BOHIOSYSTEM

CHECKLIST DE HARDENING · BOHIOSYSTEM

Checklist de Hardening

Controles de endurecimiento por capa, ordenados por relación entre esfuerzo e impacto, para aplicar y verificar.

DOCUMENTO
BS-SVC-12B

VERSIÓN
1.0

FECHA
1 de agosto de 2026

PREPARADO POR
BohioSystem

CONTROLES VERIFICABLES

> **Esta lista está ordenada por lo que más reduce el riesgo con menos esfuerzo.** Si vas a hacer solo la primera sección, ya habrás cubierto la mayor parte de los ataques habituales.

Los controles se basan en las guías CIS y en el marco NIST, adaptados al tamaño de organización con el que trabajamos normalmente. No es una lista exhaustiva de cumplimiento: es la lista de lo que de verdad se explota.

5	Priorizado	Verificable	CIS/NIST
CAPAS DE CONTROL	POR IMPACTO REAL	CADA PUNTO SE COMPRUEBA	MARCOS DE REFERENCIA

01 Prioridad alta · identidad y accesos

La mayoría de los incidentes empieza con una credencial. Esta sección es la de mayor retorno.

Autenticación

- Segundo factor obligatorio en correo, nube y VPN.
- Sin cuentas compartidas entre personas.
- Contraseñas gestionadas por gestor corporativo.
- Bloqueo tras intentos fallidos repetidos.

Autorización

- Permiso mínimo necesario por rol.
- Cuentas administrativas separadas de las de uso diario.
- Revisión trimestral de quién tiene acceso a qué.
- Acceso administrativo solo desde red controlada.

Ciclo de vida

- Procedimiento escrito de alta y baja.
- Revocación inmediata al causar baja.
- Cuentas de servicio inventariadas y con dueño.
- Rotación periódica de secretos y claves de API.

Terceros

- Accesos de proveedor temporales y nominales.
- Registro de toda actividad de terceros.
- Revocación automática al terminar el trabajo.
- Sin credenciales compartidas por mensajería.

02 Prioridad alta · respaldo y recuperación

Aislamiento

- Al menos una copia fuera de la red productiva.
- Copias inmutables o con retención bloqueada.
- Credenciales de respaldo distintas de las del dominio.
- Un cifrado masivo no debe alcanzar las copias.

Verificación

- Restauración probada en los últimos seis meses.
- Tiempo real de restauración documentado.
- Alerta automática si un respaldo falla.
- Verificación de integridad de las copias.

03 Prioridad media · sistemas y red

Sistemas

- Parches de seguridad con ventana definida.
- Sin sistemas fuera de soporte en producción.
- Servicios innecesarios deshabilitados.
- Configuración según guía de referencia de la plataforma.

Red

- Segmentación por función y criticidad.
- Red de invitados aislada de la corporativa.
- Administración no expuesta a internet.
- Reglas de cortafuegos documentadas y revisadas.

Cifrado

- TLS vigente en todo servicio publicado.
- Certificados con renovación automática.
- Cifrado en reposo en equipos portátiles.
- Protocolos y cifrados obsoletos deshabilitados.

Equipos

- Protección de endpoint activa y gestionada.
- Disco cifrado en portátiles.
- Bloqueo automático de sesión.
- Inventario de equipos con su responsable.

04 Prioridad media · aplicaciones y datos

Aplicaciones

- Dependencias analizadas y actualizadas.
- Sin secretos escritos en el código.
- Validación de entrada en todo formulario.
- Cabeceras de seguridad configuradas.

Datos

- Clasificación por sensibilidad.
- Datos personales identificados y protegidos.
- Entornos de prueba sin datos reales.
- Política de retención y borrado definida.

05 Prioridad continua · detección y respuesta

Registro

- Registros centralizados fuera del sistema origen.
- Retención suficiente para investigar.
- Registro de accesos administrativos.
- Sincronización horaria entre sistemas.

Detección

- Alertas ante acceso administrativo inusual.
- Detección de ejecución sospechosa en endpoint.
- Vigilancia de cambios en configuración crítica.
- Alguien revisa las alertas de forma efectiva.

Respuesta

- Plan de respuesta escrito y accesible sin la red.
- Árbol de contactos actualizado.
- Procedimiento de aislamiento de equipo.
- Simulacro realizado al menos una vez al año.

Personas

- Formación anual de concienciación.
- Simulación de correo fraudulento periódica.
- Canal de reporte sin consecuencias para quien avisa.
- Procedimiento conocido ante sospecha.

CÓMO USAR ESTA LISTA

Recórrela marcando solo lo que puedas **demostrar**, no lo que creas que está. La diferencia entre “tenemos respaldos” y “restauramos con éxito el mes pasado en cuarenta minutos” es exactamente la diferencia entre creer que estás protegido y estarlo.

Hablemos

SIGUIENTE PASO

Escríbenos y agendamos una sesión de trabajo sin costo para revisar tu caso concreto.

CONTACTO
contacto@bohiosystem.dev

WEB
bohiosystem.dev

DOCUMENTO
BS-SVC-12B · v1.0