10 Acciones para Mejorar la Ciberseguridad

Su plan de acción para una ciberseguridad más sólida y una infraestructura de TI resiliente.

Todos hemos visto el daño que pueden causar los ciberataques: operaciones interrumpidas, reputaciones dañadas y pérdidas financieras significativas. En América Latina, estas amenazas están evolucionando más rápido que nunca. Pero una ciberseguridad sólida no tiene por qué ser complicada.

Nuestra lista práctica y sencilla está diseñada para ayudar a su empresa a fortalecer sus defensas rápidamente. Cada acción es fácil de seguir y obtendrá medidas claras junto con una mayor confianza en su estrategia de ciberseguridad.

1. Comprenda cuales son sus principales riesgos cibernéticos

Los ciberataques están aumentando en toda América Latina poniendo a las empresas en mayor riesgo. En la primera mitad de 2024, solo México representó más de la mitad de los ataques reportados en la región. Entender estas amenazas es el primer paso para fortalecer sus defensas. Aquí le mostramos cómo mantenerse un paso adelante:

- ☐ Suscríbase a fuentes confiables de noticias sobre ciberseguridad enfocadas en LATAM. También puede consultar The Hacker News, IT Sitio y Ciberseguridad LATAM.
- ☐ Participe en webinars o eventos regionales de ciberseguridad para obtener información sobre ransomware, tácticas de phishing y otras amenazas dirigidas a negocios locales.
- ☐ Brinde capacitación mensual concisa para su equipo, empleados y clientes para resaltar tendencias clave de ciberseguridad y amenazas emergentes.

2. Convierta a sus empleados en su primera línea de defensa

Los empleados pueden ser su defensa más fuerte o su eslabón más débil. Los correos electrónicos de phishing y las estafas por WhatsApp son especialmente frecuentes en América Latina, pero invertir en capacitación constante puede reducir significativamente su riesgo:

- ☐ Programe sesiones regulares de capacitación en ciberseguridad con ejemplos del mundo real.
- ☐ Realice simulaciones de phishing periódicas para evaluar y mejorar la conciencia de los empleados.
- ☐ Monitoree proactivamente la web oscura, estableciendo alertas para credenciales filtradas o información sensible relacionada con su negocio.

3. Audite y evalúe su seguridad regularmente

A menudo, debido a limitaciones presupuestarias, falta de conocimiento o miedo a interrumpir operaciones, muchas empresas en América Latina siguen utilizando software obsoleto, lo cual las deja vulnerables a ataques. Las evaluaciones regulares de seguridad pueden ayudarle a identificar y corregir vulnerabilidades antes de que se conviertan en problemas graves.

- ☐ Analice sus sistemas expuestos a internet para detectar puntos de entrada no seguros o vulnerabilidades.
- ☐ Revise los permisos de red e identifique configuraciones incorrectas o fugas de protocolos.
- ☐ Asegure las redes inalámbricas para prevenir accesos no autorizados.

4. Asegure el trabajo remoto con soluciones VPN robustas

El trabajo híbrido y remoto se ha convertido en la norma, pero esto también ha incrementado la dependencia de conexiones a internet inseguras y puntos de acceso Wi-Fi. Proteja a su fuerza laboral remota o clientes educándolos sobre evitar Wi-Fi público y siempre utilizar soluciones móviles VPN seguras. Aquí le mostramos cómo abordar este desafío:

- ☐ Encripte siempre el tráfico de internet de los empleados con protocolos VPN robustos como L2TP/IPsec u OpenVPN.
- ☐ Utilice soluciones de gestión de endpoints para configurar, administrar y monitorear el uso de VPN en toda su fuerza laboral.
- ☐ Automatice las reconexiones VPN para garantizar que su equipo permanezca continuamente protegido, sin importar desde dónde se conecten.

5. Establezca una política sólida para dispositivos personales con MFA

El uso de dispositivos personales para el trabajo difumina la línea entre el uso empresarial y personal, creando riesgos de seguridad. Para proteger los datos sensibles, establezca políticas claras y haga cumplir medidas como la autenticación multifactor (MFA). Aquí le mostramos cómo:

- ☐ Defina claramente los estándares mínimos de seguridad requeridos para dispositivos personales utilizados para negocios.
- ☐ Exija certificados SSL para autenticar de manera segura los dispositivos en su red.
- ☐ Implemente contraseñas fuertes y únicas, inicio de sesión único (SSO) y MFA utilizando aplicaciones autenticadoras o llaves de seguridad físicas en lugar de verificación por SMS.
- ☐ Establezca procedimientos seguros para borrar datos de dispositivos personales cuando los empleados abandonen su organización.

6. Mantenga la seguridad mediante la gestión de vulnerabilidades

Las actualizaciones de software pueden parecer una molestia, pero retrasarlas pone a su empresa en riesgo. Los ciberdelincuentes explotan activamente software desactualizado, convirtiendo vulnerabilidades sin parchar en puntos de entrada fáciles. Aquí le mostramos cómo asegurarse de que su sistema se mantenga protegido sin esfuerzo manual:

- ☐ Utilice un sistema de gestión de endpoints que despliegue automáticamente parches críticos en todos sus dispositivos.
- ☐ Obtenga visibilidad en tiempo real del estado de parches de toda su red para identificar rápidamente las brechas.
- ☐ Programe análisis regulares de vulnerabilidades con respuestas automatizadas para corregir fallas antes de que puedan ser explotadas.

---

7. Prepare su estrategia de respaldo y recuperación para el futuro

Ninguna solución de seguridad es infalible. Los ciberataques, fallas de hardware y errores humanos aún pueden poner en riesgo sus datos. Proteja su negocio creando respaldos confiables, especialmente fuera de línea o desconectados (air-gapped), que los atacantes no puedan comprometer. Considere estas mejores prácticas:

- ☐ Integre sus soluciones de respaldo en su plataforma de gestión de endpoints, simplificando la recuperación durante emergencias.
- ☐ Automatice sus pruebas de respaldo de manera regular.
- ☐ No olvide sus aplicaciones SaaS como Microsoft 365 o Google Workspace. Respáldelas regularmente para proteger datos esenciales en la nube.

---

8. Proteja su negocio de amenazas internas

En América Latina, las amenazas internas provenientes de empleados descontentos o que abandonan la empresa son una preocupación importante. Estas amenazas pueden causar filtraciones de datos graves o incluso sabotaje. Para gestionar proactivamente estos riesgos internos, fortalezca su plan de respuesta ante amenazas internas:

- ☐ Monitoree regularmente los comportamientos de inicio de sesión, detectando rápidamente actividades inusuales como accesos fuera de horario laboral o desde ubicaciones inesperadas.
- ☐ Limite el acceso privilegiado estrictamente al personal esencial y realice auditorías frecuentes para asegurar que los permisos sean apropiados.
- ☐ Configure alertas automatizadas para detectar y responder de inmediato a actividades sospechosas o no autorizadas en la red, minimizando el daño potencial.

9. Mejore su protección de endpoints

El software antivirus básico ya no es suficiente, especialmente contra amenazas avanzadas como exploits de día cero o ransomware sofisticado. Su protección de endpoints debe mantenerse al día con los riesgos cibernéticos modernos, incluyendo soluciones confiables de EDR. Aquí le mostramos cómo mejorar sus defensas:

- ☐ Implemente herramientas avanzadas de EDR para detectar, analizar y responder a amenazas en tiempo real, reduciendo significativamente el riesgo de violaciones graves.
- ☐ Aplique funciones de remediación automatizada para contener amenazas rápidamente con mínima interrupción de sus operaciones.
- ☐ Monitoree continuamente la actividad de los endpoints para identificar y detener comportamientos sospechosos antes de que escalen.

10. Prepárese proactivamente para cualquier desastre

El peor momento para darse cuenta de que no está preparado para un ciberataque es cuando sucede. Muchas empresas en América Latina aún carecen de un plan claro y probado de respuesta a incidentes. No deje su seguridad al azar. Haga de la preparación proactiva su prioridad siguiendo estos pasos:

- ☐ Defina claramente los roles y responsabilidades de cada miembro de su equipo de respuesta a incidentes para evitar confusiones durante crisis.
- ☐ Documente un plan detallado de continuidad del negocio que aborde específicamente amenazas cibernéticas como ransomware o violaciones de datos, adaptado a las operaciones de su empresa.
- ☐ Realice ejercicios prácticos periódicos y simulaciones de ataques para mejorar la preparación de su equipo.
- ☐ Documente cuidadosamente los procesos críticos de recuperación de datos para restaurar operaciones rápida y eficazmente si ocurre un ataque.

¿Quiere mantenerse a la vanguardia de las ciberamenazas con Datto?

Las amenazas cibernéticas no se están desacelerando, y mantenerse un paso adelante es clave para mantener su negocio seguro. Para hacerlo de manera efectiva, necesita las herramientas adecuadas.

Con Datto RMM y Datto EDR, las empresas pueden automatizar parches y obtener monitoreo en tiempo real en un sistema simplificado. Aprenda más sobre cómo Datto puede ayudar a su negocio a mantenerse protegido contra las amenazas que afectan a América Latina.

Haz clic aquí para aprender más

datto
A Kaseya COMPANY