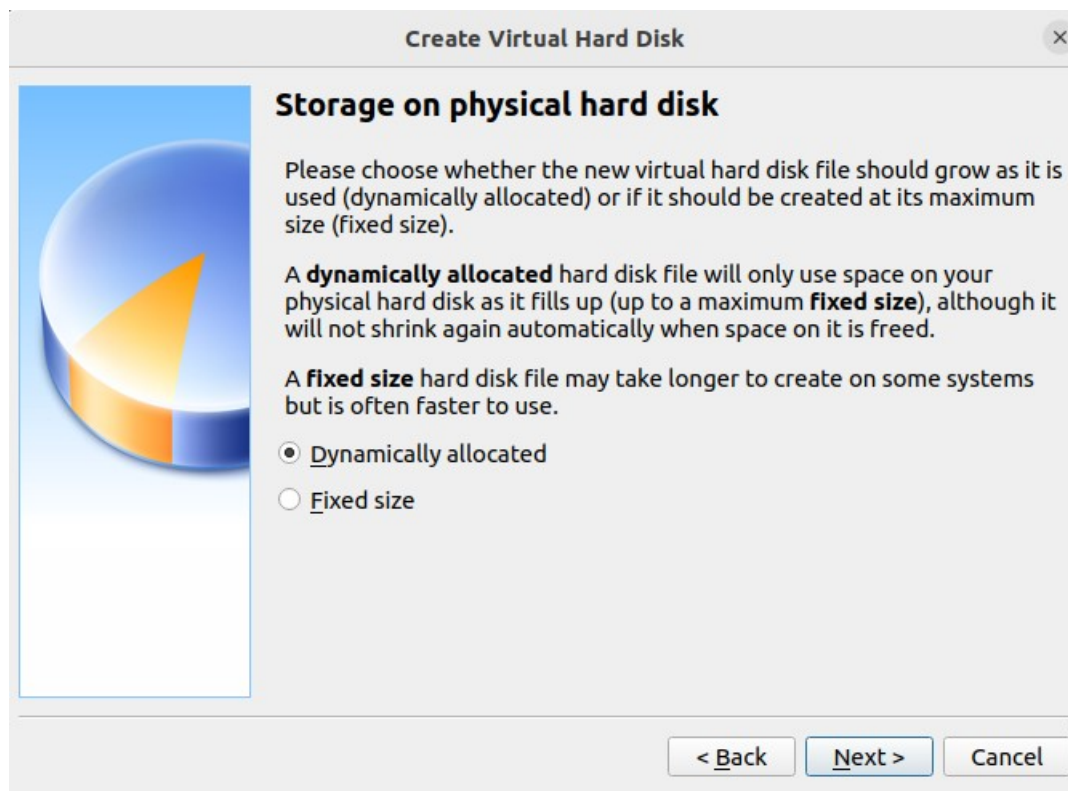
```
marcos@marcos-GL62M-7REX:~/Downloads$ echo "10f19c5b2b8d6db711582e0e27f5116296c3
4fe4b313ba45f9b201a5007056cb *ubuntu-22.04.1-live-server-amd64.iso" | shasum -a
256 --check
ubuntu-22.04.1-live-server-amd64.iso: OK
```

Tras la comprobación del hash procedemos a la instalación de la máquina:

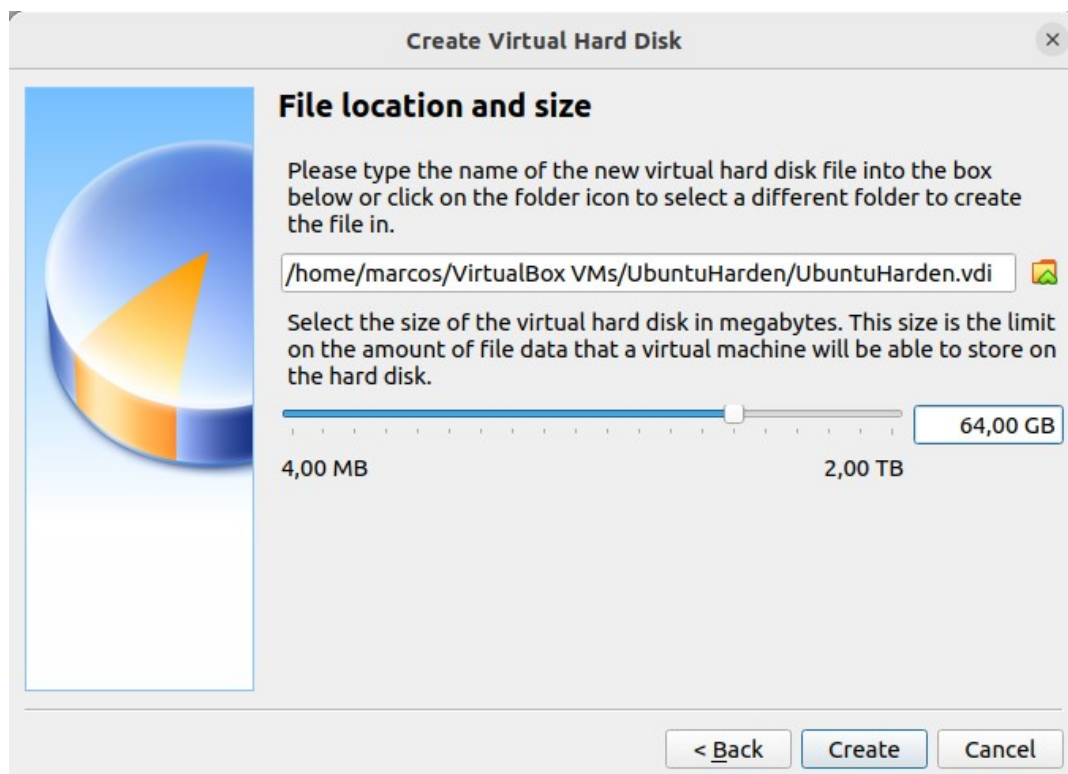


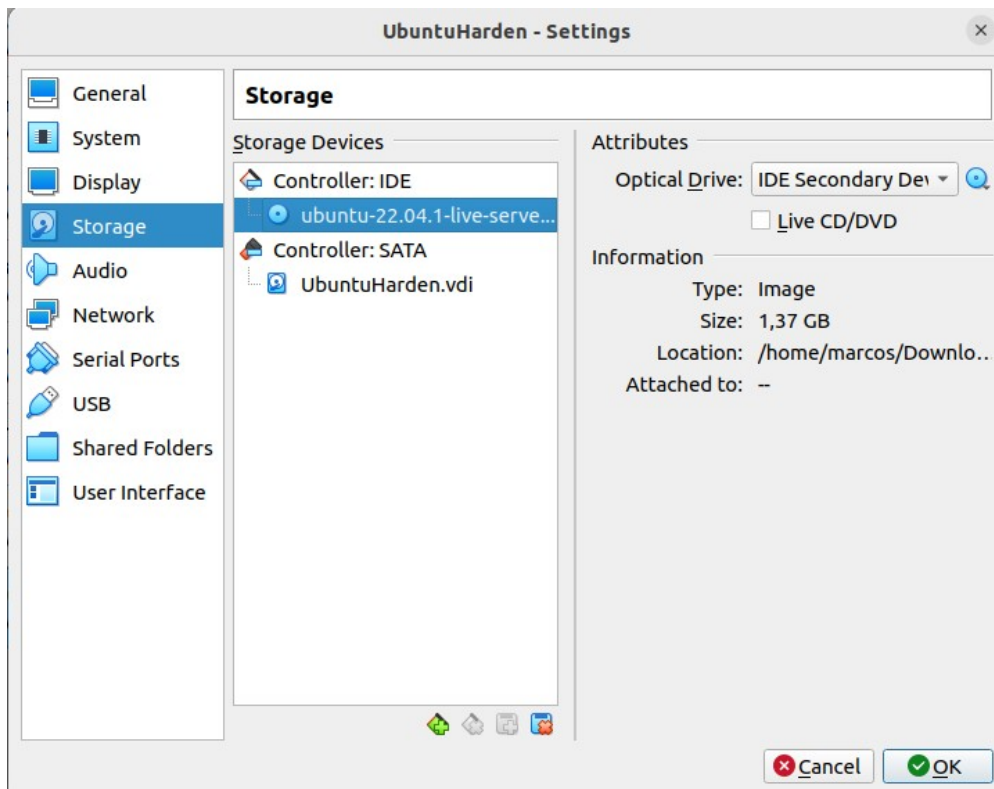
Le asignaremos en principio 4GB de RAM, al ser una MV esto podremos modificarlo posteriormente en función de las necesidades del sistema. En principio esta máquina alojará un servidor web y se harán copias de de esta ya hardenizada para almacenar los logs y distintas aplicaciones necesarias para la seguridad.



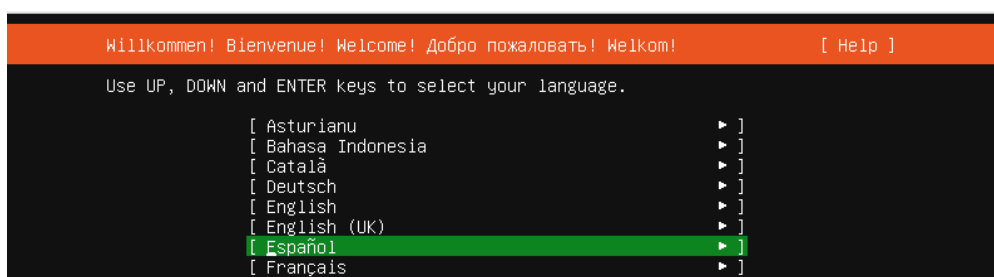
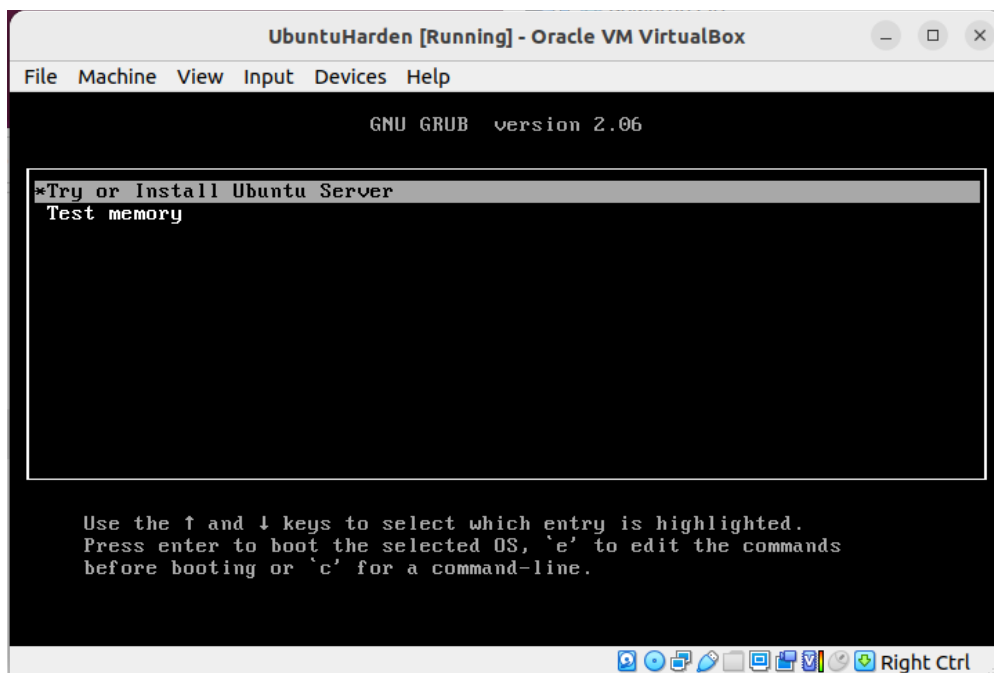


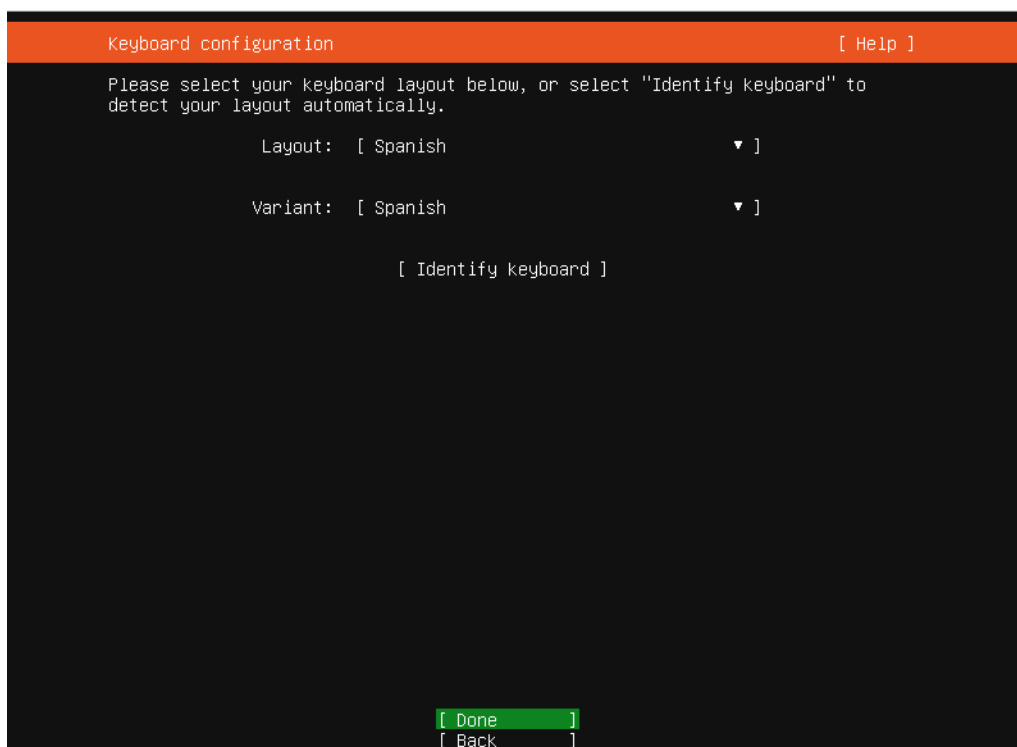
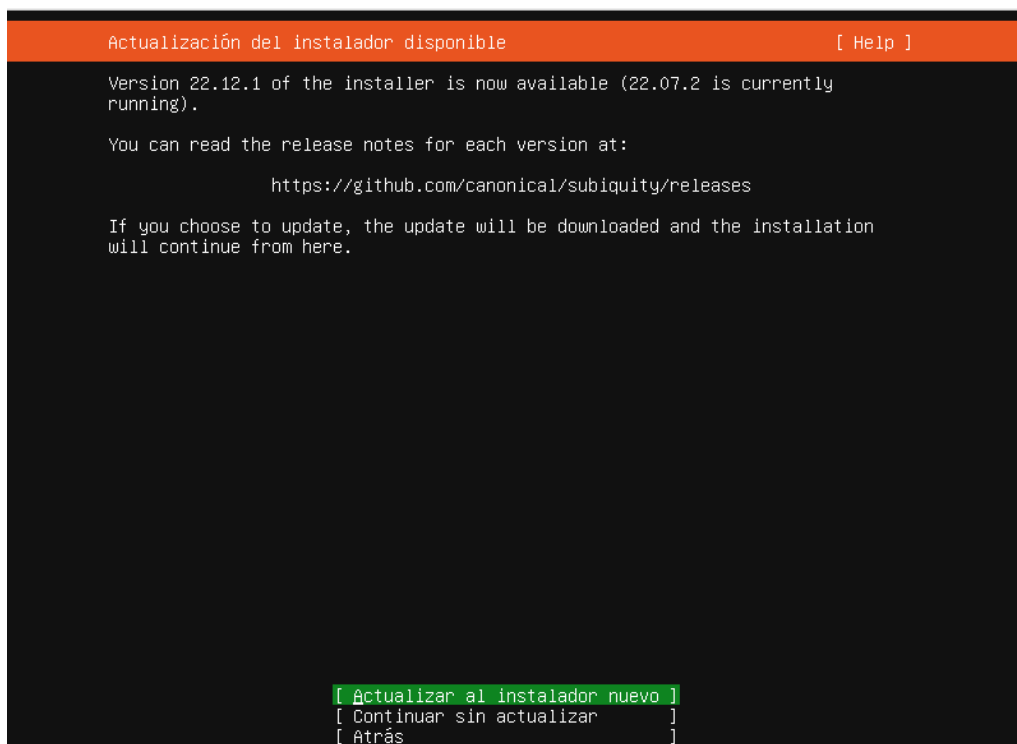
Viendo los paquetes que ofrecen los proveedores de dominios, y teniendo en cuenta las características de nuestra página web, me decanto por asignarle 64GB al servidor.

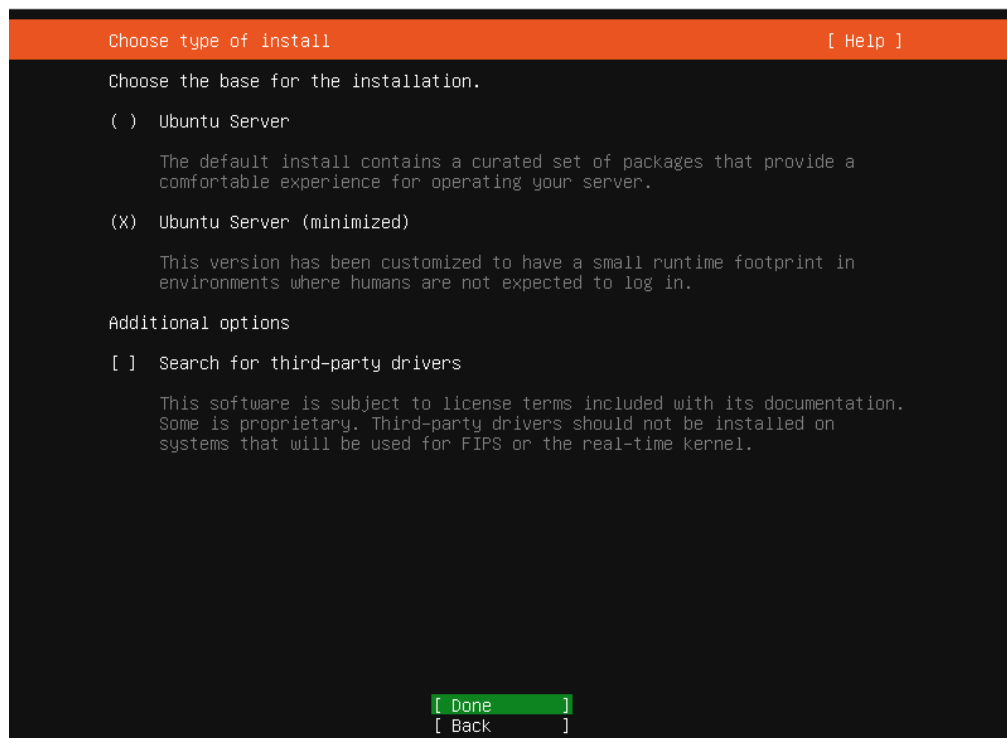




Introducimos la ISO de instalación y procedemos a arrancar la máquina.



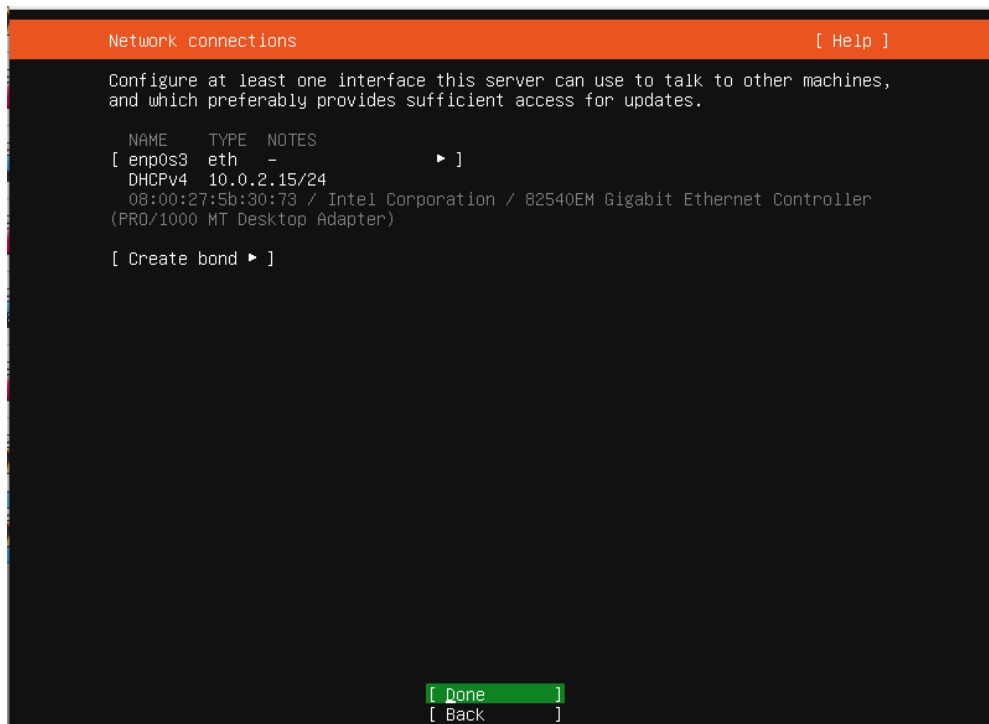




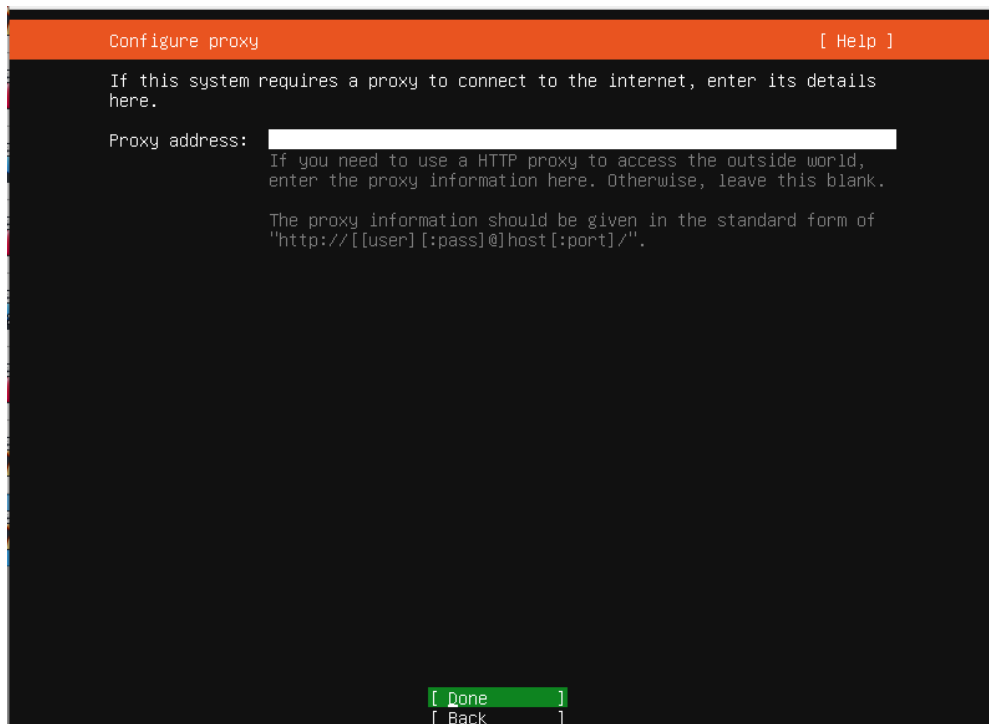
<https://wiki.ubuntu.com/Minimal>

Tras informarme un poco sobre en qué consiste la versión mínima, decido utilizar esta e ir instalando aquello que vaya necesitando, para hacer lo más pequeña posible la superficie de ataque y facilitar el mantenimiento y parcheado del sistema.

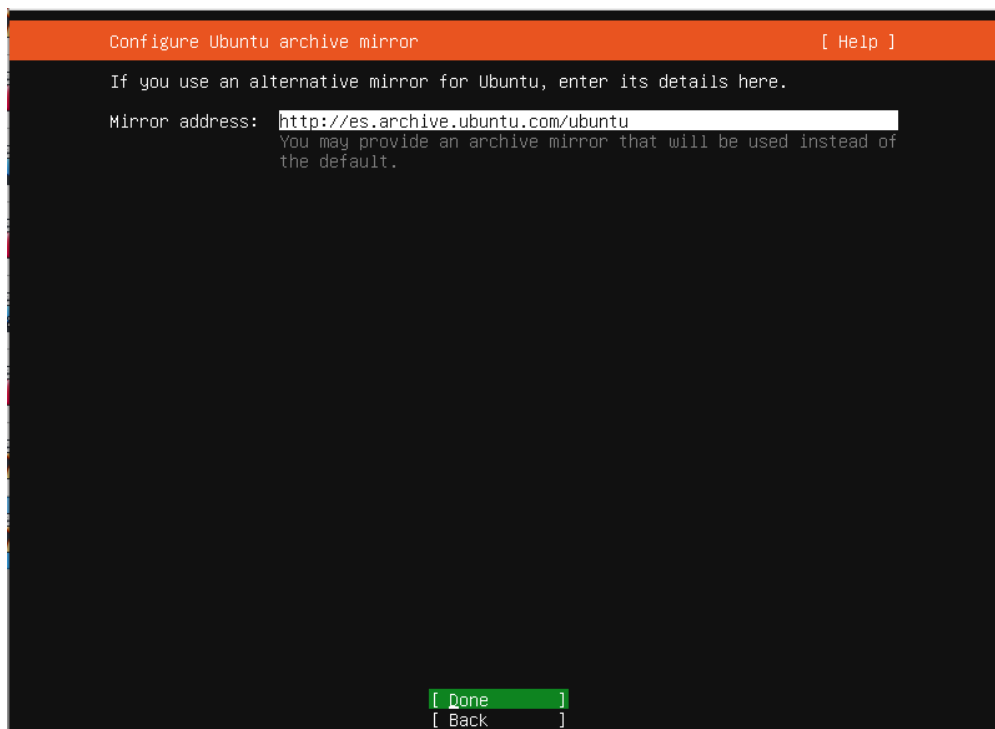
Para facilitar el hardening de futuras máquinas voy a hacer un script en para ejecutar todas las acciones necesarias.



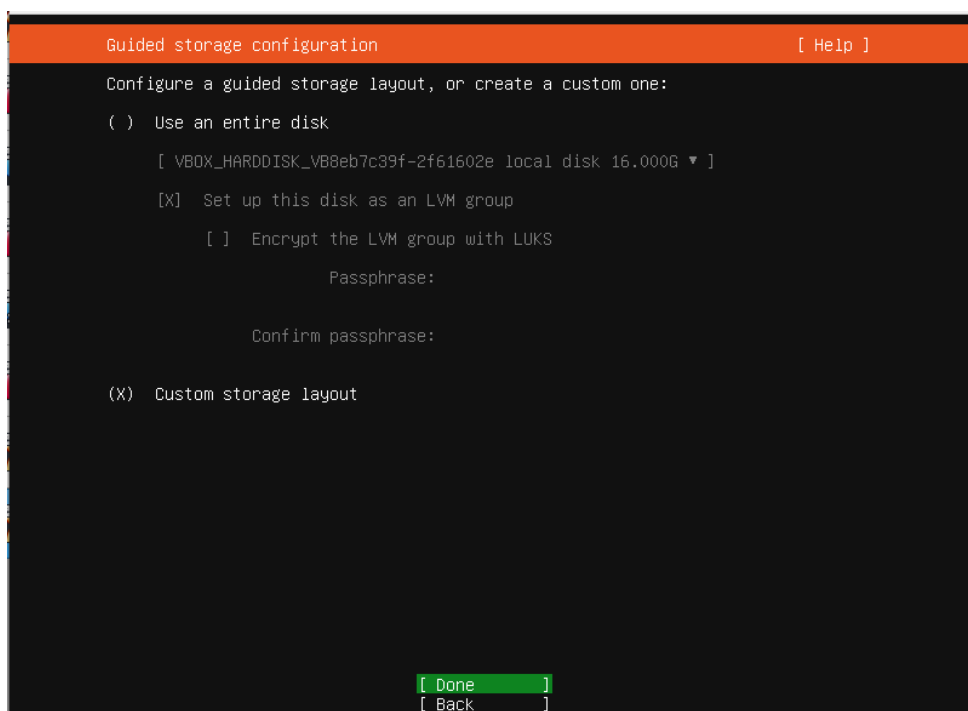
Por ahora configuraremos esta única interfaz de red, pudiendo modificarla posteriormente si fuera necesario:



No configuramos ningún proxy por el momento:



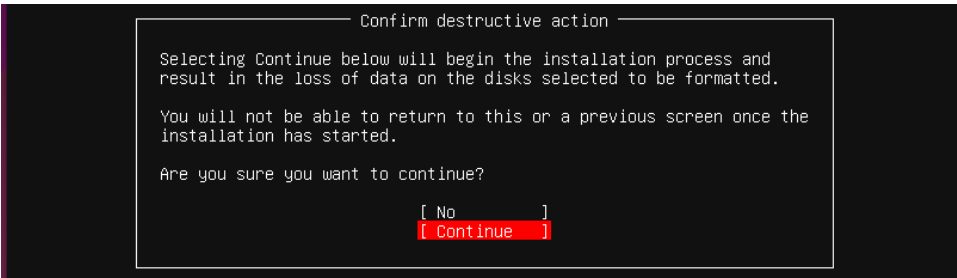
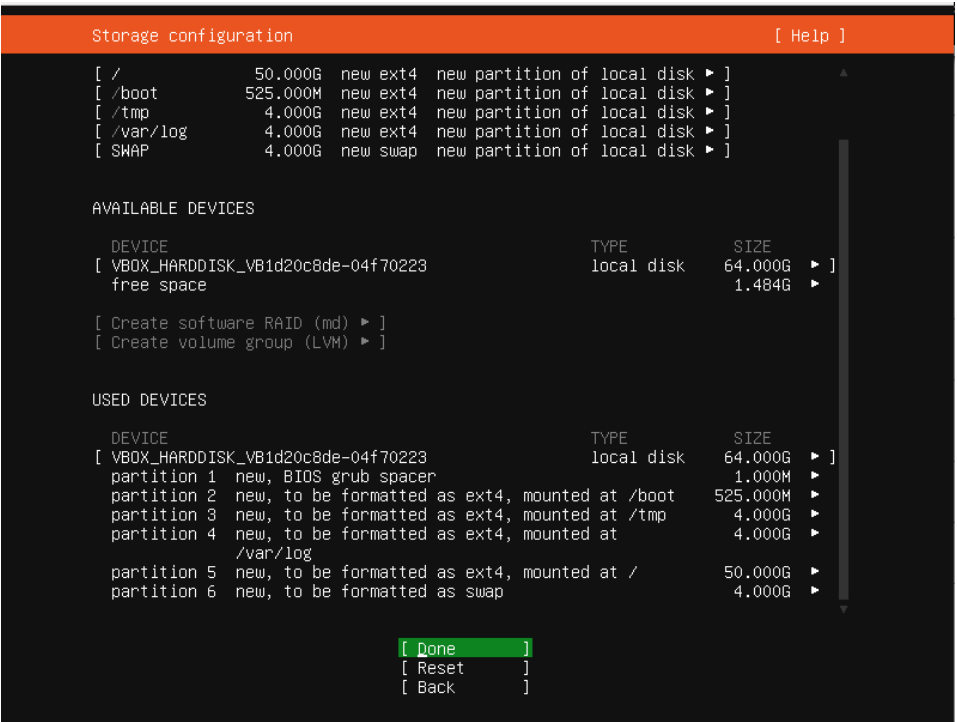
Como mirror utilizamos el configurado por defecto, que está localizado aquí en España.



Configuraremos una serie de particiones customizadas para nuestro proyecto.

A la partición /boot le asignaremos únicamente el espacio imprescindible para que un agente malicioso, en el caso de que consiguiera acceso no pudiera instalar nada. También crearemos por motivos de seguridad la partición /tmp. La máquina

no va tener usuarios que guarden cosas en ella por lo que no vemos la necesidad de crear una partición separada para el home de usuarios. Crearemos una partición pequeña para /var/log. El esquema con el espacio asignado a cada partición quedaría de la siguiente forma:



Usuario: ciber

Contraseña: th&bridg&

Profile setup[Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.

Your name:

Your server's name:
The name it uses when it talks to other computers.

Pick a username:

Choose a password:

Confirm your password:

[Done]

SSH Setup[Help]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

☒ Install OpenSSH server

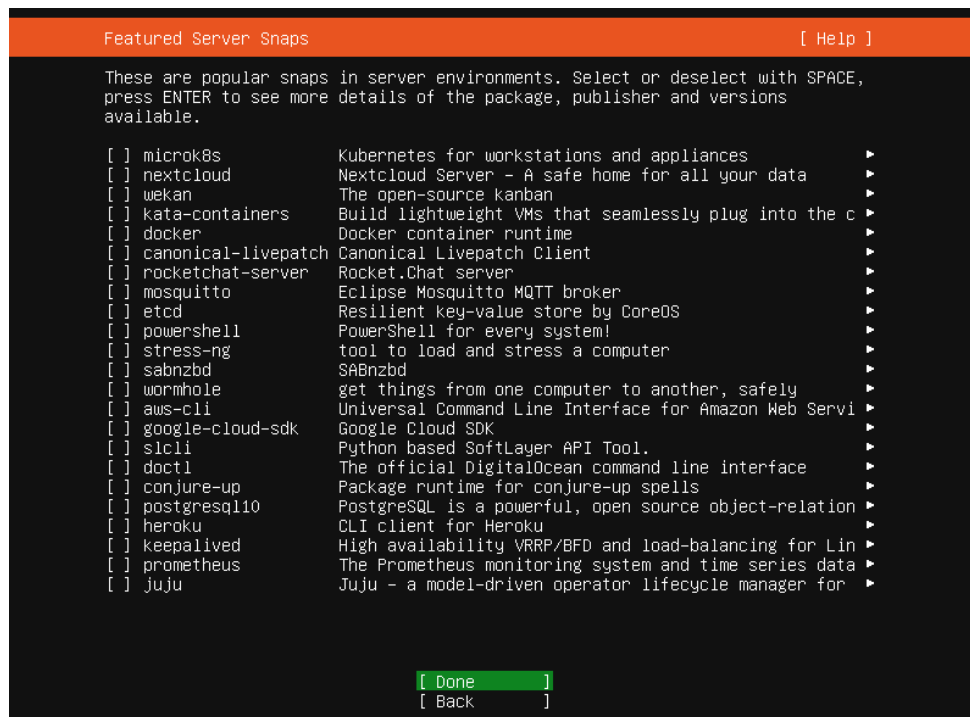
Import SSH identity:
You can import your SSH keys from GitHub or Launchpad.

Import Username:

☒ Allow password authentication over SSH

[Done]
[Back]

Instalamos SSH ya que lo vamos a utilizar posteriormente. No me permite deshabilitar la opción de permitir la autenticación por contraseña vía SSH, es una opción que creo que sería conveniente deshabilitar y lo verificaré más adelante.



Por ahora no añadiremos nada adicional y lo iremos instalando según sean necesarias.

Instalamos Apache2 para poder alojar el servidor web:

```
ciber@saracruzroja:~$ sudo apt-get install apache2
```

Hardening SSH

Para el hardening seguiremos la guía que utilizamos en clase CIS Debian Linux 10 Benchmark.

```
ciber@saracruzroja:~$ sudo apt-get install nano
```

Instalamos el editor de texto nano para poder editar los archivos de configuración de SSH.

Ensure permissions on /etc/ssh/sshd_config are configured.

```
ciber@saracruzroja:~$ sudo chmod og-r /etc/ssh/sshd_config
ciber@saracruzroja:~$ stat /etc/ssh/sshd_config
  File: /etc/ssh/sshd_config
  Size: 3281          Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d   Inode: 2229303    Links: 1
Access: (0600/-rw-----)  Uid: (  0/   root)   Gid: (  0/   root)
Access: 2023-01-18 08:13:46.276000848 +0000
Modify: 2023-01-17 07:46:08.688001643 +0000
Change: 2023-01-18 19:36:36.851919493 +0000
 Birth: 2023-01-17 07:23:10.572291870 +0000
```

Ensure permissions on SSH private host key files are configured.

```
ciber@saracruzroja:~$ find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat {} \;
  File: /etc/ssh/ssh_host_ecdsa_key
  Size: 513          Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2229055    Links: 1
Access: (0600/-rw-----)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-18 08:13:46.368000851 +0000
Modify: 2023-01-17 07:45:51.008000954 +0000
Change: 2023-01-17 07:45:51.008000954 +0000
Birth: 2023-01-17 07:45:51.008000954 +0000
  File: /etc/ssh/ssh_host_rsa_key
  Size: 2602         Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2228871    Links: 1
Access: (0600/-rw-----)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-18 08:13:46.316000849 +0000
Modify: 2023-01-17 07:45:50.936000951 +0000
Change: 2023-01-17 07:45:50.936000951 +0000
Birth: 2023-01-17 07:45:50.936000951 +0000
  File: /etc/ssh/ssh_host_ed25519_key
  Size: 411          Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2229305    Links: 1
Access: (0600/-rw-----)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-18 08:13:46.416000853 +0000
Modify: 2023-01-17 07:45:51.016000955 +0000
Change: 2023-01-17 07:45:51.016000955 +0000
Birth: 2023-01-17 07:45:51.016000955 +0000
  File: /etc/ssh/ssh_host_dsa_key
  Size: 1381         Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2229053    Links: 1
Access: (0600/-rw-----)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-17 07:45:50.996000954 +0000
Modify: 2023-01-17 07:45:50.996000954 +0000
Change: 2023-01-17 07:45:50.996000954 +0000
Birth: 2023-01-17 07:45:50.996000954 +0000
```

Todo correcto, root es el propietario y nadie a parte de él tiene permisos.

Ensure permissions on SSH public host key files are configured.

```
ciber@saracruzroja:~$ find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec stat {} \;
  File: /etc/ssh/ssh_host_ecdsa_key.pub
  Size: 179          Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2229056    Links: 1
Access: (0644/-rw-r--r--)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-18 08:13:46.404000853 +0000
Modify: 2023-01-17 07:45:51.008000954 +0000
Change: 2023-01-17 07:45:51.008000954 +0000
Birth: 2023-01-17 07:45:51.008000954 +0000
  File: /etc/ssh/ssh_host_ed25519_key.pub
  Size: 99           Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2229397    Links: 1
Access: (0644/-rw-r--r--)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-18 08:13:46.432000854 +0000
Modify: 2023-01-17 07:45:51.016000955 +0000
Change: 2023-01-17 07:45:51.016000955 +0000
Birth: 2023-01-17 07:45:51.016000955 +0000
  File: /etc/ssh/ssh_host_dsa_key.pub
  Size: 607          Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2229054    Links: 1
Access: (0644/-rw-r--r--)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-17 07:46:11.344001746 +0000
Modify: 2023-01-17 07:45:50.996000954 +0000
Change: 2023-01-17 07:45:50.996000954 +0000
Birth: 2023-01-17 07:45:50.996000954 +0000
  File: /etc/ssh/ssh_host_rsa_key.pub
  Size: 571          Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d Inode: 2229052    Links: 1
Access: (0644/-rw-r--r--)  Uid: (  0/   root)  Gid: (  0/   root)
Access: 2023-01-18 08:13:46.352000851 +0000
Modify: 2023-01-17 07:45:50.936000951 +0000
Change: 2023-01-17 07:45:50.936000951 +0000
Birth: 2023-01-17 07:45:50.936000951 +0000
```

Editamos el archivo de configuración y modificamos o añadimos todas las directivas pertinentes:

```
ciber@saracruzroja:/etc/ssh$ sudo nano /etc/ssh/sshd_config
```

```
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i loglevel
LogLevel INFO
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i x11forwarding
X11Forwarding no
#       X11Forwarding no
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i maxauthtries
MaxAuthTries 3
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i ignorerhosts
IgnoreRhosts yes
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i hostbasedauthentication
#HostbasedAuthentication no
HostbasedAuthentication no
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i permitrootlogin
PermitRootLogin no
# the setting of "PermitRootLogin without-password".
```

```
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i permitemptypasswords
PermitEmptyPasswords no
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i permituserenvironment
PermitUserEnvironment no
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i clientaliveinterval
ClientAliveInterval 300
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i clientalivecountmax
ClientAliveCountMax 0
```

```
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i logingracetime
LoginGraceTime 60
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i usepam
UsePAM yes
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i allowtcpforwarding
#AllowTcpForwarding yes
AllowTcpForwarding no
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i maxstartups
MaxStartups 10:30:100
ciber@saracruzroja:/etc/ssh$ sudo cat /etc/ssh/sshd_config | grep -i maxsessions
MaxSessions 10
```

Modificamos el archivo `issue.net` para no facilitar información a un posible atacante:

```
ciber@saracruzroja:/etc/ssh$ sudo nano /etc/issue.net_
```

```
ciber@saracruzroja:/etc/ssh$ cat /etc/issue.net
Authorized users only!
```

Por ahora, la configuración de la máquina se ha quedado hasta este punto, sería necesario continuar con la securización y configuración de la máquina para poder desplegar la aplicación correctamente.

En segundo lugar, es necesario levantar otra máquina en la que se encuentre instalado y configurado un **detector de intrusos**:

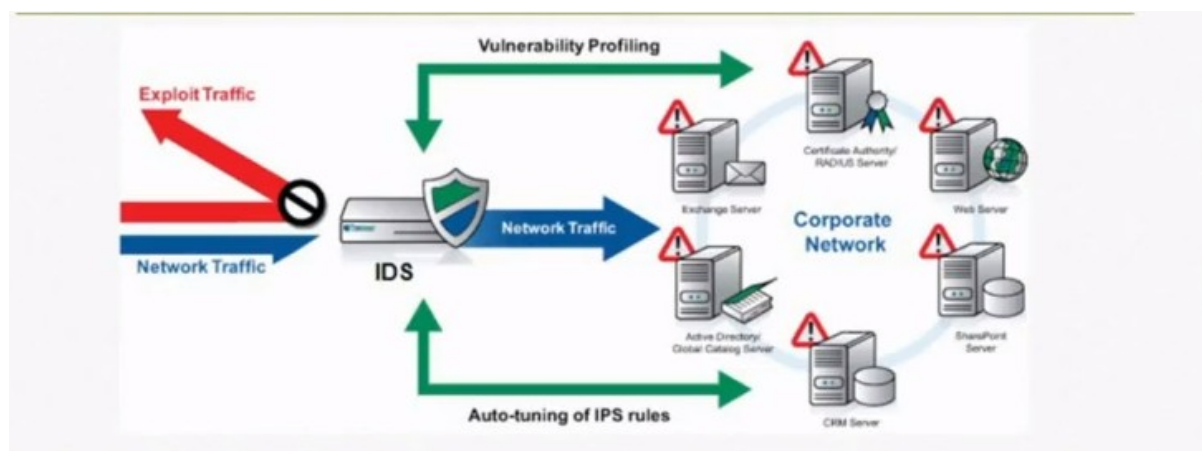
Un IDS (Sistema de Detección de Intrusiones) y un IPS (Sistema de Prevención de Intrusiones) son herramientas de seguridad informática que se utilizan para detectar y prevenir intentos de acceso no autorizado a una red o sistema.

Un IDS detecta y alerta sobre posibles intrusiones mediante el análisis de tráfico de red y la comparación con patrones conocidos de actividad maliciosa. Por otro lado, un IPS es capaz de bloquear automáticamente el tráfico malicioso antes de que pueda causar daños.

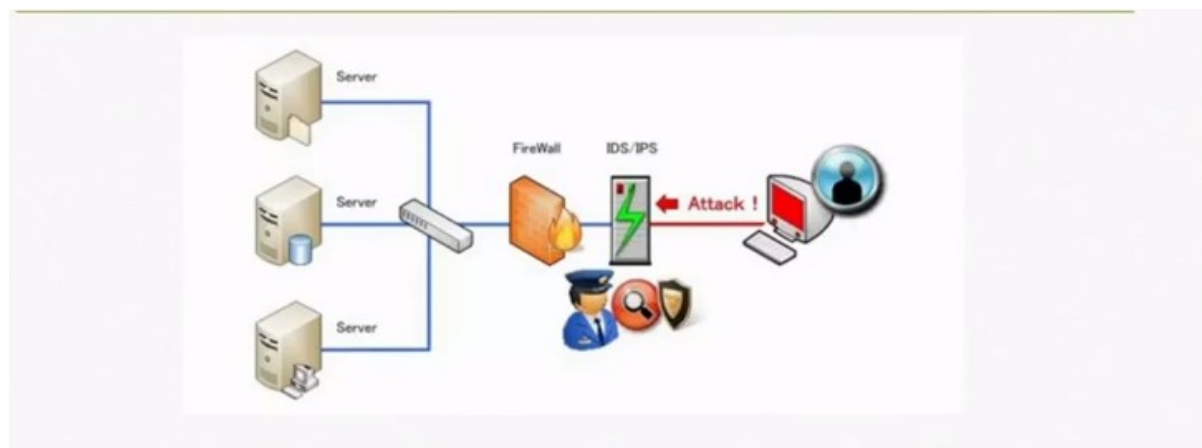
La importancia de un IDS/IPS radica en su capacidad para proteger una red o sistema de amenazas cibernéticas, como virus, malware, ataques de denegación de servicio (DoS) y robo de información. Además, estas herramientas pueden ayudar a cumplir con los estándares y regulaciones de seguridad de la información.

En resumen, un IDS/IPS son fundamentales para la seguridad informática ya que ayudan a detectar y prevenir intrusiones maliciosas en una red o sistema, protegiendo así la información confidencial y evitando posibles pérdidas económicas.

Esquema de funcionamiento de un IDS:



Esquema de funcionamiento de un IPS:



Para nuestro proyecto, se ha decidido utilizar SNORT:

SNORT es un sistema de detección de intrusos de código abierto. Funciona analizando el tráfico de red en busca de patrones que indican un intento de ataque o intrusión. SNORT puede detectar una amplia variedad de amenazas, como ataques de denegación de servicio (DoS), escaneo de puertos, explotaciones de vulnerabilidades de software y otros tipos de intrusos. Además, SNORT ofrece una serie de características avanzadas, como la capacidad de detectar contenido

malicioso en paquetes de red y la posibilidad de integrarse con otros sistemas de seguridad. En resumen, SNORT es una herramienta valiosa para proteger las redes contra amenazas cibernéticas.

Instalación y configuración de SNORT en Ubuntu Server 22.04

Buscamos la aplicación en el gestor de paquetes e instalamos los paquetes que nos solicita:

```
ciber@saracruzroja:~$ sudo apt-get install snort
[sudo] password for ciber:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauthen-sasl-perl libclone-perl libdaq2 libdata-dump-perl libdumbnet1 libencode-locale-perl
  libestr0 libfastjson4 libfile-listing-perl libfont-afm-perl libhtml-form-perl
  libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl
  libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libio-html-perl libio-socket-ssl-perl liblua5.1-2
  liblua5.1-common liblwp-mediatypes-perl liblwp-protocol-https-perl libmailtools-perl
  libnet-http-perl libnet-smtp-ssl-perl libnet-ssleay-perl libnetfilter-queue1 libnfnetlink0
  libpcap0.8 libtimedate-perl libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl
  logrotate net-tools oinkmaster perl-openssl-defaults rsyslog snort-common snort-common-libraries
  snort-rules-default
```

El siguiente paso, es descargar las reglas de Snort con las que poder trabajar y realizar la configuración adecuada del programa. El comando utilizado para realizar dicha función será el siguiente: `$sudo snort -c /etc/snort/snort.conf -T`

```

--== Initialization Complete ==--

o'-'~
.'-'~
.'-'~
.'-'~

-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: appid Version 1.1 <Build 5>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>

Snort successfully validated the configuration!
Reset output...
```

Procedemos a la configuración de SNORT

Para comenzar especificamos que snort se ejecute al inicio, ya que queremos que siempre esté trabajando.

```

Please choose how Snort should be started: automatically on boot, automatically when connecting to
the net with pppd, or manually with the /usr/sbin/snort command.

  1. boot  2. dialup  3. manual
Snort start method: 1

```

Nos da un comando para buscar la interfaz de red, lo ejecutamos para poder especificarlo en el siguiente punto:

```

ciber@saracruzroja:~$ /sbin/route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          10.0.2.2        0.0.0.0         UG    100    0      0 enp0s3
10.0.2.0         0.0.0.0         255.255.255.0   U     100    0      0 enp0s3
10.0.2.2         0.0.0.0         255.255.255.255 UH    100    0      0 enp0s3
10.0.2.3         0.0.0.0         255.255.255.255 UH    100    0      0 enp0s3

```

Especificamos la interfaz de red y el rango de IP:

```

Interface(s) which Snort should listen on: enp0s3

Please use the CIDR form - for example, 192.168.1.0/24 for a block of 256 addresses or
192.168.1.42/32 for just one. Multiple values should be comma-separated (without spaces).

You can leave this value empty and configure HOME_NET in /etc/snort/snort.conf instead. This is
useful if you are using Snort in a system which frequently changes network and does not have a
static IP address assigned.

Please note that if Snort is configured to use multiple interfaces, it will use this value as the
HOME_NET definition for all of them.

Address range for the local network: 192.168.0.0/24

Disabling promiscuous mode means that Snort will only see packets addressed to the interface it is
monitoring. Enabling it allows Snort to check every packet that passes the Ethernet segment even if
it's a connection between two other computers.

```

Y le decimos que siga funcionando en modo promiscuo ya que necesitamos que analice todos los paquetes que pasan por el segmento:

```

Should Snort disable promiscuous mode on the interface? [yes/no] n

```

Por último pero no menos importante especificamos el mail donde se enviarán diariamente los resúmenes de los logs

```

A cron job can be set up to send daily summaries of Snort logs to a selected e-mail address.
Please choose whether you want to activate this feature.

Should daily summaries be sent by e-mail? [yes/no] yes

Please specify the e-mail address that should receive daily summaries of Snort logs.

Recipient of daily statistics mails: sierranorte@cruzroja.es

Please enter the minimum number of alert occurrences before a given alert is included in the daily
statistics.

Minimum occurrences before alerts are reported: 1

```

reiniciamos para aplicar los cambios:

```
ciber@saracruzroja:~$ sudo /etc/init.d/snort restart
* Stopping Network Intrusion Detection System snort
* Starting Network Intrusion Detection System snort
```

REGLAS

A continuación, deberemos especificar las reglas que queremos asignar a nuestro IDS

Accedemos al archivo de configuración alojado en `/etc/snort/snort.conf` siempre creando una copia de seguridad con la fecha actual, en el incluimos la siguiente regla:

include \$RULE_PATH/sites.rules

Estamos especificando el path de nuestro archivo de reglas que vamos a crear en `/etc/snort/rules/nombreakivo.rules`

```
-----
# VRT Rule Packages Snort.conf
#
# For more information visit us at:
#   http://www.snort.org           Snort Website
#   http://vrt-blog.snort.org/     Sourcefire VRT Blog
#
# Mailing list Contact:   snort-users@lists.snort.org
# False Positive reports: fp@sourcefire.com
# Snort bugs:            bugs@snort.org
#
# Compatible with Snort Versions:
# VERSIONS : 2.9.15.1
#
# Snort build options:
# OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling
--enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-react --enable-f
lexresp3
#
# Additional information:
# This configuration file enables active response, to run snort in
# test mode -T you are required to supply an interface -i <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#-----
```

Algunas reglas básicas comunes que se pueden asignar a SNORT incluyen:

- Detectar y bloquear tráfico de red conocido como malicioso, como virus o malware.
- Detectar y alertar sobre intentos de inicio de sesión fallidos o intentos de acceso no autorizados a un sistema.
- Detectar y alertar sobre el uso de protocolos de red no autorizados en una red.
- Detectar y alertar sobre tráfico de red anómalo, como un gran volumen de tráfico o patrones de tráfico sospechosos.
- *Detectar y alertar sobre ataques de denegación de servicio (DoS) y distribuidos (DdoS).*

Por ejemplo:

```
alert tcp any any -> any any (msg:"Alguien entro a Facebook";content:"facebook";std:19910314;rev:1;)
alert tcp any any -> any any (msg:"Alguien esta intentando leer los puertos por
nessus";content:"nessus";std:19910315;rev:1;)
alert tcp any any -> any any (msg:"Ping";std:19919316;rev:1;)
```

Además de utilizar snort, el propio sistema nativo de Ubuntu, cuenta con herramientas para almacenar los logs que se van generando y administrarlos. Para ello utilizaremos las herramientas Rsyslog y Logrotate:

Rsyslog:

Los registros son muy útiles para analizar y solucionar cualquier problema relacionado con el sistema y las aplicaciones en Linux (Debian, Ubuntu, Fedora, CentOS, etc). Por defecto, todos los archivos de registro se encuentran dentro del **directorio /var/log** en los sistemas operativos basados **en Linux**. Hay varios tipos de archivos de registro, incluyendo cron, kernel, usuarios, seguridad y la mayoría de estos archivos, están controlados por **el servicio Rsyslog**.

Rsyslog **es un sistema potente y seguro para el procesamiento de registros**. El servidor Rsyslog recibe los registros a través de la red desde varios servidores físicos o virtualizados y supervisa la salud de diferentes servicios. Con el servidor Rsyslog, se pueden supervisar los registros de otros servidores, dispositivos de red y aplicaciones remotas desde una ubicación centralizada.

Requisitos previos

- Dos servidores con Ubuntu (con la misma versión).
- Una dirección IP estática (por ejemplo, 192.168.1.50) está configurada en la **máquina del servidor Rsyslog** y otra, está configurada en la **máquina del cliente Rsyslog** (por ejemplo, 192.168.1.62).
- Ambas máquinas en modo puente o bridge.
- Hemos configurado previamente una contraseña de root en ambos servidores.

Instalar Rsyslog

Por defecto, Rsyslog está instalado en el servidor de Ubuntu. Si no está instalado, habría que instalarlo ejecutando el siguiente comando:

apt-get install Rsyslog -y

Después de instalar Rsyslog, comprobaremos la versión de Rsyslog con el siguiente comando:

rsyslogd -v

Una vez comprobado, obtendremos la siguiente salida:

Rsyslogd 8.32.0 (versión correspondiente), compiled with:

PLATFORM: x86_64-pc-linux-gnu
PLATFORM (lsb_release -d):
FEATURE REGEXP: Yes
GSSAPI Kerberos 5 support: Yes
FEATURE_DEBUG (debug build, slow code): No
32bit Atomic operations supported: Yes
64bit Atomic operations supported: Yes
memory allocator: system default
Runtime Instrumentation (slow code): No
uuid support: Yes
system support: Yes
Number of bits in RainerScript integers: 64
See [thhp://www.rsyslog.com](http://www.rsyslog.com) for more information.

Para comprobar el estado de Rsyslog (si está activado o no) escribo el siguiente comando:

systemctl status rsyslog

A continuación nos debería aparecer el siguiente mensaje:

? rsyslog.service - System Logging Service
Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
Active: active (running) since Fri 2023-01-20 17:05:32 UTC; 2min 31s ago
Docs: man: rsyslogd (8)
<http://www.rsyslog.com/doc/>
Main PID: 724 (rsyslogd)
Tasks: 4 (limit: 1114)
CGroup: /system.slice/rsyslog.service

??724 /usr/sbin/rsyslogd -n

Jan 23 17:05:26 ubuntu1804 systemd[1]: Starting System Logging Service...

Jan 23 17:05:20 ubuntu1804 rsyslogd[724]: imuxsock: Acquired UNIX socket '/run/system/journal/syslog' (fd 3) from system. [v8.32.0] (o la versión que corresponda)

Jan 23 17:05:20 ubuntu1804 rsyslogd[724]: rsyslogd's groupid changed to 106

Jan 23 17:05:20 ubuntu1804 rsyslogd[724]: rsyslogd's userid changed to 102

Jan 23 17:05:18 ubuntu1804 rsyslogd[724]: [origin software="rsyslogd" swVersion="8.32.0" x-pid="724" x-info="http://www.rsyslog.com"] start

Jan 23 17:05:26 ubuntu1804 systemd[1]: Started System Logging Service.

Configurar Rsyslog

Ahora Rsyslog ya está instalado y funcionando, así que el siguiente paso es configurarlo para que se ejecute en modo servidor. Para ello, editamos el **archivo /etc/rsyslog.conf**, escribiendo el siguiente comando:

nano /etc/rsyslog.conf

Una vez dentro del archivo, lo **primero** que hacemos es **definir el protocolo**, ya sea **UDP o TCP**, o ambos. Para utilizar conexiones UDP y TCP al mismo tiempo, buscamos y **descomentamos** = eliminamos el símbolo de # del comienzo de **las siguientes líneas**:

\$ModLoad imudp

\$UDPServerRun 514

\$ModLoad imtcp

\$InputTCPServerRun 514

A continuación, vamos a **definir la subred, la IP o el dominio específicos** para limitar el acceso, como se muestra a continuación:

\$AllowedSender TCP, 127.0.0.1, 192.168.1.0/24, *.example.com

\$AllowedSender UDP, 127.0.0.1, 192.168.1.0/24, *.example.com

Ahora, tenemos que **crear una plantilla** para indicar al servidor Rsyslog cómo almacenar los mensajes syslog entrantes y para ello, tendré que añadir las siguientes líneas justo antes de la sección DIRECTIVAS GLOBALES:

```
$template remote-incoming-logs,  
"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"  
"."?remote-incoming-logs
```

Guardamos y cerramos el archivo una vez terminado y volvemos a comprobar si la configuración de Rsyslog presenta algún error de sintaxis escribiendo el siguiente comando:

```
rsyslogd -f /etc/Rsyslog.conf -N1
```

Deberíamos ver la siguiente salida:

```
rsyslogd: versión 8.32.0 (versión que corresponda), config validation run  
(level 1),  
master config /etc/Rsyslog.conf  
rsyslogd: End of config validation run. Bye.
```

Para finalizar con el proceso de configuración, tendremos que reiniciar el servicio Rsyslog con el siguiente comando:

```
systemctl restart rsyslog
```

Una vez reiniciado Rsyslog vamos a verificar que el mismo, está escuchando en TCP/UDP con el siguiente comando:

```
netstat -4altunp | grep 514
```

Ahora obtendremos el siguiente mensaje o salida:

```
tcp          0          0.0.0.0:514          0.0.0.0:*  
LISTEN      1332/Rsyslogd  
udp          0          0.0.0.0:514          0.0.0.0:*  
1332/rsyslogd
```

Ya hemos terminado de instalar y configurar el servidor Rsyslog para poder recibir registros de los hosts remotos que haya y ahora, pasamos a

configurar el cliente Rsyslog para que envíe mensajes syslog al servidor Rsyslog remoto.

Configuración del cliente Rsyslog

Accedemos a la máquina cliente y abrimos el archivo de configuración de Rsyslog como se muestra a continuación:

nano /etc/rsyslog.conf

Añadimos las siguientes líneas al final del archivo:

##Enable sending of logs over UDP add the following line:

“.” @192.168.1.50:514

##Enable sending of logs over TCP add the following line:

“.” @192.168.1.50:514

##Set disk queue when Rsyslog server will be down:

\$ActionQueueFileName queue

\$ActionQueueMaxDiskSpace 1g

\$ActionQueueSaveOnShutdown on

\$ActionQueueType LinkedList

\$ActionResumeRetryCount -1

Guardamos y cerramos el archivo. A continuación, reiniciamos el servidor Rsyslog para aplicar los cambios de configuración escribiendo el comando:

systemctl restart Rsyslog

Ver el registro del cliente

En este punto, el cliente Rsyslog está configurado para enviar su registro al servidor Rsyslog. Ahora, tenemos que ***iniciar sesión en el servidor Rsyslog y comprobar el directorio /var/log.*** Deberíamos ver la entrada, con el nombre de host de tus máquinas cliente incluyendo varios archivos de registro, escribiendo el siguiente comando:

ls /var/log/Rsyslog-client/

El mensaje de salida que veremos en la terminal será:

***CRON.log kernel.log rsyslogd-2039.log rsyslogd.log sudo.log
wpa_supplicant.log***

Logrotate

Este servicio va a ser ***muy importante*** ya que nos va a ayudar, de varias formas, con la gestión y el almacenamiento de los logs del sistema.

Por un lado, va a ***evitar que los Logs devoren el espacio del disco***, porque podemos crear una partición o volumen lógico para ellos (configurando un punto de montaje, por ejemplo para todo */var/log*). ***Y*** por otro lado, ***también los va a comprimir***, para que ocupen menos espacio.

Este servicio va a funcionar con el demonio de gestión de logs que hemos visto anteriormente: Rsyslogd.

Qué hace Logrotate y cómo funciona

La utilidad Logrotate se encarga de dividir los Logs, comprimirlos y archivarlos, según como lo hayamos configurado. Por defecto, se ocupa de aplicar políticas de rotación y compresión, pero también podemos personalizarlas.

Otro aspecto a tener en cuenta es que, por defecto, se ejecuta una vez a la semana, tal y como se encuentra definido en el archivo de configuración principal ubicado en la carpeta etc., o en el archivo concreto de logrotate para el demonio rsyslog (*/etc/logrotate/rsyslog*).

Archivo de logrotate.com por defecto:

```

GNU nano 2.2.6      Fichero: /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}

```

Fichero /etc/logrotate.d/rsyslog

```

GNU nano 2.2.6      Fichero: /etc/logrotate.d/rsyslog
/var/log/syslog
{
    rotate 7
    daily
    missingok
    notifempty
    delaycompress
    compress
    postrotate
        invoke-rc.d rsyslog rotate > /dev/null
    endscript
}

/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
    rotate 4
    weekly
    missingok
}

```

El Daemon rsyslog

El daemon rsyslogd se configura en ***/etc/rsyslog.conf***

En dicho archivo rsyslog.conf, podemos configurar la forma en que se deben tratar los mensajes de log, provenientes de diferentes tipos de archivo de registro, por ejemplo: mail, user, kern,daemon...

Podemos definir nuestro propio tipo de archivo de registro en /etc/rsyslog.conf, si por ejemplo queremos monitorizar la memoria, y creamos un archivo de registro llamado memoria.log.

Archivo *etc/rsyslog.conf*

```
GNU nano 2.2.6 Fichero: /etc/rsyslog.conf
##### RULES #####
#####
#
# First some standard log files. Log by facility.
#
auth,authpriv.* /var/log/auth.log
*.auth,authpriv.none -/var/log/syslog
cron.* /var/log/cron.log
daemon.* /var/log/daemon.log
kern.* /var/log/kern.log
lpr.* /var/log/lpr.log
mail.* /var/log/mail.log
user.* /var/log/user.log
#memoria.* /var/log/memoria.log
#
# Logging for the mail system. Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info -/var/log/mail.info
mail.warn -/var/log/mail.warn
mail.err /var/log/mail.err
#
# Logging for INN news system.
#
news.crit /var/log/news/news.crit
news.err /var/log/news/news.err
news.notice -/var/log/news/news.notice
```

3. Configuración de Logrotate

Existen diversos métodos para configurar la rotación de los Logs en Linux (Ubuntu) con logrotate.

3.1. Configuración 1 de Logrotate (/etc/logrotate.d/nuevo-archivo-log)

Logrotate se puede configurar en los archivos específicos que se encuentran en *etc/logrotate.d/nuevoarchivo.Rsyslog* es el demonio que gestiona en los logs.

Un ejemplo de configuración de un nuevo tipo de archivo de Log podría ser este:

```
/var/log/memoria.log
{
rotate 4
hourly
missingok
notifempty
compress
maxsize 10K
}
```

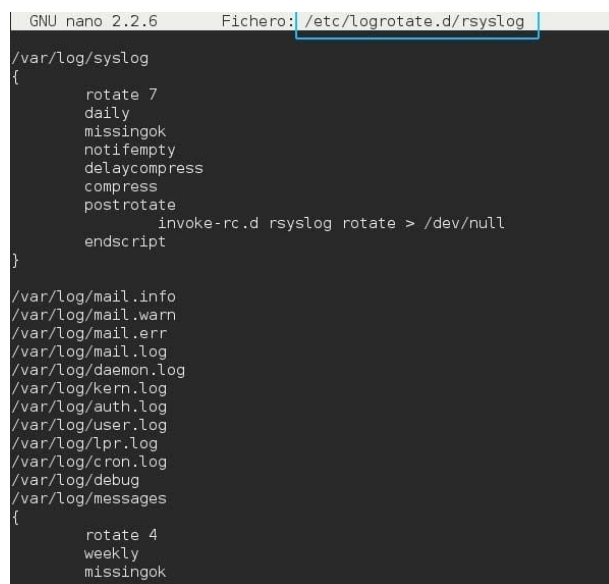
```
GNU nano 2.2.6 Fichero: /etc/logrotate.d/memoria
/var/log/memoria.log
{
rotate 4
hourly
missingok
notifempty
compress
maxsize 5K
}
```

Reiniciar rsyslogd
y ejecutar *etc/cron.daily/logrotate*

3.2. Configuración 2 de Logrotate (/etc/logrotate.d/rsyslog)

Definir nuevo tipo de archivo de Log en */etc/logrotate.d/rsyslog* (dentro del subdirectorio */logrotate.d*), en el propio archivo principal de configuración del servicio del daemon rsyslogd (en el subdirectorio de configuraciones de logrotate).

Recordemos que el daemon rsyslogd es el que gestiona todos los tipos de logs del sistema que están definidos en el archivo:



```
GNU nano 2.2.6 Fichero: /etc/logrotate.d/rsyslog
/var/log/syslog
{
    rotate 7
    daily
    missingok
    notifempty
    delaycompress
    compress
    postrotate
        invoke-rc.d rsyslog rotate > /dev/null
    endscript
}

/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
    rotate 4
    weekly
    missingok
```

Después tenemos que reiniciar rsyslogd con el comando:

`/etc/init.d/rsyslog restart`

Y después ejecutar:

`/etc/cron.daily/logrotate`

3.3. Configuración 3 de Logrotate (/etc/rsyslog.conf)

Definir en `/etc/rsyslog.conf` (archivo principal de configuración de rsyslog) un tipo de archivo de log personalizado, por ejemplo `memoria.log`, de esta forma, escribiendo:

`memoria.* -/var/log/memoria.log`

```
GNU nano 2.2.6      Fichero: /etc/rsyslog.conf

#### RULES ####
#####

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*          /var/log/auth.log
*.*;auth,authpriv.none   /var/log/syslog
#cron.*                  /var/log/cron.log
daemon.*                 /var/log/daemon.log
kern.*                   /var/log/kern.log
lpr.*                    /var/log/lpr.log
mail.*                   /var/log/mail.log
user.*                   /var/log/user.log
memoria.*                 /var/log/memoria.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                 /var/log/mail.info
mail.warn                 /var/log/mail.warn
mail.err                  /var/log/mail.err
#
# Logging for INN news system.
#
news.crit                 /var/log/news/news.crit
news.err                  /var/log/news/news.err
news.notice               /var/log/news/news.notice

[ 121 líneas leídas ]
```

Nuevo tipo
de archivo de
log que
definimos
en
/etc/rsyslog.conf,
el archivo de
config de rsyslogd,
el demonio
de los Logs.

Reiniciar rsyslogd.

Y ejecutar /etc/cron.daily/logrotate.

3.4. Configuración 4 de logrotate (/etc/logrotate.conf)

También existe el archivo /etc/logrotate.conf, que contiene la configuración principal y predeterminada de logrotate, y la de algunos registros no específicos, que a su vez llama a todos los archivos de configuración contenidos de /etc /logrotate.d cuando se carga. Aunque se puede incluir aquí nuestro nuevo archivo de Log, es mejor utilizar el método 1.

```
GNU nano 2.2.6      Fichero: /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}
```

Ejecutar */etc/cron.daily/logrotate*