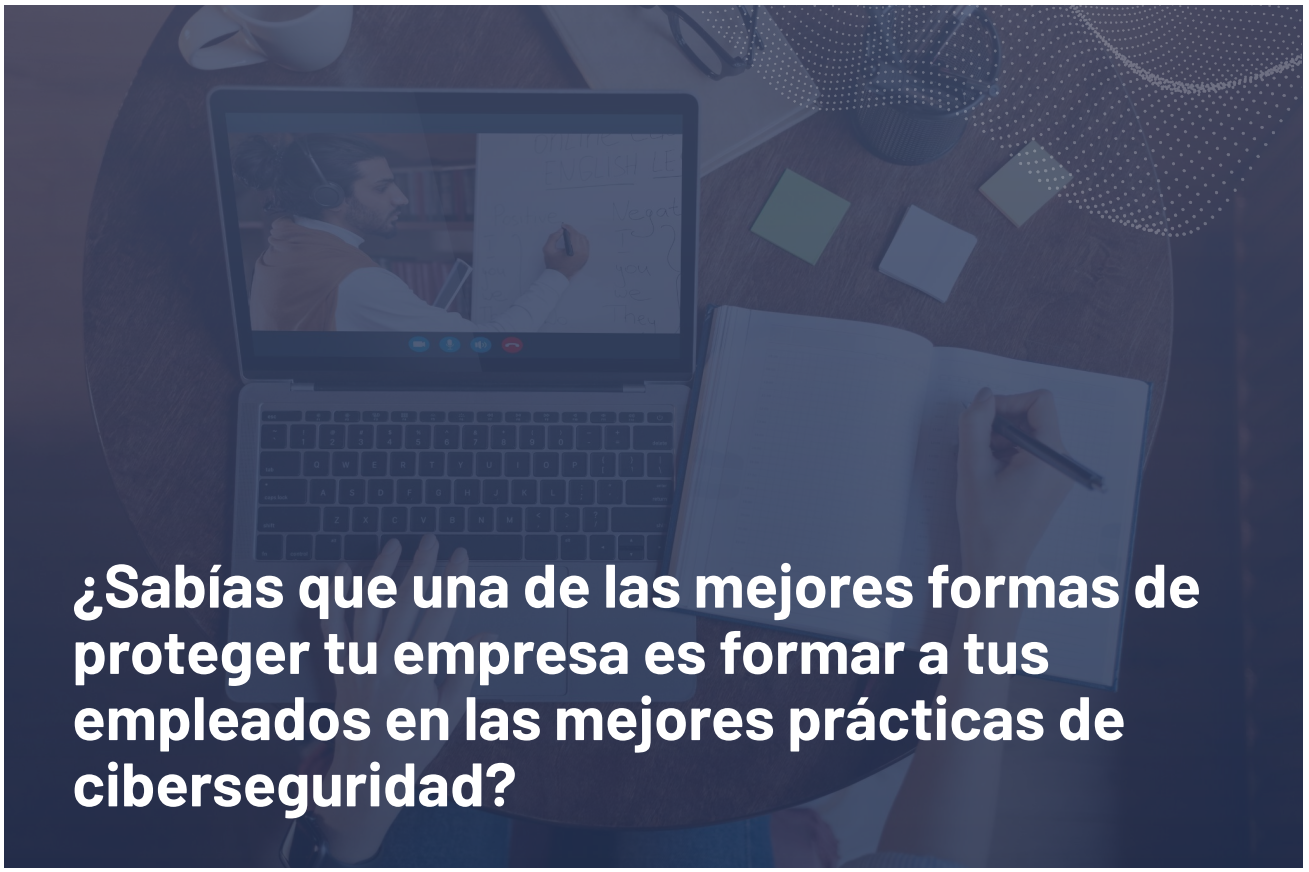
HACKNOID

# 5 buenas prácticas de ciberseguridad para capacitar a tus colaboradores

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

www.hacknoid.com



# ¿Sabías que una de las mejores formas de proteger tu empresa es formar a tus empleados en las mejores prácticas de ciberseguridad?

Como CISO, sabes que proteger tu empresa de los ciberataques es fundamental. Proporcionándoles sencillos consejos y directrices, puedes contribuir a que tomen las precauciones necesarias para mantener a salvo tu empresa.

## ¿Cuáles son las mejores prácticas de ciberseguridad?

Los ataques pueden provocar la pérdida de millones de dólares

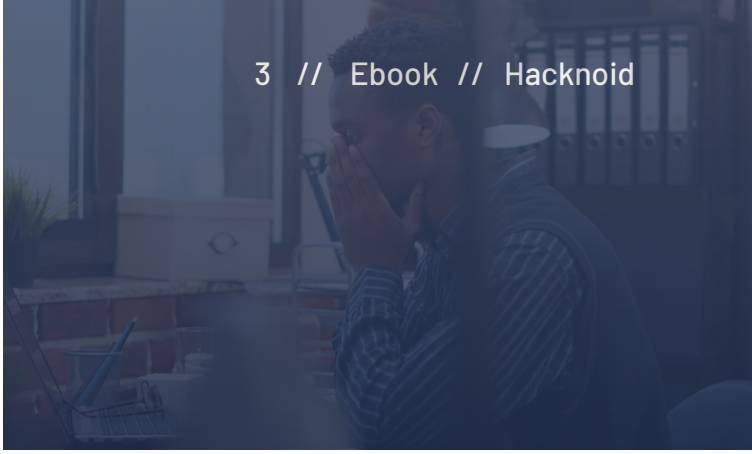
Las mejores prácticas de ciberseguridad deben implementarse en un **programa de formación integral para todos los empleados**, con el fin de garantizar que todos son conscientes y están preparados para protegerse a sí mismos y a la organización frente a las ciberamenazas.

La formación debe incluir temas como la seguridad de las contraseñas, la identificación y respuesta a los correos electrónicos de phishing, la protección contra el malware, la navegación y la eliminación segura de documentos confidenciales.

Asegúrate de recordarles a menudo la importancia de la seguridad cibernética.

Cuanto más sepan de esta importancia y las consecuencias, menos probabilidades tendrán de caer en una estafa o ser víctimas de un robo de identidad.

# 5 buenas prácticas de ciberseguridad para capacitar a tus colaboradores



Las medidas de ciberseguridad para los empleados son esenciales para proteger tu empresa de los ciberataques.

## Los ciberdelitos costaron más de 6.900 millones de dólares, según FBI

La ciberdelincuencia es una industria en crecimiento. La peor noticia es que las predicciones de Google sobre ciberseguridad para 2023 anticipan que esta economía maliciosa no hará más que seguir expandiéndose y diversificándose.

Leer estudio

# Destaca la importancia de la ciberseguridad

**Hacer hincapié en la importancia de la ciberseguridad a tus empleados es una de las mejores formas de proteger tu empresa de los ciberataques. Es fundamental que tus empleados comprendan los peligros potenciales a los que se enfrentan y cómo proteger sus datos y dispositivos.**

Explica a tus empleados que los ciberdelincuentes atacan a las empresas, para obtener un beneficio propio. Un ciberataque con éxito puede tener consecuencias devastadoras para las organizaciones, tanto económicas como de reputación.

Una forma de asegurarse de que todo el mundo entiende cuáles son las mejores prácticas esperadas es crear una política de empresa que describa las medidas de seguridad que debe adoptar cada empleado.

Debe incluir directrices sobre cómo crear contraseñas seguras, con qué frecuencia deben cambiarse las contraseñas, qué tipo de información no debe compartirse en Internet, etc.

**Para asegurarse de que todos los colaboradores estén lo suficientemente capacitados para hacer frente a posibles amenazas cibernéticas, es necesario planificar y llevar a cabo un entrenamiento en ciberseguridad regular y efectivo**

**¿Por qué es importante capacitar a los empleados en temas de ciberseguridad?**

- Para evitar el robo de datos y otros actos delictivos cibernéticos.
- Para identificar riesgos críticos antes de que sucedan.
- Para descubrir brechas críticas en su infraestructura tecnológica y adoptar nuevas medidas preventivas.
- Para promover un entorno laboral más consciente e informado sobre seguridad informática.

**Reforzar ideas y conceptos**

**Una forma de asegurarse de que tus empleados son conscientes de los conceptos de ciberseguridad es repetirlos hasta que se conviertan en algo natural, o parte de su "ADN".**

# Gestión eficaz de contraseñas

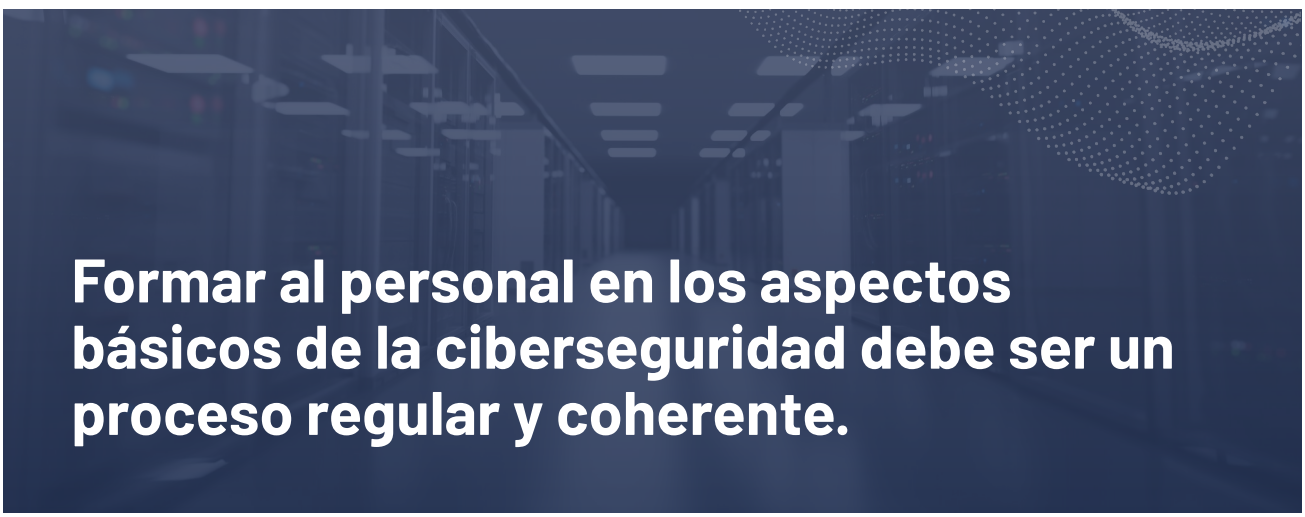
**La gestión de contraseñas es una parte esencial de la protección de tu empresa frente a las ciberamenazas. Tus empleados deben conocer las mejores prácticas para crear y gestionar contraseñas seguras, así como los peligros de utilizar contraseñas débiles.**

En la medida de lo posible, los empleados deben evitar reutilizar contraseñas en varias cuentas. Si esto no es factible debido a la cantidad de cuentas diferentes que tienen que recordar, considera la posibilidad de implementar un sistema de inicio de sesión único (SSO), que les permita almacenar sus credenciales de forma segura en un solo lugar e iniciar sesión en las cuentas rápidamente con un solo conjunto de credenciales.

Por último, las empresas deben facilitar a los empleados el acceso a las opciones de cambio de contraseña en la página de configuración de la cuenta.

Fomenta los cambios regulares al menos cada 3 meses, para mantener a los actores maliciosos fuera de tus sistemas.

Si es posible, considerar la posibilidad de establecer normas que obliguen a todos los usuarios a cambiar sus contraseñas al menos una vez cada seis meses para mayor seguridad.




Para garantizar que los empleados retienen los conocimientos que les estás proporcionando, es importante asegurarse de que los temas tratados durante la formación se repiten con frecuencia. Lo mejor es dividir las sesiones en lecciones cortas a lo largo de varios días o semanas, para que los empleados puedan asimilar cada concepto más fácilmente y reforzarlo con ejercicios prácticos o cuestionarios.

# Identificar el phishing y otras estafas

**El phishing y otras estafas son una gran amenaza para la seguridad de las empresas, ya que pueden provocar filtraciones de datos e infecciones de malware.**

**Las empresas deben implementar un plan de respuesta a incidentes que describa los procedimientos para responder rápidamente y mitigar efectos**

## Señales que pueden ayudar a tus empleados a diferenciar entre los correos electrónicos reales y los intentos de phishing.

Verificar el origen de los mails al recibir por ejemplo los típicos (promociones, pedido de cambio o verificación de datos, anuncios sospechosamente beneficiosos), es una de las primeras acciones que deben hacerse verificar a los empleados, o como mínimo llamar a la mesa de ayuda si no están 100% seguros de su origen.

Por otra parte, verificar, que al pasar el ratón o mouse por encima de alguno de los links del cuerpo del mail, aparezca la dirección institucional de donde dice estar dirigido y no cualquier otra, o alguna que contenga palabras o caracteres extra y sospechosos.

Los atacantes copian enteramente las páginas de destino y a simple vista parece todo tener coherencia. Por eso lo primero es estar alertas para levantar la sospecha cuando la oferta o el pedido resultan ser demasiado beneficiosos o solicitan datos confidenciales del usuario.

Tomando estas medidas, las empresas pueden prepararse mejor contra posibles ciberamenazas como el phishing y reducir sus posibilidades de sufrir efectos adversos a nivel organizativo.

### Efectos del Phishing en las empresas

Los efectos del phishing a nivel organizativo son polifacéticos y pueden ser devastadores para las empresas.

Los ataques de phishing se dirigen a empleados desprevenidos con correos electrónicos o enlaces maliciosos que pueden contener virus, ransomware u otras formas de software malicioso.

Estos ataques pueden provocar el robo de datos confidenciales, la interrupción de las operaciones y pérdidas económicas debidas al tiempo de inactividad de los empleados y a los costes de reparación.

Además, el phishing también puede provocar daños a la reputación cuando la información confidencial de los clientes queda expuesta como resultado de la estafa.

# Business Continuity Planning

**Es esencial ser consciente de los riesgos y comprender cómo reconocer y responder a las amenazas habituales.**

Para asegurarte de que tus empleados están preparados, considera la posibilidad de utilizar pruebas internas de ingeniería social y phishing como parte de su formación.

**Ataques de ingeniería social**

Los ataques de ingeniería social suelen utilizar tácticas de engaño, como la suplantación de direcciones de correo electrónico o la suplantación de ejecutivos de la empresa, para acceder a información sensible.

Mediante el uso de estas pruebas, puedes aumentar la probabilidad de que tus empleados identifiquen estos intentos antes de que tengan éxito.

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

**Business Continuity Planning / Planes de recuperación**

La planificación de la continuidad de la actividad (BCP) y los planes de recuperación en caso de catástrofe también son parte importante de la formación en ciberseguridad, ya que ayudan a esbozar los procedimientos para responder a los incidentes y proteger los datos en caso de catástrofe.

Estos planes **deben comprobarse periódicamente**, tanto interna como externamente, para asegurarse de que son actuales, están al día y son eficaces.

Es importante comprobar que los planes incorporan las mejores prácticas más recientes para proteger las redes de los ciberataques.

Cuando desarrolles **políticas de seguridad** para tu organización, asegúrate de incluir formación obligatoria para los empleados sobre ciberamenazas, medidas de prevención, protocolos de respuesta a incidentes, requisitos de complejidad de contraseñas, normas de encriptación, políticas de uso seguro de dispositivos, así como otros temas relacionados.

# Re-planificar en consecuencia

**Una vez establecidas tus prácticas de ciberseguridad, es importante probarlas y actualizarlas con regularidad para asegurarte de que siguen siendo eficaces.**

A medida que surjan nuevas amenazas o se produzcan cambios en la empresa, es esencial revisar el plan en consecuencia.

Para asegurarte de que las medidas que has puesto en marcha están haciendo su trabajo, hay varios pasos que puedes dar.

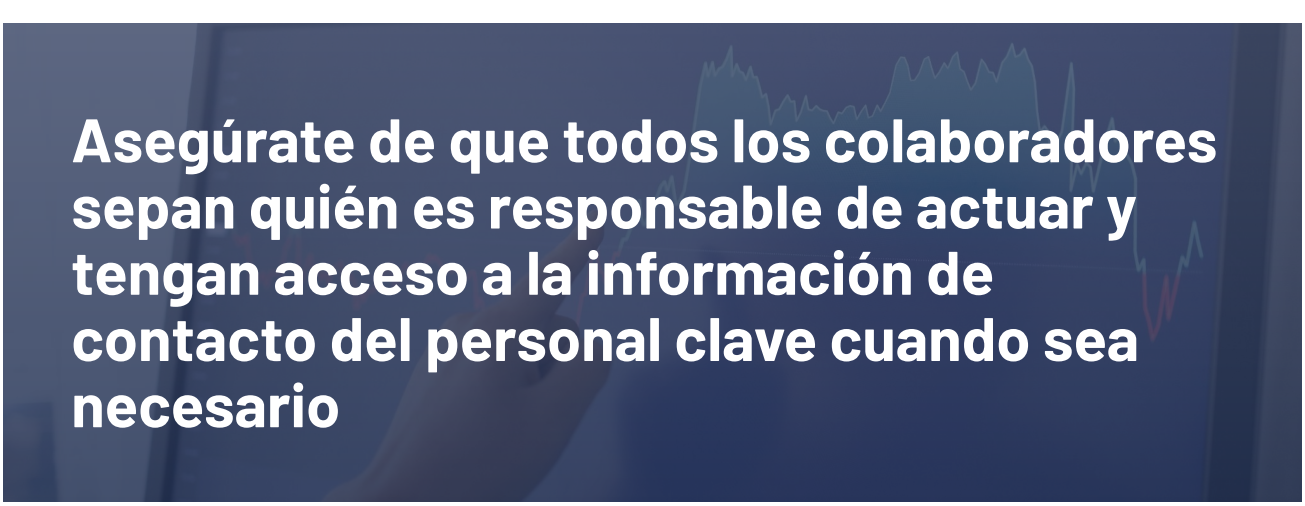
En primer lugar, imparte formación continua sobre ciberseguridad a tus empleados y asegúrate de que comprenden la importancia de la seguridad y cómo se aplica en su trabajo diario.

La formación debe abarcar temas como la identificación de correos electrónicos de phishing, la comprensión de las mejores prácticas de seguridad de contraseñas y el reconocimiento de actividades sospechosas en las redes informáticas.

Realiza periódicamente pruebas que evalúen los conocimientos de los empleados sobre las ciberamenazas e informa al área en la que se necesite instrucción adicional.

Elabora un plan exhaustivo de respuesta a incidentes que describa a quién debe notificarse en caso de violación o ataque, así como los pasos que deben darse una vez identificado el problema.

Crea un calendario de escaneos de sistemas y evaluaciones de vulnerabilidades que garantice que tus sistemas permanecen seguros a lo largo del tiempo mediante la búsqueda rutinaria de código malicioso o vulnerabilidades de software antes de que puedan ser aprovechadas por los atacantes.



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