CyberPYME 2025

GUÍA PRÁCTICA DE CIBERSEGURIDAD PARA PYMES

Protege tu empresa de amenazas digitales con pasos simples y efectivos.

HODEITEK

info@hodeitek.com
hodeitek.com

ÍNDICE

El 95% de los ciberataques se deben a errores humanos. Formar a tus empleados en ciberseguridad es la forma más efectiva de proteger tu empresa de amenazas digitales.

INTRODUCCIÓN

La guía esencial para proteger tu negocio en el mundo digital.

IMPORTANCIA

Imagina por un momento que un ciberataque pone en jaque tu negocio: datos robados, operaciones paralizadas y la confianza de tus clientes en peligro. ¿Te suena aterrador? La buena noticia es que puedes evitarlo. La ciberseguridad no es solo para grandes empresas; es una herramienta clave para que negocios como el tuyo se mantengan fuertes y seguros en un mundo digital lleno de riesgos.

OBJETIVO

Nuestro objetivo con este ebook es darte el poder de proteger tu empresa, sin necesidad de ser un experto en tecnología. Te enseñaremos pasos simples pero efectivos para que te sientas seguro frente a las amenazas digitales.

EL DESAFÍO

Sabemos que el tiempo, el presupuesto y la falta de conocimientos técnicos pueden hacer que la ciberseguridad parezca algo lejano. Sin embargo, esa percepción es lo que convierte a empresas como la tuya en objetivos fáciles para los cibercriminales. Pero no estás solo. Con esta guía, descubrirás que protegerte no es tan complicado como parece.

LA SOLUCIÓN

Este ebook te ofrece una hoja de ruta clara y práctica para que transformes el riesgo en tranquilidad. Desde las acciones más básicas hasta herramientas accesibles, aquí encontrarás todo lo que necesitas para fortalecer la seguridad de tu negocio, paso a paso.

¿POR QUÉ ES TAN URGENTE?

Las estadísticas no mienten: el 43% de los ciberataques se dirigen a empresas pequeñas y medianas. Y lo peor es que el 60% de las empresas afectadas terminan cerrando en menos de seis meses. No queremos que seas parte de esta estadística. Cada medida que tomes hoy puede ser la diferencia entre una crisis y la continuidad de tu negocio.

¿POR QUÉ ELEGIR ESTA GUÍA?

A diferencia de otras soluciones complicadas y caras, aquí te ofrecemos herramientas y estrategias diseñadas específicamente para empresas como la tuya. Esta no es una guía técnica; es una guía práctica que habla tu idioma, para que actúes con confianza desde el primer momento.

¿Por qué la ciberseguridad es esencial para las PYMES?

En un mundo cada vez más conectado, las pequeñas y medianas empresas (PYMES) se han convertido en objetivos frecuentes de los ciberataques. Aunque la atención mediática suele centrarse en los grandes hackeos a multinacionales, el **43% de los ciberataques** están dirigidos a empresas pequeñas. Esto se debe a que, a menudo, las PYMES no cuentan con medidas de seguridad adecuadas, lo que las hace vulnerables frente a amenazas digitales.

Para muchas empresas, la idea de implementar una estrategia de ciberseguridad puede parecer compleja o costosa. Sin embargo, la realidad es que no se necesita ser un experto en tecnología ni contar con presupuestos millonarios para protegerse. Este ebook está diseñado para brindarte las herramientas, el conocimiento y los pasos necesarios para fortalecer la seguridad de tu negocio de forma práctica y accesible.

El impacto de los ciberataques en las PYMES

¿Sabías que el **60% de las pequeñas empresas cierran sus puertas en los 6 meses posteriores a un ciberataque**? Esto sucede porque las consecuencias de un ataque van más allá de la pérdida de datos. Incluyen costos financieros, pérdida de confianza de los clientes y daños a la reputación que pueden ser difíciles de reparar.

Entre los riesgos más comunes que enfrentan las PYMES están:

- **Ransomware**: Secuestro de datos críticos, con exigencias de pago para su recuperación.
- **Phishing**: Correos fraudulentos que buscan engañar a los empleados para robar información.
- **Ataques de malware**: Instalación de software malicioso que daña los sistemas o roba datos sensibles.

Estos riesgos no solo afectan a las grandes empresas. Incluso un negocio pequeño puede convertirse en víctima debido a contraseñas débiles, equipos desactualizados o empleados mal informados.

¿Qué encontrarás en esta guía?

El objetivo de esta guía es ayudarte a proteger tu negocio frente a las amenazas digitales más comunes. No importa si no tienes conocimientos técnicos previos; este ebook está diseñado para ser accesible y directo. Aquí encontrarás:

- Aprenderás consejos prácticos para establecer las bases de tu ciberseguridad.
- Descubrirás herramientas recomendadas que puedes implementar fácilmente.
- Tendrás a mano un checklist para revisar y fortalecer tu seguridad digital.
- Conocerás pasos claros para reaccionar en caso de un ciberataque.

Un camino hacia la tranquilidad digital

Proteger tu PYME no solo se trata de evitar problemas, sino de garantizar que puedas operar con confianza en el mundo digital. Al seguir las recomendaciones de esta guía, estarás dando un gran paso hacia la tranquilidad y seguridad que tu negocio necesita para prosperar.
No lo pospongas más: la ciberseguridad comienza aquí y ahora. ¡Empecemos!

¡Empecemos!

¿POR QUÉ LAS PYMES SON UN OBJETIVO FÁCIL?

¿Crees que tu negocio es demasiado pequeño para atraer a los cibercriminales? Si piensas que los hackers solo se enfocan en grandes corporaciones, déjame decirte que estás cometiendo el mismo error que muchas otras PYMES. Los ciberdelincuentes saben que, en general, las pequeñas empresas no están preparadas para protegerse, y eso las convierte en un blanco fácil.

Tú también podrías estar en su radar, pero no te preocupes: con algunos ajustes sencillos que aprenderás en esta guía, puedes pasar de ser vulnerable a estar preparado.

Razones por las que las PYMES son vulnerables

RECURSOS LIMITADOS

Como propietario de una PYME, seguramente priorizas cada euro de tu presupuesto. A menudo, la ciberseguridad queda fuera de la lista porque parece cara o complicada.

Solución: Hay herramientas y pasos accesibles que puedes implementar desde hoy mismo sin afectar tus finanzas.

FALTA DE CONOCIMIENTO TÉCNICO

Puede que sientas que no entiendes lo suficiente sobre tecnología para proteger tu empresa. Eso es normal, pero no significa que debas ignorar el tema.

Solución: Con esta guía, aprenderás lo esencial sin necesidad de ser un experto en TI.

ERRORES HUMANOS

Los hackers saben que las personas son el eslabón más débil. Un clic en un enlace equivocado o una contraseña débil puede ser todo lo que necesitan para entrar.

Solución: Te mostraremos cómo formar a tu equipo y minimizar estos riesgos con pequeños ajustes.

CONFIANZA EXCESIVA

Es común pensar: “Mi negocio es demasiado pequeño para ser atacado”. Este falso sentido de seguridad es lo que te puede dejar más expuesto.

Solución: Proteger tu empresa no significa invertir una fortuna, solo tomar medidas inteligentes para evitar sorpresas desagradables.

El impacto es real, pero puedes prevenirlo

Un ciberataque puede detener tus operaciones, poner en riesgo los datos de tus clientes y afectar tu reputación. No queremos que te conviertas en una de esas estadísticas donde el **60% de las PYMES cierra tras un ataque**. Este ebook está aquí para cambiar eso.

EJEMPLO REAL

Un negocio familiar en España fue víctima de un phishing y **perdió 15.000€** en una transferencia bancaria fraudulenta. Todo se debió a un clic en un correo falso. Podrías pensar que algo así nunca te sucederá, pero ¿estás realmente seguro?

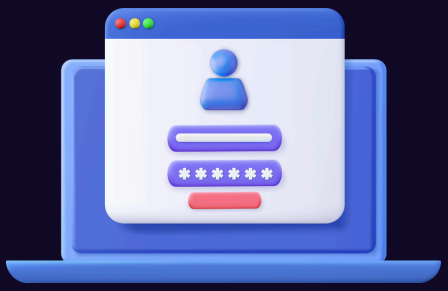
El primer paso hacia la acción

La buena noticia es que proteger tu negocio no tiene por qué ser complicado. Con pequeñas acciones que aprenderás en esta guía, puedes marcar una gran diferencia y hacer que los cibercriminales te vean como un objetivo difícil. La ciberseguridad está a tu alcance. ¿Qué esperas para empezar?

LAS BASES DE LA CIBERSEGURIDAD PARA TU NEGOCIO

Proteger tu negocio no tiene que ser complicado. A menudo, las acciones más simples son las que tienen mayor impacto. ¿Sabías que medidas básicas como usar contraseñas seguras o mantener tus sistemas actualizados pueden prevenir hasta el **80% de los ciberataques**? En esta sección, te guiaremos paso a paso para que establezcas las bases de la ciberseguridad en tu empresa.

Recuerda: No se trata de hacerlo todo de golpe, sino de empezar con pequeñas acciones que generen grandes resultados. ¡Vamos allá!



USA CONTRASEÑAS FUERTES Y SEGURAS

Por qué es importante:
Las contraseñas débiles son como dejar la puerta abierta para los hackers. Un atacante puede adivinar fácilmente combinaciones simples como "123456" o "password".

Qué hacer:

- Utiliza contraseñas de al menos **12 caracteres**, mezclando **letras mayúsculas, minúsculas, números y símbolos**.
-
- Evita usar la misma contraseña en diferentes cuentas.

- Considera usar un gestor de contraseñas para generar y guardar contraseñas seguras de manera fácil.

USA AUTENTICACIÓN EN DOS PASOS (2FA)

Por qué es importante:
Incluso si alguien logra obtener tu contraseña, la autenticación en dos pasos agrega una capa adicional de protección.

Qué hacer:

- Activa la **autenticación en dos pasos** en todas las cuentas que lo permitan.
- Usa aplicaciones como Google Authenticator o Authy para generar códigos de acceso temporales.

ACTUALIZACIONES AUTOMÁTICAS

Por qué es importante:
El software desactualizado tiene vulnerabilidades que los hackers pueden explotar. Mantener todo actualizado cierra esas brechas de seguridad.

Qué hacer:

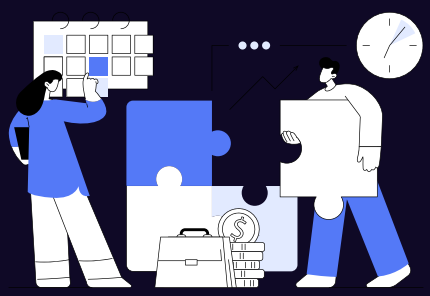
- Configura actualizaciones automáticas para tus sistemas operativos, aplicaciones y programas de seguridad.
- Si usas herramientas específicas para tu negocio, revisa que estén siempre en su última versión.

REALIZA COPIAS DE SEGURIDAD REGULARES

Por qué es importante:
Los ciberataques como el ransomware pueden bloquearte el acceso a tus datos. Tener una copia de seguridad te asegura que no perderás información valiosa.

Qué hacer:

- Realiza **copias de seguridad automáticas al menos una vez por semana**.
- Usa soluciones en la nube o discos externos seguros para almacenar tus backups.
- Verifica periódicamente que las copias sean funcionales.



LIMITA EL ACCESO A LA INFORMACIÓN

Por qué es importante:
No todos en tu empresa necesitan acceso a toda la información. Limitar los permisos puede reducir el riesgo de fugas o errores.

Qué hacer:

- Define **roles y permisos claros** para cada miembro de tu equipo.
- Asegúrate de que solo las personas necesarias tengan acceso a datos sensibles.

La ciberseguridad es un hábito. Cuanto más implementes estas prácticas básicas, más protegido estará tu negocio frente a amenazas digitales.

Empieza hoy con las prácticas de esta guía y fortalece tu negocio frente a cualquier amenaza.

CÓMO INVOLUCRAR A TU EQUIPO EN LA CIBERSEGURIDAD

La ciberseguridad no es solo responsabilidad del dueño del negocio o del departamento de TI, ¡es un esfuerzo de todo el equipo! Los empleados son la primera línea de defensa contra los ciberataques, pero también pueden ser el eslabón más débil si no están preparados. En esta sección, aprenderás cómo convertir a tu equipo en aliados clave para proteger tu empresa.

1. **Educa a tu equipo en los conceptos básicos**
2. **Establece políticas claras de seguridad**
3. **Simula ataques para medir la preparación**
4. **Crea un ambiente de confianza**
5. **Nombra embajadores de ciberseguridad**

EDUCA A TU EQUIPO EN LOS CONCEPTOS BÁSICOS

Por qué es importante:
La mayoría de los ciberataques comienzan con **errores humanos**, como hacer clic en un enlace sospechoso o usar contraseñas débiles. Si tu equipo no entiende los riesgos, no podrá evitarlos.

Qué hacer:

- Organiza sesiones breves de formación en ciberseguridad (pueden ser mensuales o trimestrales).
- Usa ejemplos prácticos, como reconocer un correo de phishing o crear contraseñas seguras.
- Comparte recursos, como tutoriales en línea o guías rápidas, que sean fáciles de entender y aplicar.

ESTABLECE POLÍTICAS CLARAS DE SEGURIDAD

Por qué es importante:
Sin normas claras, cada persona puede interpretar la seguridad a su manera, lo que deja a tu empresa vulnerable.

Qué hacer:

- Define políticas sencillas como:
  - Cambiar contraseñas cada 3 meses.
  - No acceder a información sensible desde redes Wi-Fi públicas.
  - Usar solo dispositivos aprobados por la empresa.
- Comunica estas políticas de manera regular y asegúrate de que todos las comprendan.

SIMULA ATAQUES PARA MEDIR LA PREPARACIÓN

Por qué es importante:
Las simulaciones ayudan a identificar puntos débiles en el equipo antes de que un atacante real los descubra.

Qué hacer:

- Realiza simulaciones de phishing: envía correos falsos y mide cuántas personas hacen clic.
- Ofrece retroalimentación inmediata y utiliza los resultados para reforzar las formaciones.
- Evalúa el cumplimiento de las políticas de seguridad periódicamente.

Por ejemplo, prueba enviar un correo de phishing interno que simule una oferta laboral falsa y analiza los resultados.

CREA UN AMBIENTE DE CONFIANZA

Por qué es importante:
Si los empleados tienen miedo de reportar errores, podrías no enterarte de un incidente hasta que sea demasiado tarde.

Qué hacer:

- Anima a tu equipo a reportar cualquier actividad sospechosa sin miedo a ser culpados.
- Reconoce los esfuerzos de aquellos que sigan las mejores prácticas de seguridad.
- Establece un canal claro y accesible para reportar problemas, como un correo dedicado o un chatbot interno.

NOMBRA EMBAJADORES DE CIBERSEGURIDAD

Por qué es importante:
Tener personas dentro del equipo que sean responsables de promover la ciberseguridad ayuda a reforzar el compromiso de todos.

Qué hacer:

- Elige a empleados clave que puedan actuar como embajadores o líderes de ciberseguridad.
- Proporciónales formación adicional para que puedan apoyar al resto del equipo.
- Reconoce públicamente su rol para motivar al resto del personal.

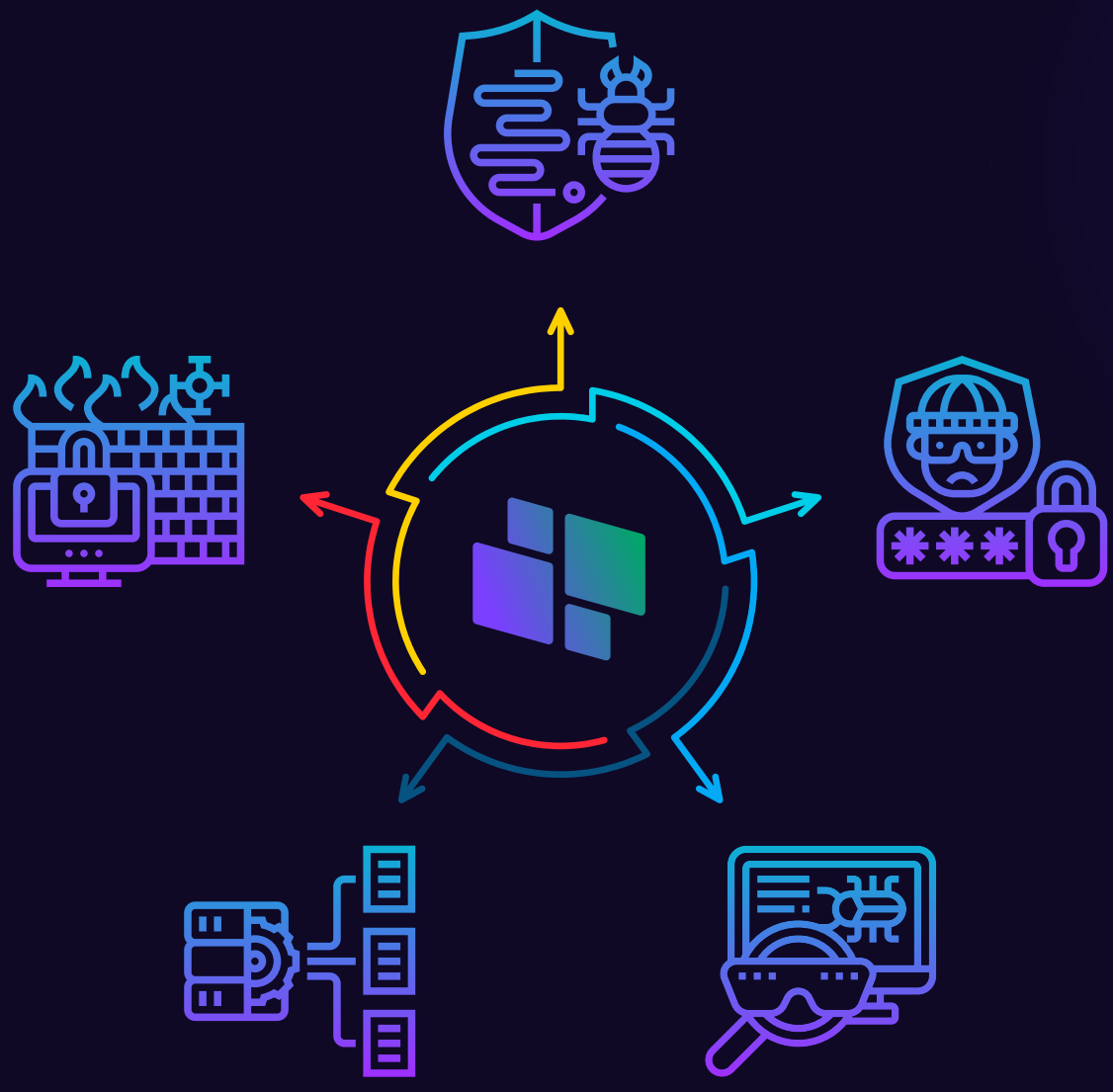
La ciberseguridad es un esfuerzo compartido.

Cuando todos en tu equipo están informados y comprometidos, la seguridad de tu empresa mejora exponencialmente. Empieza hoy mismo a **educar, motivar y preparar a tu equipo** para que sean defensores activos de tu negocio.

Próximo paso: Implementa al menos una de estas estrategias esta semana. ¡Cada pequeño paso cuenta!

HERRAMIENTAS ESENCIALES DE CIBERSEGURIDAD PARA PYMES

La ciberseguridad requiere no solo estrategias y educación, sino también herramientas que fortalezcan la protección de tu negocio. En Hodeitek, sabemos que elegir las soluciones adecuadas puede marcar la diferencia. Aquí te presentamos las herramientas esenciales para PYMES, pensadas para que des un gran paso hacia la seguridad digital.



SOLUCIONES EDR (ENDPOINT DETECTION AND RESPONSE)

Por qué es importante:

Los ataques avanzados como el ransomware necesitan herramientas que puedan detectar y responder a amenazas en tiempo real. El EDR es la evolución de los antivirus tradicionales, diseñado para proteger cada dispositivo de tu red.

Herramientas recomendadas:

- **Kaspersky Endpoint Detection and Response:** Ideal para PYMES que buscan una solución efectiva y accesible.
- **Bitdefender GravityZone:** Protección avanzada con detección basada en inteligencia artificial.
- **SentinelOne:** Una opción robusta que automatiza la respuesta ante incidentes.

Cómo implementarlo:

- Configura EDR en todos los dispositivos críticos de tu empresa para detectar amenazas antes de que causen daño.
- Asegúrate de contar con monitorización continua y respuesta rápida.

En Hodeitek, podemos ayudarte a implementar y gestionar estas soluciones de manera eficiente.

GESTORES DE CONTRASEÑAS

Por qué es importante:

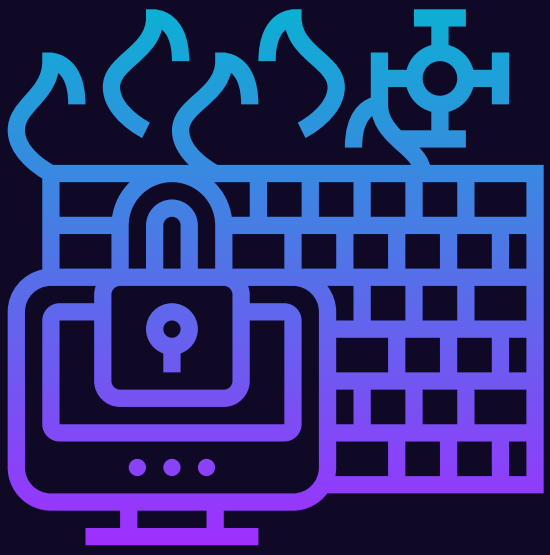
Las contraseñas son la primera barrera de acceso a tus sistemas. Usar un gestor de contraseñas ayuda a tu equipo a mantener sus credenciales seguras sin complicaciones.

Herramientas recomendadas:

- **LastPass:** Solución sencilla y segura para equipos pequeños.
- **Dashlane:** Genera y almacena contraseñas seguras, con auditorías incluidas.
- **1Password:** Ideal para entornos colaborativos.

Cómo implementarlo:

- Integra un gestor de contraseñas en tu empresa y forma a tu equipo para usarlo correctamente.



FIREWALLS EMPRESARIALES AVANZADOS

Por qué es importante:

Los firewalls son esenciales para proteger la red de tu empresa, actuando como una barrera entre tus sistemas internos y amenazas externas. Los firewalls avanzados no solo filtran el tráfico, sino que también identifican patrones sospechosos.

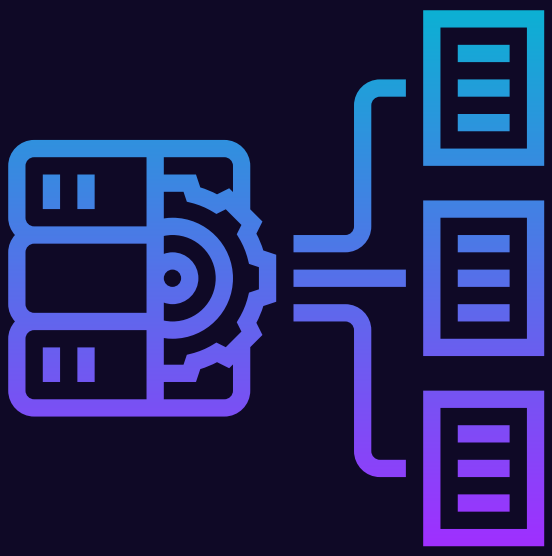
Herramientas recomendadas:

- **Palo Alto Networks:** Seguridad de red avanzada, ideal para empresas en crecimiento.
- **Fortinet:** Soluciones flexibles con capacidades integradas de filtrado web y control de aplicaciones.

Cómo implementarlo:

- Consulta con especialistas para desplegar un firewall adaptado a tus necesidades específicas.
- Realiza auditorías regulares para garantizar su eficacia.

Hodeitek ofrece la gestión de firewalls para asegurar una protección constante y optimizada.



COPIAS DE SEGURIDAD

Por qué es importante:

Un ciberataque puede comprometer tus datos y paralizar tu operación. Tener un servicio gestionado de copias de seguridad asegura que siempre tengas acceso a la información clave, sin importar lo que ocurra.

Herramienta recomendada:

- **Hodeitek Backup Management Service:** Un servicio diseñado para PYMES que necesitan copias de seguridad automáticas y seguras, gestionadas por expertos.

Cómo implementarlo:

- Configura copias de seguridad automáticas en sistemas externos o en la nube.

- Permite que un equipo especializado como Hodeitek supervise tus backups para garantizar su funcionalidad.

CTI Y VMAAS (CYBER THREAT INTELLIGENCE Y VULNERABILITY MANAGEMENT AS A SERVICE)

Por qué es importante:

La inteligencia de amenazas (CTI) y la gestión de vulnerabilidades (VMaaS) son servicios que te permiten anticiparte a los ataques y reforzar tus puntos débiles antes de que los atacantes los exploten.

Herramientas recomendadas:

- **Hodeitek CTI Service:** Accede a informes de inteligencia de amenazas para prevenir ataques dirigidos.
- **Hodeitek VMaaS:** Evalúa continuamente las vulnerabilidades en tus sistemas y recibe soluciones proactivas.

Cómo implementarlo:

- Integra un servicio gestionado que te permita identificar y mitigar riesgos de manera continua.
- Usa los informes generados para mejorar tu postura de seguridad.

Empieza con las herramientas que más necesites

No tienes que implementarlo todo de golpe. En Hodeitek, podemos ayudarte a priorizar las herramientas y servicios que mejor se adapten a tu negocio, asegurando que tu empresa esté protegida con soluciones accesibles y efectivas.

Próximo paso: Contáctanos para recibir una evaluación inicial y descubrir cómo estas soluciones pueden proteger tu empresa de manera inmediata.

CÓMO RESPONDER A UN CIBERATAQUE

Por mucho que implementes medidas preventivas, ningún sistema es 100% infalible. En el desafortunado caso de un ciberataque, actuar rápidamente puede marcar la diferencia entre un daño controlado y una crisis devastadora. Esta sección te guiará en los pasos clave para responder eficazmente ante un incidente de seguridad.

1

Mantén la calma y evalúa la situación

Por qué es importante:
La reacción inicial ante un ataque puede empeorar la situación si no es controlada. Mantener la calma te ayudará a tomar decisiones acertadas.

Qué hacer:

- Identifica el alcance del ataque: ¿Qué sistemas han sido afectados?
- Evalúa si se trata de un incidente menor (como un phishing) o de un ataque más complejo (ransomware o intrusión).
- Documenta todo lo que notes, como mensajes de error, archivos comprometidos o cualquier actividad sospechosa.

2 Aísla los sistemas afectados

Por qué es importante:
Evitar la propagación del ataque es crucial para minimizar el daño.

Qué hacer:

- Desconecta inmediatamente los dispositivos afectados de la red.
- Si se trata de un servidor o sistema crítico, consulta con un especialista antes de apagarlo.
- Usa tus sistemas de respaldo (si están disponibles) para mantener la operación.

En Hodeitek, ofrecemos soporte inmediato para aislar y contener ataques.

3 Contacta a tu proveedor de ciberseguridad o especialista

Por qué es importante:
Un ciberataque puede ser complejo y requerir experiencia técnica avanzada para manejarlo adecuadamente.

Qué hacer:

- Informa a tu proveedor de servicios de ciberseguridad (como Hodeitek) para una respuesta rápida y especializada.
- Si no tienes un proveedor, busca ayuda profesional de un equipo de respuesta a incidentes (CSIRT).
- Comparte toda la documentación del incidente para facilitar la investigación.

4 Identifica y neutraliza la causa

Por qué es importante:
Resolver el ataque sin identificar la causa puede dejar tu sistema vulnerable a nuevos incidentes.

Qué hacer:

- Analiza el origen del ataque: ¿Fue un correo fraudulento? ¿Una vulnerabilidad en el sistema?
- Usa herramientas de análisis de seguridad para identificar brechas específicas.
- Revisa los logs de actividad y busca patrones inusuales.

5 Restaura y refuerza la seguridad

Por qué es importante:
Después de neutralizar el ataque, debes recuperar los datos y fortalecer tu infraestructura para evitar que vuelva a ocurrir.

Qué hacer:

- Restaura los datos desde tus copias de seguridad.
- Cambia todas las contraseñas relacionadas con los sistemas afectados.
- Actualiza las herramientas de seguridad y verifica que todos los sistemas estén al día.

Hodeitek puede ayudarte a reforzar tu ciberseguridad con servicios como CTI y VMaaS para monitorizar y prevenir futuros ataques.

6 Comunica y aprende del incidente

Por qué es importante:
Mantener la confianza de tus clientes y equipo depende de una comunicación clara y transparente. Además, cada incidente es una oportunidad de aprendizaje.

Qué hacer:

- Notifica a las partes afectadas (clientes, proveedores, empleados) si el ataque compromete información sensible.
- Documenta todos los pasos que seguiste durante la respuesta al ataque para mejorar tus protocolos.
- Realiza una sesión de retroalimentación con tu equipo y proveedor de ciberseguridad para implementar mejoras.

Recuerda: La velocidad y la preparación son clave

Un ciberataque puede ser un gran desafío, pero con los pasos adecuados y el soporte de expertos como Hodeitek, puedes minimizar el impacto y salir adelante.

Próximo paso: Evalúa tu plan de respuesta ante incidentes y ajusta cualquier punto débil que encuentres. ¡Estar preparado marca la diferencia!

CHECKLIST DE SEGURIDAD

Paso	Descripción	Estado (☑)
Contraseñas fuertes	Usa contraseñas de al menos 12 caracteres con letras, números y símbolos. Cambia cada 3 meses.	
Gestor de contraseñas	Implementa un gestor para organizar y proteger todas las contraseñas.	
Autenticación en dos pasos (2FA / MFA)	Activa 2FA en todas las cuentas críticas usando apps como Google Authenticator.	
Implementación de EDR	Configura y supervisa un EDR como Kaspersky, Bitdefender o SentinelOne para monitorear y responder amenazas en tiempo real.	
Actualizaciones automáticas	Configura actualizaciones automáticas para sistemas, software y EDR.	
Copias de seguridad regulares	Realiza backups automáticos en la nube o discos externos, y prueba su funcionalidad periódicamente.	
Acceso limitado a datos sensibles	Define roles y permisos claros para el equipo. Revisa accesos regularmente.	
Formación en ciberseguridad	Organiza talleres para educar al equipo en ciberseguridad.	
Plan de respuesta a incidentes	Diseña un protocolo claro para actuar en caso de ciberataque.	
Firewalls empresariales avanzados	Implementa firewalls de Palo Alto o Fortinet para proteger la red.	
Servicios gestionados	Contrata servicios gestionados como backups, CTI o VMaaS para mayor protección.	

ESTAMOS AQUÍ PARA AYUDARTE

HODEITEK

La ciberseguridad no es una opción, es una necesidad. Contáctanos hoy y construyamos juntos un entorno digital más seguro para tu PYME

¡RESERVA AQUI TU CONSULTA GRATUITA!

✉️ **Correo electrónico:**
info@hodeitek.com

🌐 **Sitio web:**
hodeitek.com/es

💬 **WhatsApp**
+34 722 18 41 02

📞 **Teléfono:**
+34 747 42 45 03