BOHIOSYSTEM

FICHA DE SERVICIO · BOHIOSYSTEM

Ciberseguridad

Protegemos la operación con controles proporcionados al riesgo real: diagnóstico, hardening, monitoreo y respuesta ante incidentes.

DOCUMENTO
BS-SVC-12

VERSIÓN
1.0

FECHA
1 de agosto de 2026

PREPARADO POR
BohioSystem

EL SERVICIO

> **La seguridad no se compra, se opera. Un cortafuegos caro sobre una red sin segmentar y con contraseñas compartidas no protege nada.**

Evaluamos el estado real de seguridad de una organización, priorizamos por riesgo y ejecutamos las medidas que reducen exposición: control de accesos, endurecimiento de sistemas, segmentación, monitoreo y capacidad de respuesta.

Trabajamos siempre bajo autorización escrita y con alcance definido. Toda prueba técnica se realiza dentro de los límites acordados y con reporte completo de lo encontrado.

Por riesgo
PRIORIZACIÓN, NO CATÁLOGO

Autorizado
ALCANCE ESCRITO

Continuo
NO UNA FOTO ANUAL

Accionable
CON PLAN DE REMEDIACIÓN

01 Qué resolvemos

Lo que encontramos con más frecuencia en un primer diagnóstico.

SITUACIÓN FRECUENTE	QUÉ SIGNIFICA PARA EL NEGOCIO
Credenciales compartidas	Varias personas usan la misma cuenta administrativa, así que ninguna acción es atribuible y las bajas de personal no revocan nada.
Sin segundo factor	El acceso a correo, sistemas y nube depende solo de una contraseña que probablemente se reutiliza en otros servicios.
Sistemas sin actualizar	Servidores y equipos con vulnerabilidades conocidas y parche disponible desde hace meses.
Respaldos alcanzables por un ataque	Las copias están en la misma red y con las mismas credenciales, así que un cifrado masivo se las lleva también.
Sin visibilidad	No hay registros centralizados, así que si hubo un acceso indebido nadie podría saberlo ni reconstruir qué pasó.
Sin plan de respuesta	Nadie sabe a quién llamar, qué desconectar ni qué comunicar si mañana aparece una nota de rescate.

02 Qué incluye el servicio

01 Diagnóstico de seguridad

Una foto honesta del estado actual, con hallazgos priorizados por riesgo real y no por severidad teórica.

Revisión de arquitectura · Análisis de vulnerabilidades · Revisión de accesos y permisos · Exposición externa · Informe ejecutivo y técnico

02 Gestión de identidades y accesos

El control con mejor relación entre esfuerzo y reducción de riesgo. Casi siempre es por donde empezamos.

Cuentas nominales · Segundo factor obligatorio · Permiso mínimo necesario · Gestor de contraseñas corporativo · Revisión periódica de accesos · Procedimiento de alta y baja

03 Endurecimiento de sistemas

Reducir la superficie de ataque de servidores, equipos y servicios expuestos.

Configuración segura por plataforma · Gestión de parches · Cierre de servicios innecesarios · Cifrado en tránsito y en reposo · Segmentación de red

04 Monitoreo y detección

Que exista registro de lo que pasa y alguien que lo mire cuando algo se sale de lo normal.

Registros centralizados · Correlación de eventos · Detección en el endpoint · Alertas priorizadas · Retención para investigación

05 Respuesta a incidentes

Un procedimiento acordado antes del incidente, porque durante el incidente no hay tiempo de escribirlo.

Plan de respuesta escrito · Roles y árbol de contactos · Contención y erradicación · Recuperación verificada · Informe posterior y lecciones

06 Cultura y concienciación

La mayoría de los incidentes empieza con una persona haciendo clic. Es el control más barato y el más ignorado.

Formación por rol · Simulaciones de correo fraudulento · Políticas comprensibles · Canal de reporte sin castigo · Medición de mejora

03 Cómo trabajamos

Por etapas cortas, con algo verificable al final de cada una.

FASE	QUÉ OCURRE	QUÉ QUEDA
01 · Descubrimiento	Entendemos el negocio, el estado actual y la restricción real.	Diagnóstico y alcance acordado.
02 · Diseño	Definimos la solución, sus riesgos y su plan de ejecución.	Arquitectura y plan por hitos.
03 · Construcción	Implementamos por incrementos verificables, no en una entrega única.	Avances funcionales por hito.
04 · Puesta en marcha	Despliegue controlado, pruebas y transferencia de conocimiento.	Solución en producción y equipo capacitado.
05 · Evolución	Operación, medición y mejora continua bajo acuerdo de servicio.	Reporte periódico y roadmap vivo.

04 Qué recibes

Diagnóstico

- Informe ejecutivo para dirección.
- Informe técnico con detalle reproducible.
- Hallazgos priorizados por riesgo.
- Plan de remediación con esfuerzo estimado.

Implementación

- Controles aplicados y verificados.
- Configuración documentada.
- Matriz de accesos actualizada.
- Evidencia del antes y el después.

Operación

- Monitoreo con alertas activas.
- Plan de respuesta a incidentes.
- Procedimientos de contención.
- Calendario de revisiones.

Políticas

- Política de seguridad adaptada.
- Normas de uso aceptable.
- Procedimiento de altas y bajas.
- Material de formación.

05 Tecnologías con las que trabajamos

Elegimos la herramienta por el problema, no por moda ni por acuerdo con un fabricante.

WAZUH · CIS BENCHMARKS · OWASP · NMAP · OPENVAS · BURP SUITE · BITWARDEN · KEYCLOAK · WIREGUARD · PFSENSE · FAIL2BAN · LET'S ENCRYPT · VAULT · NIST CSF · ISO 27001

06 Modelos de contratación

MODELO	CÓMO FUNCIONA	CUÁNDO CONVIENE
Proyecto cerrado	Alcance y entregables definidos, precio y plazo acordados.	Necesidades acotadas con objetivo claro.
Retainer mensual	Capacidad reservada del equipo mes a mes.	Evolución continua y soporte sostenido.
Equipo dedicado	Perfiles asignados en exclusiva bajo tu dirección.	Programas largos o alta carga de trabajo.
Bolsa de horas	Horas consumibles con prioridad acordada.	Demanda variable o trabajo puntual.

07 Nuestros compromisos

COMPROMISO	CÓMO SE CUMPLE
Autorización escrita siempre	Ninguna prueba técnica se ejecuta sin alcance, ventana y autorización firmada por quien tiene potestad para darla.
Priorizamos por riesgo real	Un hallazgo crítico en un sistema sin datos ni exposición va después de uno medio en el sistema que factura.
Sin alarmismo comercial	No inflamos severidades para vender más. El informe distingue lo urgente de lo conveniente.
Confidencialidad	Los hallazgos se tratan bajo acuerdo de confidencialidad y se entregan solo a los destinatarios acordados.
Transferencia de capacidad	Explicamos cada hallazgo de forma que el equipo interno pueda evitar que se repita.

POR DÓNDE EMPEZAR SI EL PRESUPUESTO ES LIMITADO

Segundo factor en todos los accesos, cuentas nominales sin compartir, respaldos aislados y probados, y parches al día. Esas cuatro medidas cuestan poco y cubren la mayor parte de los incidentes que vemos. Todo lo demás viene después.

08 Siguiente paso

EMPEZAR

Una sesión de una hora, sin costo, para revisar tu situación actual y definir juntos el alcance mínimo con el que empezar.

CONTACTO
contacto@bohiosystem.dev

WEB
bohiosystem.dev

DOCUMENTO
BS-SVC-12 · v1.0