SENDMARC

Lista de verificación contra ransomware

El ransomware es el tipo de **ciberdelito que más crece** en el mundo y representa una amenaza urgente para empresas de todos los tamaños. Cada vez hay más ataques, más sofisticados y con un impacto más costoso.

Esta lista de verificación te ayudará a evaluar si tu empresa está lista para prevenir ataques de ransomware y recuperarse con rapidez y efectividad.

Se estima que el ransomware costará a las víctimas US$ 265.000 millones anuales para 2031

72%+

Más del 72% de las empresas sufrieron ataques de ransomware en 2023, el nivel más alto registrado

Para 2031, se espera un ataque cada 2 segundos

1 Identificar posibles puntos de entrada

Conoce por dónde podría entrar el ransomware.

- [ ] ¿Tienes visibilidad sobre todas las fuentes de correo electrónico entrante?
- [ ] ¿Tus dominios están protegidos contra el phishing, spoofing y otras formas de suplantación?
- [ ] ¿Los accesos remotos están protegidos y monitoreados?
- [ ] ¿Revisas periódicamente integraciones con terceros y proveedores?
- [ ] ¿Realizas auditorías de seguridad sobre tus configuraciones en la nube?

2 Evalúa tu preparación para prevenir ataques

Analiza si tus defensas existentes pueden detener los ataques antes de que se propaguen.

- [ ] ¿Tienes DMARC implementado con política p=reject?
- [ ] ¿SPF y DKIM están configurados y monitoreados correctamente?
- [ ] ¿Cuentas con reportes proactivos sobre tu ecosistema de correo?
- [ ] ¿Tienes habilitada la autenticación multifactor (MFA)?
- [ ] ¿Aplicas actualizaciones y parches de software de forma regular?
- [ ] ¿Tu equipo recibe formación sobre phishing y ciberseguridad?

3 Verifica tu preparación para responder a incidentes

¿Puedes actuar de forma rápida y eficaz si a tu empresa la afecta un ataque de ransomware?

- [ ] ¿Tienes un plan de respuesta a incidentes probado y activo?
- [ ] ¿Cuentas con un protocolo específico para ataques de ransomware?
- [ ] ¿Tienes copias de seguridad seguras, fuera de línea y protegidas contra alteraciones?
- [ ] ¿Ya identificaste socios externos clave (jurídico, forense, comunicación) para responder rápido?

4 Refuerza tu capacidad de recuperación y resiliencia

¿Qué sucede después de un ataque de este tipo?

- [ ] ¿Puedes restaurar tus sistemas desde backups limpios de forma rápida?
- [ ] ¿Tienes un plan de continuidad de negocio documentado y actualizado?
- [ ] ¿Analizas los incidentes y aplicas las lecciones aprendidas?
- [ ] ¿Tu presupuesto prioriza mejoras continuas de seguridad?

5 Implementa defensas proactivas

- [ ] El 95% de las empresas aumentaron su presupuesto de prevención para 2025.
  ¿Ya lo hizo tu organización?

Al implementar el protocolo Domain-based Message Authentication, Reporting, and Conformance (DMARC) con una política de p=reject puedes evitar que tu organización sea víctima de un ataque de ransomware. ¿Cómo? Bloqueando uno de los principales vectores de entrada: la suplantación de identidad por correo electrónico.

Los beneficios de DMARC con Sendmarc incluyen:

Confianza

Impide que se envíen correos falsos desde tu dominio y garantiza que todos los destinatarios puedan confiar en los correos electrónicos que reciben de tu parte.

Visibilidad

Nuestros reportes DMARC recopilan datos de servidores de todo el mundo, los convierten en información práctica y te permiten saber quién envía correos desde su dominio.

Entrega

Las políticas y cumplimiento pleno de DMARC garantizan que todos tus correos legítimos lleguen a la bandeja de entrada deseada, no a spam o correo no deseado.

Conformidad

Sendmarc garantiza el cumplimiento de los estándares globales y la conformidad de los servicios de correo utilizados por cada sector de una compañía.

¿Estás listo/a para fortalecer tus defensas contra el ransomware?

Asegurémonos de que tu correo electrónico no sea tu eslabón más débil:

Solicita una demo | Pruebe su dominio ahora | Prueba gratuita