

DESCARGABLE

Lista de verificación de seguridad de sistemas

Siete verificaciones para determinar si un sistema está realmente protegido, o solo monitoreado.

Cómo usarla. Para cada afirmación marque Sí solo cuando exista evidencia que pueda mostrarse, por ejemplo una configuración, un registro, un documento o una prueba con fecha. Marque Parcial cuando la medida exista pero no cubra todos los sistemas, y No cuando no exista o no pueda demostrarse. Una respuesta basada en la suposición de que algo debe estar hecho se cuenta como No.

Organización / sistema evaluado

Responsable de la revisión

Fecha

1. Inventario de activos	Sí	Parcial	No
Lo que no está identificado no puede protegerse			
Existe una lista actualizada de sistemas, aplicaciones y servidores en uso, con un responsable por cada uno.	☐	☐	☐
Se sabe qué datos sensibles maneja cada sistema y dónde se almacenan.	☐	☐	☐
Están identificados los proveedores y servicios externos con acceso a los sistemas o a los datos.	☐	☐	☐
En los últimos doce meses se revisó si hay equipos o servicios en uso que no figuran en el inventario.	☐	☐	☐
2. Identidad y accesos	Sí	Parcial	No
Quién entra, con qué permisos y desde dónde			
La autenticación de múltiples factores está activa en correo, acceso remoto y paneles de administración.	☐	☐	☐
Cada persona tiene solo los permisos que su función requiere.	☐	☐	☐
Las cuentas de personas que dejaron la organización fueron desactivadas.	☐	☐	☐
Las cuentas de servicio y las de proveedores están inventariadas y con permisos acotados.	☐	☐	☐
No hay contraseñas ni llaves de acceso almacenadas en código, repositorios o documentos compartidos.	☐	☐	☐

3. Configuración y actualizaciones	Sí	Parcial	No
El estado real de cada componente			
Los sistemas operativos, aplicaciones y dependencias reciben parches con una frecuencia definida.	☐	☐	☐
No hay software sin soporte del fabricante en producción, o tiene un plan de reemplazo con fecha.	☐	☐	☐
Se revisaron los puertos y servicios expuestos a internet y permanecen solo los necesarios.	☐	☐	☐
Las credenciales y configuraciones por defecto fueron cambiadas.	☐	☐	☐
La información viaja y se almacena cifrada.	☐	☐	☐
4. Detección y registros	Sí	Parcial	No
Capacidad de enterarse de lo que ocurre			
Los registros de acceso y de actividad administrativa se conservan fuera del sistema que los genera.	☐	☐	☐
Existen alertas ante eventos relevantes, como inicios de sesión fallidos repetidos o cambios de permisos.	☐	☐	☐
Una persona o equipo tiene asignada la revisión de las alertas, con un plazo de atención.	☐	☐	☐
El tiempo de retención de los registros permite investigar un incidente ocurrido varios meses atrás.	☐	☐	☐
5. Respaldo y recuperación	Sí	Parcial	No
Una copia solo cuenta si se ha restaurado			
Existen copias de los sistemas y datos críticos con una frecuencia acorde con la pérdida de información tolerable.	☐	☐	☐
Al menos una copia está aislada de la red principal o no puede modificarse.	☐	☐	☐
La restauración se probó en el último año y se midió cuánto tardó.	☐	☐	☐
El tiempo de recuperación medido es compatible con lo que el negocio puede soportar.	☐	☐	☐

6. Pruebas independientes

Verificación hecha por quien no construyó el sistema

Sí

Parcial

No

Se ejecutan análisis de vulnerabilidades de forma periódica sobre sistemas y dependencias.

☐☐☐

Se realizó una prueba de penetración con alcance definido en los últimos doce meses.

☐☐☐

Cada hallazgo tiene responsable, prioridad y fecha de corrección.

☐☐☐

Se verificó que los hallazgos corregidos quedaron efectivamente resueltos.

☐☐☐

7. Respuesta y gobierno

Qué ocurre cuando algo falla y quién responde

Sí

Parcial

No

Existe un plan escrito de respuesta a incidentes con roles y contactos.

☐☐☐

Se realizó al menos un simulacro en el último año.

☐☐☐

Se sabe a quién notificar y en qué plazo si hay una filtración de datos personales, según la norma aplicable.

☐☐☐

Hay un responsable de seguridad con autoridad para decidir, que reporta a la dirección.

☐☐☐

Estas verificaciones se repiten con una periodicidad definida.

☐☐☐

Cómo leer el resultado

Cada respuesta Parcial o No en las secciones 1, 2 y 5 conviene atenderla antes que el resto. Sin inventario no se sabe qué proteger, sin control de accesos se abre la puerta principal, y sin una restauración probada no hay certeza de poder recuperarse. Las demás secciones se ordenan según el riesgo de cada sistema y su impacto en la operación.

Para cada punto pendiente defina un responsable, una fecha y la evidencia que se aceptará como cierre, y vuelva a aplicar la lista con la periodicidad acordada.

Esta lista orienta una revisión interna y no sustituye una auditoría ni una prueba de penetración realizada por un tercero. Si necesita apoyo para evaluar alguno de estos puntos, U-SITE puede acompañar el diagnóstico técnico.