HACKNOID

4 formas de convencer a tu empresa de que invierta en ciberseguridad

Todo tu ambiente tecnológico,
monitoreado de forma automática

www.hacknoid.com

El trabajo del CISO no consiste únicamente en proteger los activos de la empresa, sino que también vela por su estado financiero

Como Director de Seguridad de la Información (CISO), sabes que la ciberseguridad es esencial para proteger los datos de tu empresa.

Convencer a tus jefes de que inviertan en ciberseguridad puede ser todo un reto.

Inversión Ciberseguridad

Para tener éxito en el juego de la ciberseguridad, es necesario que se haga un caso de inversión.

El trabajo del CISO

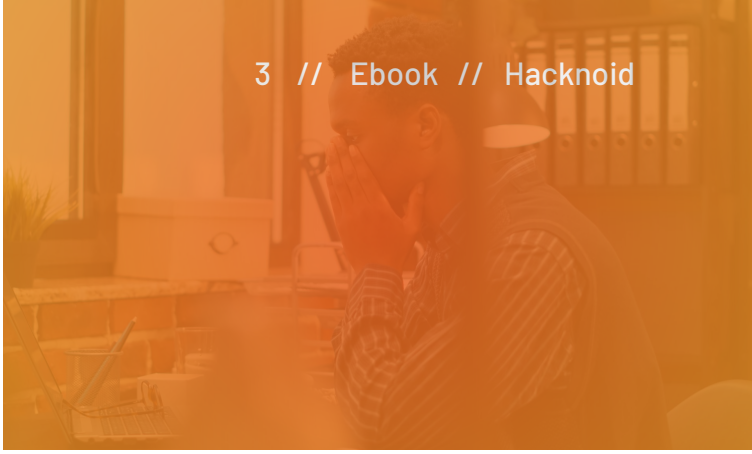
Un rol clave dentro de las organizaciones

El trabajo del CISO no consiste únicamente en proteger los activos de la empresa, sino que también vela por su estado financiero. Por este motivo, batalla por la seguridad de sus operaciones para que, en caso de que ocurra algo, sus pérdidas tampoco sean tan graves desde este punto de vista.

4 formas de conseguir que tu empresa se comprometa a invertir en ciberseguridad

La ciberseguridad es una amenaza que cada vez está más presente en nuestras vidas.

A diario leemos noticias de empresas que han sido víctimas de ataques informáticos, y el número de incidencias sigue en aumento.



Cada 10 segundos hay un ataque de Ransomware

Según un reciente informe de Infosecurity Magazine, existe una víctima de ransomware cada 10 segundos.

Leer estudio

Muéstrales las cifras

No es ningún secreto que los números dominan el mundo de los negocios. Nos guste o no, todo se reduce a dinero. ¿Pero qué significa eso para los CISO? ¿Cómo pueden asegurarse de que su organización se centra en lo correcto?

La ciberdelincuencia va en aumento, y el costo de una violación de datos también.

Según un informe de **IBM Security**, el costo medio de una violación de datos es ahora de 3,92 millones de dólares, **un 29% más que en 2018.**

El **60% de las empresas cierran el negocio** en los seis meses siguientes a un ciberataque.

El **78% de las grandes corporaciones**, ha sufrido un ciberataque en el último año.

Mostrar a tu empresa las cifras concretas les ayudará a comprender lo importante que es la ciberseguridad.

Un ciberataque puede ser costoso para las empresas de varias maneras: dinero y reputación

Una de las cosas más importantes que hay que recordar sobre la ciberseguridad es que no se trata de un solo sistema, sino de muchas capas.

- Siempre surgen nuevas amenazas, por lo que es necesario contar con software antimalware, cortafuegos y herramientas de escaneo inteligente.

- Cada una de estas capas de seguridad se complementan entre sí.

Aumento de ataques Ransomware

Muéstrales las cifras

¿Cómo han evolucionado los ciberataques?

Los ciberataques llevan muchos años evolucionando en todo el mundo. En los primeros tiempos de la informática, eran simples ataques cuyo objetivo era inutilizar un ordenador o una red.

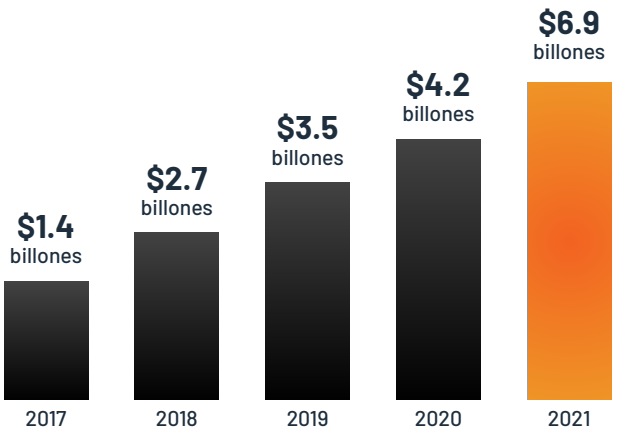
Hoy en día, los ciberataques son mucho más sofisticados y pueden causar daños importantes a empresas y particulares.

Por ejemplo, un ciberataque puede robar datos sensibles, como números de tarjetas de crédito o credenciales de acceso.

Los ciberdelincuentes también son cada vez más sofisticados en sus tácticas.

Las organizaciones deben estar preparadas para este tipo de ataques e invertir en soluciones de ciberseguridad para proteger sus datos.

Costo total de Ciberataques



Estudio: Federal Bureau of Investigation Internet Crime Report 2021

25%

Los ciberataques a empresas crecen un 25% a causa de la pandemia

80%

Casi el 80% de los líderes senior de TI y seguridad creen que sus organizaciones carecen de protección suficiente contra ciberataques

77%

Más del 77% de los afectados por ransomware estaban ejecutando una protección de endpoints actualizada

93%

93% del malware observado el año 2019 es polimórfico, es decir que es capaz de modificar su programación para evitar ser detectado

Ayúdales a entender los riesgos

¿A qué se exponen las empresas ante un ciberataque? ¿Cuáles son sus riesgos?

No sólo las grandes empresas corren el riesgo de sufrir ciberataques: las pequeñas empresas también están en peligro. Si ayudas a tu empresa a comprender los riesgos a los que se enfrenta, será más probable que quieran **invertir en ciberseguridad.**

Los ciberataques pueden causar un daño importante a una empresa, ya sea una gran corporación o una pequeña empresa.

En caso de ataque, las empresas podrían enfrentarse a la **pérdida de datos confidenciales, pérdidas financieras, daños a la reputación e interrupciones en sus operaciones.**

Las consecuencias para los clientes pueden ser aún más graves, incluyendo el **robo de información personal** y pérdidas económicas.

Es importante que las empresas comprendan que no son inmunes a estos riesgos; de hecho, **las pequeñas empresas pueden ser incluso más vulnerables** debido a la falta de recursos y experiencia en medidas de ciberseguridad.

Reconociendo los peligros potenciales e **invirtiendo en medidas de seguridad** como la encriptación de datos y la formación de los empleados en prácticas seguras en línea, las empresas pueden mitigar el riesgo de ser objetivo de los ciberatacantes.

En ciberseguridad, los **directivos deben entender** que existen distintos tipos de ataques. La mayoría de los directivos tiende a creer que "nadie va a atacar su empresa o negocio", sin embargo, en la mayoría de los casos los ataques no siempre son dirigidos, sino que los hackers apuntan a todas las empresas que no presentan un alto nivel de conocimiento técnico.

Este tipo de ataque cibernético es uno de los más frecuentes, ya que los atacantes se aprovechan de cualquier vulnerabilidad que encuentran al "barrer", sin distinguir a quién o a qué tipo de empresa.

Si el hacker encuentra una brecha, simplemente va a disparar a la primera oportunidad que se le presente.

Invertir en software y educar en formación a todo el personal es la mejor inversión

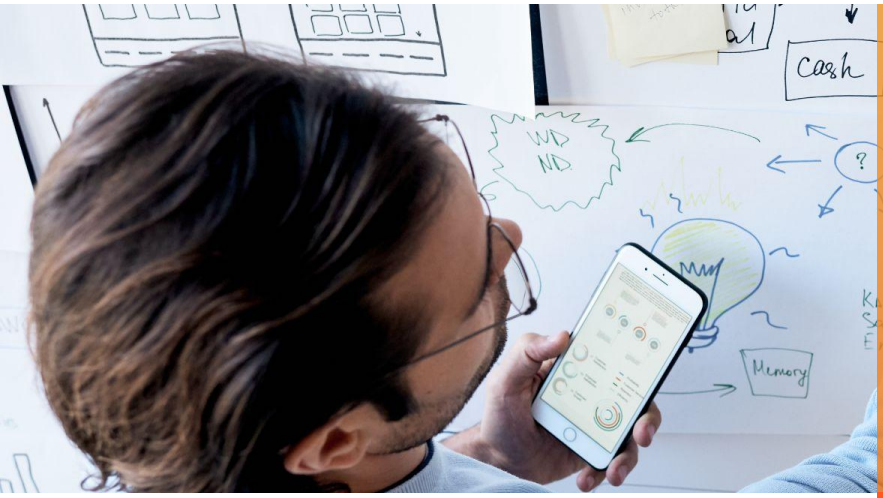
Las empresas están expuestas a muchos riesgos en caso de ciberataque, como la pérdida de datos, el daño a la reputación y las responsabilidades legales.

- Estos riesgos pueden provocar importantes pérdidas económicas, daños a la reputación y pérdida de confianza de los clientes.

- Para mitigar estos riesgos, las empresas deben invertir en fuertes medidas de seguridad y disponer de un sólido plan de respuesta a incidentes.

Haz un plan

Una vez que tu empresa comprenda los riesgos y la importancia de la ciberseguridad, puedes empezar a elaborar un plan para proteger mejor sus datos.



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

Cada empresa es diferente, y cada una tiene su propio conjunto de necesidades y vulnerabilidades.

Sin embargo, hay algunos pasos básicos que todas las empresas pueden dar para crear un plan de ciberseguridad que las proteja de los ciberataques.

Asegúrate siempre de hacer un seguimiento de las ciberamenazas recientes y de cómo pueden afectar a tu negocio.

Incluye inversión en herramientas y soluciones de ciberseguridad, como el cifrado y la autenticación de dos factores

- **Identifica tus amenazas**
  Incluye tanto las amenazas internas como las externas, así como las específicas de tu sector.
- **Crea una evaluación de riesgos**
  Te ayudará a determinar cuáles son más urgentes y requieren una atención prioritaria.
- **Desarrolla una estrategia de mitigación**
  Incluye la aplicación de medidas de seguridad, la formación de los empleados sobre las mejores prácticas de ciberseguridad y la creación de planes de respuesta a incidentes.
- **Supervisa y ajusta tu plan**
  Actualiza tus medidas de seguridad, la formación de los empleados y la creación de nuevos planes de respuesta a incidentes.

Explica cómo les beneficiará

Invertir en ciberseguridad no sólo ayuda a proteger los datos de tu empresa, sino que también puede ayudarles a ahorrar dinero a largo plazo.

Por ejemplo, invertir en encriptación puede ayudar a tu empresa a evitar costosas multas si sufre una violación de datos. Y la inversión en la autenticación de dos factores puede ayudar a evitar los ataques de phishing, cuya limpieza puede costar más de un millón de dólares.

Ayudar a tu empresa a ver cómo le beneficiará invertir en ciberseguridad hará que sea más probable que quiera invertir.

6 beneficios de invertir en ciberseguridad para las empresas

0.1
La ciberseguridad puede ayudar a proteger los datos de tu empresa.

0.2
La ciberseguridad puede ayudar a proteger a tu empresa de las amenazas online, como los hackers o el malware

0.3
La ciberseguridad puede ayudarte a responder a los ciberataques con rapidez y eficacia

0.4
La ciberseguridad puede ayudarte a cumplir las normativas

0.5
La ciberseguridad puede ayudarte a mejorar el estado de madurez lo cual repercute en la continuidad del negocio

0.6
La ciberseguridad puede ayudarte a ahorrar dinero a largo plazo

Explica cómo les beneficiará

Ciberseguridad y continuidad del negocio

Un ciberataque puede tener un impacto significativo en las operaciones empresariales, causando la interrupción de servicios vitales y provocando pérdidas financieras.

Además de los costos directos de investigar y reparar los daños causados por el ataque, las empresas pueden sufrir una pérdida de ingresos cuando los clientes se van a la competencia, y un aumento de los gastos mientras trabajan para mejorar sus defensas de ciberseguridad.

4 mil millones de dólares
JP Morgan, Citigroup, BestBuy y VISA

En la década de 2000, Epsilon era uno de los proveedores de servicios de marketing por correo electrónico más destacados hasta que sufrió un hackeo que puso en peligro los datos de aproximadamente 60 millones de usuarios.

3.8 mil millones de dólares
Telefónica, Nissan, Hitachi, Renault, FedEx o Deutsche Bahn

El virus WannaCry, ampliamente considerado como el mayor ciberataque de la historia, se llevó a cabo en 2017.

Infectó miles de ordenadores en todo el mundo y causó pérdidas millonarias a empresas como Telefónica, Nissan, Hitachi, Renault, FedEx o Deutsche Bahn.

Las vulnerabilidades se reducen al estar permanentemente alerta y tratarlas en una gestión continua, asegurando que el tiempo de convivencia con ellas sea el mínimo posible

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