INTERLACE

Run Free. Grow Better.

GUÍA DE AUTOEVALUACIÓN / CIBERSEGURIDAD

Guía de Autoevaluación: ¿está tu empresa lista para una brecha de seguridad?

Identifica tus brechas. Actúa a tiempo. No esperes a que un ataque te lo diga.

Adaptada al español por INTERLACE, partner e implementador de SentinelOne Singularity XDR en México.
Basada en el Breach Readiness Self-Assessment Guide de SentinelOne.

Introducción

Conforme los ciberataques se vuelven más rápidos, más encubiertos y más dañinos, incluso las organizaciones mejor equipadas en herramientas se encuentran sin preparación cuando ocurre un incidente real. Las alertas se acumulan, el contexto queda incompleto, y los equipos se ven forzados a tomar decisiones de alto impacto bajo presión, muchas veces sin la claridad o la experiencia necesaria para actuar con decisión.

Mientras muchos programas de seguridad se concentran en prevención y detección, la protección real depende de la preparación: la capacidad de entender rápidamente qué está pasando, contener el impacto y responder con confianza a través de equipos técnicos, operativos y de negocio. Sin embargo, para muchas organizaciones, las brechas de visibilidad, validación y planeación de respuesta permanecen ocultas hasta que ocurre una brecha de seguridad.

Usa la siguiente autoevaluación para identificar posibles brechas en cinco dimensiones clave de preparación. Para cada área, reflexiona con honestidad sobre tu estado actual. Las áreas donde no puedas responder "sí" con confianza representan oportunidades para fortalecer tu postura, y posibles puntos de entrada para un atacante.

Las dimensiones y los criterios de evaluación de esta guía están alineados con marcos ampliamente reconocidos como NIST CSF, SANS y las guías de CISA, y están informados por hallazgos comunes en investigaciones reales de respuesta a incidentes. Esta guía está diseñada para iniciar una conversación, no para cerrarla. Donde aparezcan brechas, en INTERLACE podemos ayudarte a convertir esos hallazgos en un plan de acción con SentinelOne Singularity XDR.

---

1 Detección y Visibilidad

Pregunta diagnóstica

¿Puedes ver y confiar en lo que sucede en tu entorno en tiempo real?

- Tienes visibilidad en tiempo real sobre endpoints, identidades, cargas de trabajo en la nube y tráfico de red.
- Las detecciones de comportamiento identifican actividad sospechosa más allá de los indicadores de compromiso (IOC) conocidos.
- La telemetría y los registros se conservan el tiempo suficiente para respaldar investigaciones retrospectivas (considera tus mínimos regulatorios).
- La lógica de detección se valida regularmente contra técnicas reales de atacantes (por ejemplo, el marco MITRE ATT&CK).
- Los registros se almacenan de forma segura y protegidos contra manipulación o destrucción por parte de actores maliciosos.
- Puedes determinar rápidamente el alcance, la línea de tiempo y el radio de impacto de un incidente.

Por qué importa esta brecha

Los puntos ciegos retrasan la contención, permiten que los atacantes persistan sin ser detectados y extienden el tiempo de permanencia dentro de la red, aumentando el daño y el costo de la investigación. Las organizaciones que detectan brechas aquí suelen carecer de un camino claro y preestablecido hacia una respuesta experta cuando más lo necesitan.

2 Caza de Amenazas y Defensa Proactiva

Pregunta diagnóstica

¿Se cazan amenazas de forma proactiva, o tu equipo solo investiga después de que suena una alerta?

- La caza de amenazas (threat hunting) se realiza de forma continua, no de manera improvisada o solo después de un incidente conocido.
- Los analistas prueban hipótesis a lo largo de toda la cadena de ataque, no solo responden a alertas de alta severidad.
- Las señales débiles o tempranas de un atacante se investigan activamente antes de que escalen.
- Las brechas de cobertura de detección se identifican mediante resultados de caza y evaluaciones periódicas (por ejemplo, un análisis trimestral contra MITRE ATT&CK).
- Los hallazgos de la caza retroalimentan mejores detecciones, analítica e inteligencia de amenazas.

Por qué importa esta brecha

Los ataques avanzan en silencio hasta que el daño ya está hecho. Los equipos que solo reaccionan enfrentan de forma consistente mayores tiempos de permanencia del atacante y mayor impacto. Las organizaciones sin un programa de caza proactiva suelen descubrir las amenazas más tarde, cuando el costo de la respuesta ya es mucho mayor.

3 Preparación para la Respuesta a Incidentes

Pregunta diagnóstica

¿Puede tu equipo actuar de forma decisiva y correcta en las primeras horas críticas de un incidente?

- Los roles, responsabilidades y rutas de escalamiento de respuesta a incidentes están claramente definidos por escrito (modelo RACI o equivalente).
- Existen playbooks de respuesta, se mantienen actualizados y se han probado en ejercicios reales, no solo documentados.
- Puedes contratar rápidamente expertos en DFIR (Digital Forensics and Incident Response) sin retrasos de procuración, por ejemplo, mediante un contrato preestablecido.
- Los procesos de recolección de evidencia y cadena de custodia están documentados y establecidos antes de que ocurra un incidente.
- Existen canales de comunicación alternos (fuera de banda) disponibles si tus sistemas principales se ven comprometidos durante un ataque.
- Entiendes qué significa una "buena contención" en distintos escenarios de ataque (ransomware, amenaza interna, compromiso en la cadena de suministro, etc.).

Por qué importa esta brecha

La confusión y los retrasos multiplican el riesgo cuando cada minuto cuenta. Las organizaciones sin un contrato de respuesta a incidentes preestablecido pierden horas críticas buscando ayuda durante una brecha activa. Las que se recuperan más rápido son las que ya habían decidido, antes del incidente, a quién llamar, qué hacer primero y cómo contener.

4 Preparación Organizacional y Ejecutiva

Pregunta diagnóstica

¿Está el negocio preparado para responder de forma efectiva más allá del equipo de seguridad?

- Los directivos entienden sus roles específicos y su autoridad de decisión durante un incidente.
- Legal, cumplimiento y comunicación están integrados en la planeación de respuesta a incidentes, y no se involucran por primera vez durante un evento real.
- Los requisitos de notificación regulatoria están claramente documentados (por ejemplo, la regla de 72 horas del GDPR, requisitos como HIPAA o disposiciones de la SEC, o las leyes de protección de datos aplicables en tu país e industria).
- La cobertura del seguro cibernético ha sido revisada, y se entienden las obligaciones de respuesta, exclusiones y plazos de notificación.
- La autoridad de decisión y el escalamiento al consejo de administración están definidos y acordados antes de una crisis.
- La coordinación de respuesta se ha puesto a prueba mediante ejercicios de simulación (tabletop), tanto a nivel directivo como técnico.

Por qué importa esta brecha

La respuesta técnica puede tener éxito, pero el riesgo de negocio sigue escalando. Las sanciones regulatorias, el daño reputacional y la exposición legal suelen derivarse de una mala coordinación organizacional, no de una mala herramienta de seguridad.

5 Inteligencia de Amenazas y Mejora Continua

Pregunta diagnóstica

¿Tu nivel de preparación mejora activamente conforme evoluciona el panorama de amenazas?

- Recibes inteligencia oportuna y accionable sobre amenazas emergentes, campañas activas y tácticas, técnicas y procedimientos de adversarios relevantes para tu industria.
- Las nuevas técnicas de ataque se incorporan rápidamente a la lógica de detección, los playbooks de caza y los procedimientos de respuesta a incidentes.
- Las revisiones posteriores a un incidente producen mejoras documentadas y medibles, no solo reportes que terminan guardados en una carpeta.
- La postura de seguridad y la madurez de preparación se evalúan de forma continua, no como un ejercicio anual único.
- Proveedores, socios y terceros han sido evaluados por su impacto potencial en tu capacidad de respuesta a incidentes.

Por qué importa esta brecha

La preparación de hoy puede fallar contra las amenazas de mañana. Los programas de seguridad estáticos se quedan atrás. El panorama de amenazas evoluciona de forma constante, y la preparación construida para los ataques del año pasado puede no resistir los de este año.

Qué significan tus resultados

Esta guía no es un examen de pasa o no pasa, es un punto de partida. Cualquier área donde hayas respondido "no", "parcialmente" o "no lo sé" es una señal que vale la pena explorar, no un juicio. Organizaciones de todos los niveles de madurez encuentran brechas. Lo que distingue a las organizaciones resilientes de las vulnerables es qué hacen con esa información.

El patrón más común que se observa en investigaciones reales de respuesta a incidentes es este: las organizaciones saben, de forma intuitiva, dónde están sus brechas, pero no tienen un camino estructurado para cerrarlas.

Cómo ayuda Interlace a cerrar estas brechas

En INTERLACE somos partner e implementador de SentinelOne Singularity XDR en México. No solo instalamos la tecnología: la ajustamos a tu operación y la operamos desde nuestro propio SOC (Security Operations Center), las 24 horas, los 7 días de la semana.

DIMENSIÓN DE ESTA GUÍA	CÓMO LA CUBRE SINGULARITY XDR, OPERADO POR INTERLACE
1. Detección y visibilidad	**EDR autónomo**, detección basada en comportamiento sin depender de firmas ni de la nube, más **Ranger**, que descubre los dispositivos no gestionados en tu red corporativa.
2. Caza de amenazas proactiva	**Vigilance MDR**: nuestro SOC monitorea la operación de forma continua, no solo reacciona a alertas puntuales.
3. Respuesta a incidentes	**Storyline** reconstruye el ataque completo en segundos, con causa raíz y remediación; **Vigilance MDR** escala y responde en menos de 15 minutos.
4. Preparación organizacional y ejecutiva	Se resuelve en conversación directa con tu equipo. Si tu organización requiere una evaluación experta más profunda, SentinelOne ofrece el servicio especializado Wayfinder Incident Readiness & Response, al cual Interlace puede ayudarte a conectar.
5. Inteligencia y mejora continua	La plataforma Singularity incorpora inteligencia de amenazas de forma continua; nuestro equipo revisa contigo los hallazgos y ajusta la operación de forma periódica.

1 min
TIEMPO DE DETECCIÓN

100%
PREVENCIÓN DE RANSOMWARE

24/7
RESPUESTA DESDE NUESTRO SOC

Cifras publicadas por Interlace para su implementación de SentinelOne Singularity XDR, plataforma XDR líder del Cuadrante Mágico de Gartner.

¿Listo para convertir estos hallazgos en un plan?

Habla con el equipo de Interlace para revisar en dónde están las brechas de tu organización y cómo SentinelOne Singularity XDR, implementado y operado por nuestro SOC, puede cerrarlas.

Conocer Singularity XDR → **Agendar una demo →**

Visita: interlace.com/soluciones

Contacto: a través de nuestro sitio, interlace.com

Sobre Interlace. Interlace es partner HP #1 en México y partner e implementador de SentinelOne Singularity XDR, con casi dos décadas de experiencia en servicios administrados de tecnología, impresión, cómputo, infraestructura y ahora ciberseguridad gestionada desde nuestro propio SOC.
