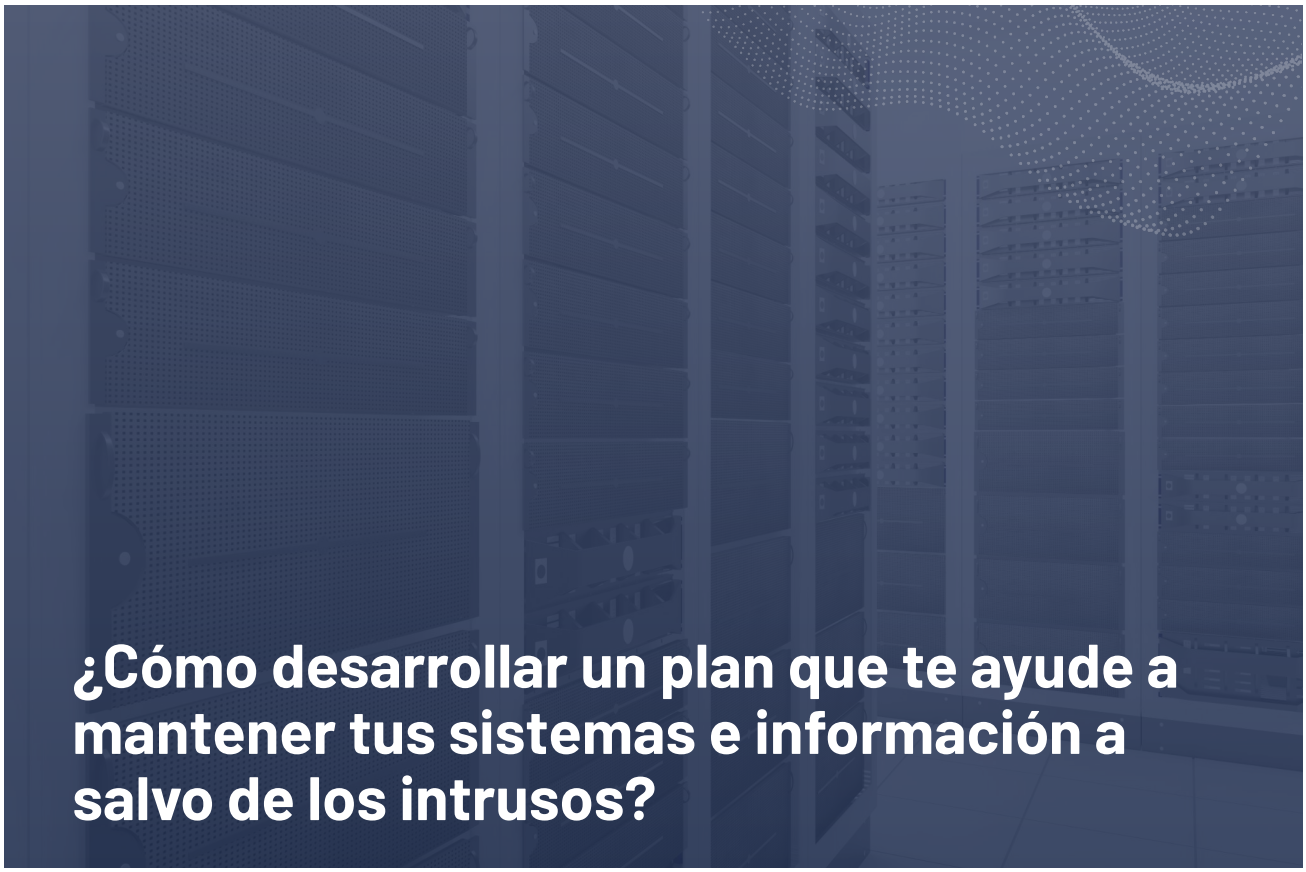
HACKNOID

5 pasos para elaborar un plan de ciberseguridad

La manera más completa de abordar todos los aspectos de la seguridad informática

www.hacknoid.com



¿Cómo desarrollar un plan que te ayude a mantener tus sistemas e información a salvo de los intrusos?

Los ciberataques son cada vez más frecuentes y cuestan a las empresas miles de millones de dólares cada año. Para proteger tus redes informáticas, tus datos y tus dispositivos de estos ataques, necesitas tener un plan de ciberseguridad.

¿Qué es un ciberataque y por qué son cada vez más frecuentes?

Los ataques pueden provocar la pérdida de millones de dólares

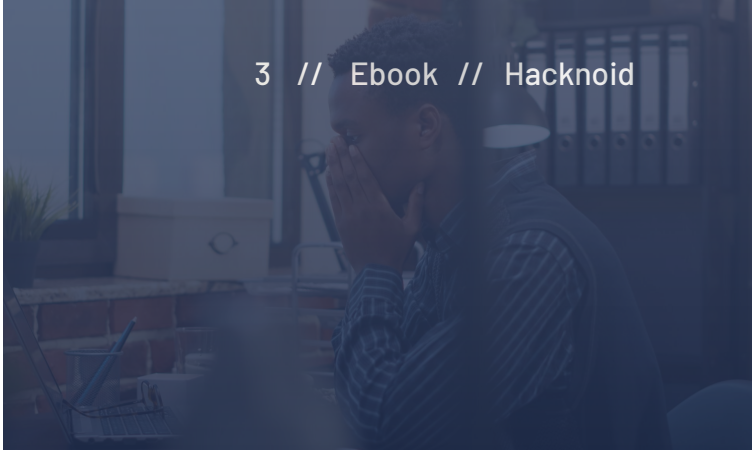
Un ciberataque es un ataque a una red, sistema o dispositivo informático que se lleva a cabo de forma remota. Los ciberataques pueden utilizarse para robar información, interrumpir las operaciones o dañar los sistemas, entre otros.

Una de las razones por las que los ciberataques son cada vez más frecuentes es porque cada vez son más fáciles de llevar a cabo. Muchos atacantes utilizan malware o ransomware para infectar los sistemas con software malicioso que les da acceso a las redes y a los datos.

Además, las empresas dependen cada vez más de los sistemas informáticos y las redes, lo que las convierte en un objetivo de los ciberataques. A medida que se almacenan más y más datos en línea y se interconectan más sistemas, las empresas se exponen más y se vuelven más vulnerables a ataques que pueden provocar la pérdida de millones de dólares.

Los 5 pasos para desarrollar un plan de ciberseguridad

Un plan de ciberseguridad es una parte vital para proteger tus redes informáticas, datos y dispositivos de los ciberataques.



Microsoft advierte que los hackeos crecieron un 74% el último año

La compañía realizó un informe sobre ciberseguridad entre 2021 y 2022. Sin embargo, en Estados Unidos y Europa los casos de ransomware mostraron un descenso.

Leer estudio

Identificación y evaluación

El primer paso para crear un plan de ciberseguridad es identificar los activos a proteger, pero que se van a desprender del proceso de negocio al cual proveen valor.

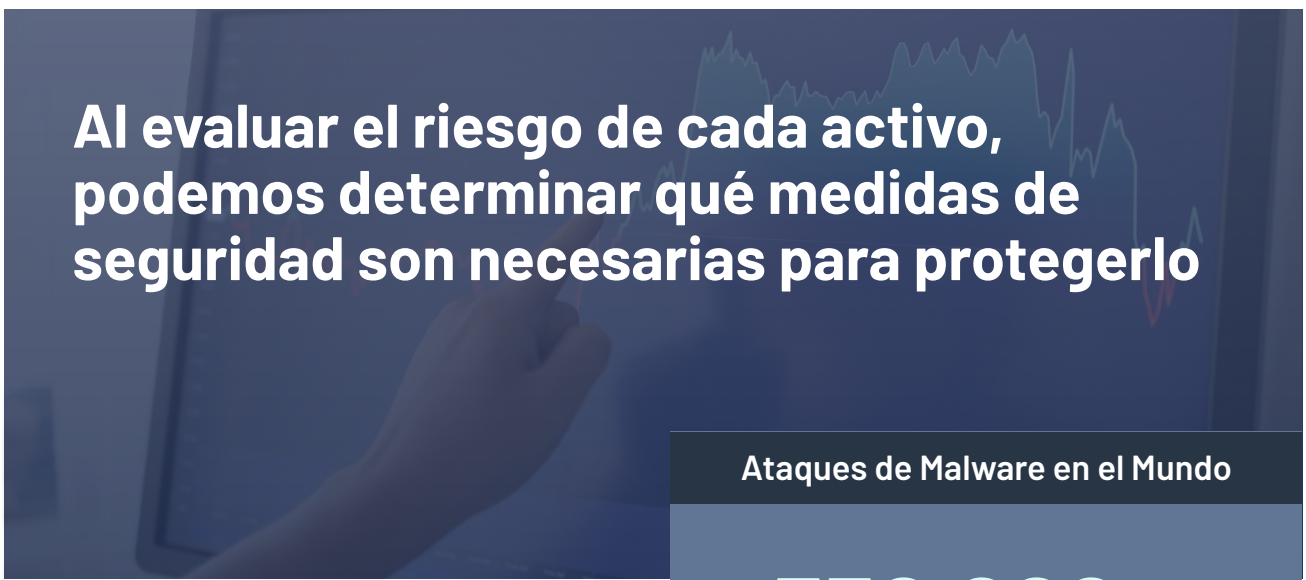
En función de la **criticidad** del proceso de negocio primero, se determinan los activos que dan soporte al mismo y se pondera su criticidad en él. Así se obtiene un listado priorizado de cada activo con sus amenazas asociadas, alineado con el objetivo de negocio de la organización, lo que garantiza que estén protegidos en consecuencia, al tiempo que se permite el acceso cuando sea necesario.

El valor del activo: Si un atacante fuera capaz de robar o dañar un activo, ¿cuánto le costaría a la empresa?

La sensibilidad de los datos: ¿qué valor tienen los datos almacenados en tus sistemas? ¿Podría un atacante utilizarlos para obtener beneficios económicos o para perjudicar a tu empresa?

La vulnerabilidad del activo: ¿es fácil para un atacante acceder a tus sistemas o datos? ¿Existen puntos débiles que puedan ser explotados?

La probabilidad de que se produzca un ataque: ¿cuál es la probabilidad de que tu sistema sea objeto de un ciberataque?



¿Por qué es clave realizar un plan de ciberseguridad en tu empresa?

- Para proteger los datos de la organización.
- Para proteger tus sistemas y dispositivos.
- Cumplir con la normativa.
- Para apoyar la continuidad de su negocio.
- Para proteger la reputación de tu organización.

Identificación de las amenazas

Una vez que hayas identificado los activos que hay que proteger, tienes que identificar las amenazas que suponen un riesgo para ellos.

A la hora de crear un plan de ciberseguridad, es importante identificar las **amenazas internas y externas** a los sistemas y datos de su empresa.

Las amenazas internas pueden provenir de empleados malintencionados o descuidados, mientras que las externas pueden provenir de hackers, ciberdelincuentes u otras organizaciones.

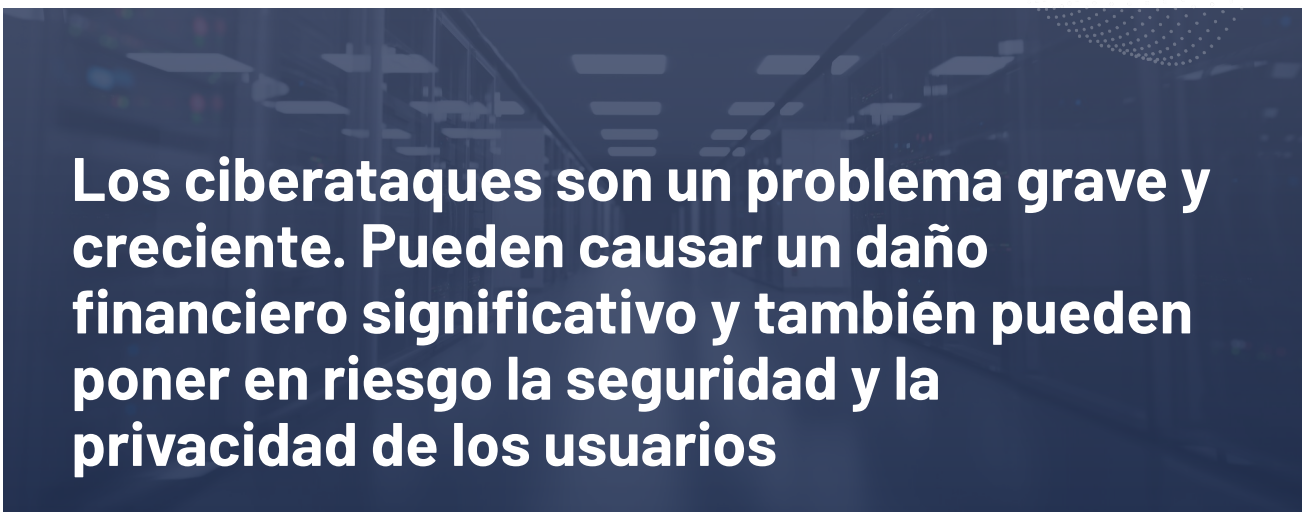
Para **identificar las amenazas internas**, es importante evaluar la arquitectura de la red (subdivisión de áreas) y la eficacia de las políticas de ciberseguridad (cambios de clave, procesos de ABM de usuarios, medidas disciplinarias para los empleados que la infrinjan, entre otros). Además, es necesario revisar los controles de acceso y los privilegios según el concepto **"Need To Know"** (que requiere la persona para desarrollar sus tareas).

También debes realizar auditorías de seguridad periódicas para asegurarse de que los empleados siguen la política y para detectar cualquier actividad maliciosa o accidental.

En el caso de las **amenazas externas**, debes identificar una lista de todas las vulnerabilidades de tu empresa y luego desarrollar estrategias para mitigar estos riesgos.

Puedes apoyarte de auditorías o software de monitoreo de vulnerabilidades, y actualizar periódicamente este software para protegerte de las últimas amenazas.

También debes establecer relaciones con proveedores externos de confianza que puedan ayudarte a proteger sus sistemas contra los ciberataques.



Un ciberataque es cualquier peligro o peligro potencial que existe en el ciberespacio. Puede incluir malware, ransomware y ataques de phishing, por nombrar solo algunos. Los ciberataques también pueden incluir incidentes como la violación de datos, o la escalación de privilegios, en los que se roba o se pone en peligro información sensible.

Evaluación del riesgo

Tras identificar las amenazas, tienes que evaluar los riesgos que suponen para tus activos. Esto incluye evaluar la probabilidad de que se produzca un ataque y el daño potencial que podría causarse si uno tuviera éxito.

Cuando se trata de ciberseguridad, no hay una solución única para todos.

A la hora de evaluar el riesgo que corren tus activos en caso de un ciberataque, debes tener en cuenta el valor de los datos que podrían ser robados o puestos en peligro, así como los daños potenciales que podrían producirse.

Hay que tener en cuenta las vulnerabilidades existentes categorizadas por su **probabilidad** de eventual ocurrencia y por el **impacto** que podría ocasionar de efectivizarse un daño.

Para evaluar la **probabilidad** de un ataque, se pueden tener en cuenta factores como el tipo de datos que se almacenan, el grado de acceso a los mismos, quién podría querer acceder a ellos, y también los "scorings" que proveen las propias bases de datos de vulnerabilidades internacionales sobre cada vulnerabilidad.

También puedes examinar la seguridad de tu red y el grado de protección de sus sistemas.

A la hora de estimar el **impacto** de un ciberataque, es importante utilizar una matriz de riesgo que te ayude a asignar valores a los diferentes aspectos del ataque. Los valores de la matriz deben establecerse dentro de una escala (típicamente del 1 al 5).

¿Cómo evaluar el riesgo e impacto de un ciberataque en mi organización?

¿Cómo medir el daño potencial?

Una forma de **medir el daño potencial (impacto)** que un ciberataque podría causar a tu empresa es considerar el costo de una violación de datos.

Una filtración de datos puede ser muy costosa para una empresa, no solo por el dinero que se pierde, sino también por el daño a su reputación.

Otra forma de medir el daño potencial es considerar cuánto negocio podría perderse si los sistemas de la empresa no estuvieran disponibles durante un período de tiempo.

Además, debes considerar cuánto costaría recuperarse de un ciberataque.

Medidas de seguridad

Una vez que hayas evaluado los riesgos, tienes que establecer las medidas de seguridad adecuadas para proteger tus activos.

Hay una variedad de medidas de ciberseguridad que se pueden poner en práctica en tu empresa para proteger tus sistemas y datos de los ciberataques.

Algunas de estas medidas son:

1. Implementar contraseñas fuertes y procedimientos de autenticación.
2. Equiparte de herramientas que te apoyen desde lo preventivo, lo detectivo y lo reactivo (cortafuegos, antivirus, escaners, detectores de intrusos)
3. Formar a los empleados en las mejores prácticas de ciberseguridad.
4. Desarrollar un plan de respuesta a incidentes.

¿Cómo saber qué medidas de ciberseguridad son más eficientes en mi organización?

0.1
Comienza por evaluar tu nivel de riesgo. ¿Cuáles son los activos más importantes que hay que proteger?

0.2
Considera tu presupuesto y recursos. ¿Cuánto dinero puedes invertir en ciberseguridad? ¿De qué tipo de conocimientos técnicos dispones en tu empresa?

0.3
Utiliza las mejores prácticas del sector como punto de partida. Existe mucha información útil sobre cómo proteger sus sistemas de los ciberataques.

0.4
Mantente al día sobre las nuevas amenazas y vulnerabilidades. La ciberseguridad es un campo en constante evolución, por lo que es importante mantenerse informado sobre las últimas amenazas y cómo defenderse de ellas.

0.5
Prueba y evalúa tus medidas de seguridad con regularidad. Una vez que hayas puesto en marcha algunas medidas de seguridad básicas, es importante que las pruebes con regularidad para asegurarte de que funcionan correctamente y mantienen tus sistemas a salvo.

Pruebas y revisión

Una vez que tus medidas de seguridad estén en marcha, tienes que probarlas para asegurarte de que son eficaces. También tienes que revisar tu plan a medida que surjan nuevas amenazas o cambie tu negocio.

Uno de los aspectos más importantes de un plan de ciberseguridad es asegurarse de que las medidas que se aplican son eficaces.

Para ello, debes probar y actualizar regularmente tus medidas de seguridad, así como las nuevas amenazas que van surgiendo.

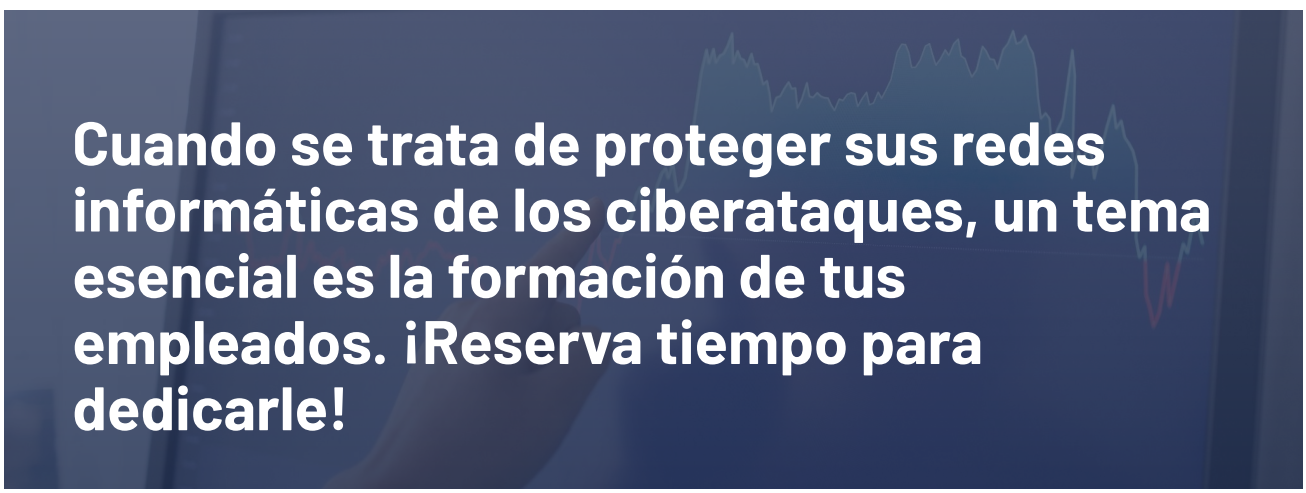
Revisa periódicamente tus políticas de seguridad de la red y de los datos para asegurarte de que están actualizadas y son eficaces.

La planificación de la ciberseguridad puede ayudarte a proteger tus redes informáticas y sus datos de los ciberataques. Recuerda que se trata de un ciclo continuo que se retroalimenta y que debe mantenerse actualizado. Asegúrate de contar con las herramientas y los recursos necesarios para ello.

Además, debes asegurarte de que tus colaboradores son conscientes de los riesgos asociados a los ciberataques y de cómo pueden ayudar a proteger las redes y los datos de tu empresa.

¿Cómo capacitar a mis empleados?

- Asegúrate de que todo el mundo entiende los fundamentos de la ciberseguridad.
- Enséñales a detectar los correos electrónicos de phishing.
- Explica la importancia de la seguridad de las contraseñas.
- Enséñales cómo informar de actividades sospechosas.
- Insistir en que no comparta información confidencial en línea.



HACKNOID

Solicita una Demo de Hacknoid

www.hacknoid.com

URUGUAY
Durazno 1504 Oficina 1 esq. Martínez Trueba
Palermo, Montevideo

CHILE
Av. Nueva Tajamar 481 Torre Norte, Of 1403,
Las Condes, Santiago