

RECUPERACIÓN CON CONFIANZA

Implemente un plan que brinde absoluta confianza en la recuperación.

Evite el daño que pueden causar el tiempo fuera de servicio y el robo de datos. Prepárese hoy para la resiliencia del mañana con nuestra lista de verificación de recuperación informática.

FASE 1

Fase 1 | 30 días

Establecer la base.

Lo que puede hacer AHORA para proteger su negocio.



Crear políticas de protección y retención para todas las cargas de trabajo.



Utilizar el almacenamiento inmutable.



Implementar la estrategia de respaldo 3-2-1: tres copias en dos formatos; uno externo que incluya un servidor aislado ("air gap") virtual y/o físico; el aislamiento de SaaS es vital.



Aplicar controles de seguridad (p. ej. MFA, MPA, segmentación de redes, RBAC, cifrado).



Considerar la posibilidad de utilizar appliances reforzados y especialmente diseñados.



Habilitar la detección de anomalías impulsada por IA.



Activar las reglas de detección y retención de malware.



Actualizar software y parches de seguridad (en curso).

FASE 2

Fase 2 | 60 días

Gestionar el riesgo de forma proactiva.

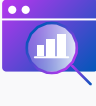
Enfocarse en las personas, los procesos y la tecnología.



Identificar los activos críticos "faltantes".



Llevar a cabo una evaluación de datos oscuros.



Descubrir y clasificar datos confidenciales.



Identificar y supervisar el comportamiento de alto riesgo de los usuarios finales.



Crear un entorno de recuperación aislado (IRE o sala limpia).



Desarrollar runbooks de recuperación que prioricen el orden de las operaciones.



Integrar al equipo de operaciones de seguridad y establecer manuales de estrategias de respuesta a incidentes (p. ej. integraciones SIEM/SOAR/XDR).

FASE 3

Fase 3 | 90 días

Refinar, ensayar, adaptar.



Ajustar las políticas de protección de datos para lograr un éxito del 100 % en los respaldos, de acuerdo con los acuerdos de nivel de servicio (SLA).



Realizar ajustes finos de la detección de anomalías impulsada por IA (eliminar falsos positivos/negativos).



Ejecutar ejercicios de simulación, incluyendo ensayos de recuperación que no perturben las operaciones actuales.



Ensayar la recuperación y validar los resultados.

[Consulte la lista de verificación de recuperación informática completa >](#)