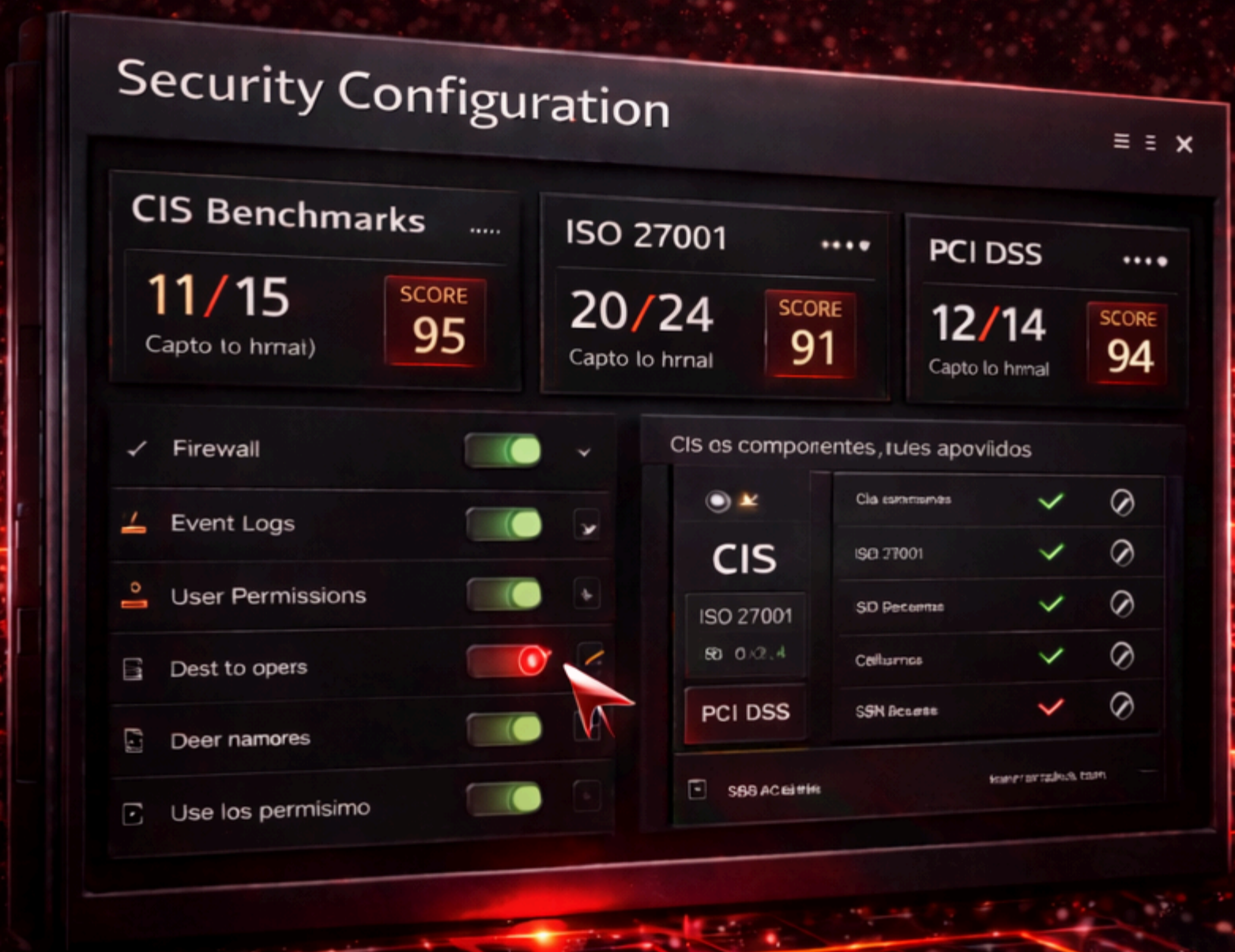
PentaSec
Cybersecurity

Catálogo de Servicios de Hardenización y Vulnerabilidades

Reducir la superficie de ataque
comienza con **configuraciones seguras.**



- **Aplicación de controles oficiales de CIS Benchmark**
- **Cumplimiento de la postura de seguridad** y preparación **para auditorías**
- **Priorización** basada en **riesgo** y **criticidad de activos**

Alcance de Hardening por Tipo de Activo & Vulnerabilidades

Cobertura integral de hardening basada en el **estándar CIS.**

Tipo de Activo	Alcance de Hardening	Ejemplos de Controles
Infraestructura Enterprise 	Servidores físicos y virtuales, bases de datos, aplicaciones corporativas y plataformas cloud	• Configuración segura del sistema operativo. • Deshabilitación de servicios innecesarios. • Aplicación de parches. • Control de privilegios. • Registro de eventos (logging).
Endpoints y Usuarios 	Estaciones de trabajo y laptops corporativas	• Aseguramiento del endpoint • Políticas de contraseñas. • Control de privilegios. • Cifrado de disco. • Actualización de sistemas.
Red y Seguridad 	Routers, switches, firewalls, VPN y segmentación de red	• Configuración segura. de interfaces. • Control de accesos. • Uso de protocolos seguros. • Auditoría de tráfico.
IoT / OT 	Sensores y dispositivos industriales conectados	• Endurecimiento de credenciales. • Segmentación de red. • Restricción de servicios. • Monitoreo de dispositivos.
Dispositivos Móviles 	Smartphones y tablets corporativos	• Políticas MDM, • Cifrado. • Autenticación segura. • Control de aplicaciones y accesos corporativos.

Alcance del Servicio

*Implementación **integral de hardening** para reforzar la **ciberseguridad** de tus activos.*

Evaluación inicial

- Revisión de la configuración actual de cada activo.
- Identificación de desviaciones frente a CIS Benchmark.

Definición de baseline seguro

- Establecimiento de configuraciones recomendadas según criticidad del activo y nivel de madurez deseado.

Implementación de controles de hardening

- Aplicación de configuraciones seguras, parches y ajustes de políticas.

Validación técnica

- Verificación de la correcta aplicación de los controles, incluyendo pruebas de cumplimiento y seguridad.

Seguimiento y reporting

- Dashboards permanentes y reportes periódicos que permiten medir la evolución del Hardening y mantener evidencia para auditorías.

Metodología de Trabajo

*El **hardening** efectivo es un proceso continuo basado en **riesgo.***

Assessment de Seguridad

- Inventario de activos.
- Identificación de vulnerabilidades.
- Evaluación de criticidad.

Priorización basada en riesgo.

- Impacto en el negocio.
- Roadmap de hardening.

Implementación de Hardening.

- CIS Benchmark.
- Endurecimiento de sistemas.
- Deshabilitación de servicios innecesarios.

Validación y Control

- Revisión de configuración.
- Pruebas de cumplimiento.

Monitoreo y Mejora Continua

- Dashboards permanentes y reportes periódicos.
- Actualización de baseline.
- Remediaciones periódicas.

Entregables Técnicos

Reporte de estado inicial

- Identificación de desviaciones y vulnerabilidades.

Plan de hardening priorizado

- Roadmap basado en criticidad y riesgo.

Reporte de implementación

- Evidencia de controles aplicados.

Dashboards de seguimiento

- Visualización de cumplimiento, evolución y desviaciones.

Documentación de procesos y guías de operación

- Lineamientos para mantenimiento del baseline seguro.

Beneficios para la Organización

Reducción de superficie de ataque

- Disminución de vulnerabilidades críticas y configuraciones inseguras.

Cumplimiento y capacidad de auditoría

- Alineación con estándares CIS, PCI, ISO 27001 y NIST.

Gobernanza de seguridad basada en riesgo

- Priorización efectiva de inversiones y esfuerzos de seguridad.

Escaneo de Vulnerabilidades

El **escaneo de vulnerabilidades** permite **identificar** debilidades técnicas antes de que puedan ser **aprovechadas** por un atacante.

A través de evaluaciones sistemáticas, PentaSec analiza la infraestructura tecnológica para detectar **configuraciones inseguras**, **vulnerabilidades conocidas** y **oportunidades de mejora** en la arquitectura de seguridad.

Qué incluye el servicio

Identificación de vulnerabilidades

Detección de debilidades en servidores, sistemas, redes y otros componentes de la infraestructura tecnológica.

Evaluación de controles de seguridad

Revisión de los controles existentes para determinar su nivel de efectividad.

Análisis de parchado y configuraciones

Identificación de vulnerabilidades relacionadas con actualizaciones pendientes o configuraciones inseguras.

Recomendaciones específicas de mitigación

Entrega de acciones concretas adaptadas a la infraestructura del cliente para reducir el riesgo.

Evaluación de arquitectura de seguridad

Análisis general de la arquitectura tecnológica para identificar mejoras que fortalezcan la postura de seguridad.

Objetivo y Alcance

Gestión estructurada de vulnerabilidades para fortalecer la seguridad de la organización

Objetivo:

Establecer un proceso claro y **eficiente** para **identificar**, **priorizar**, **corregir** y **validar vulnerabilidades** en los activos tecnológicos de la **organización**, reduciendo la **superficie de ataque** y el **riesgo cibernético.**

Alcance:

El servicio cubre **todos los** activos definidos por el cliente,

- Servidores e infraestructura tecnológica.
- Estaciones de trabajo y dispositivos de usuario.
- **Aplicaciones** web y **bases de datos.**
- Entornos cloud y plataformas digitales.

Tipo de Evaluación

Las evaluaciones de seguridad se realizan bajo un modelo controlado y autorizado, que permite identificar vulnerabilidades reales en la infraestructura del cliente sin afectar la operación del negocio.

Modalidad: Caja Gris

El cliente proporciona el listado de hosts o activos que serán evaluados.

Esto permite enfocar las pruebas en los sistemas relevantes para la organización.

Entorno: Interno

Las evaluaciones se realizan dentro de la infraestructura autorizada por la organización, analizando los sistemas y servicios definidos en el alcance del servicio.

Roles y Responsabilidades

Una gestión **efectiva** de **vulnerabilidades** requiere **claridad** en las responsabilidades.

Equipo de Ciberseguridad / SOC

Responsable de **gestionar y analizar las vulnerabilidades** identificadas.

- ✓ Operación de las herramientas de escaneo de **vulnerabilidades.**
- ✓ Validación de los **hallazgos** y eliminación de **falsos positivos.**
- ✓ **Priorización** de **vulnerabilidades según riesgo** y criticidad del activo.
- ✓ Asignación de tareas de remediación a **los equipos responsables.**
- ✓ Verificación de las correcciones mediante re-escaneo.

Equipo de TI / Infraestructura / Desarrollo / PentaSec (Dueños del Activo)

Responsables de aplicar las acciones necesarias para eliminar o mitigar **las vulnerabilidades.**

- ✓ Aplicación de parches, actualizaciones y ajustes de configuración.
- ✓ Reporte de **incidencias** o limitaciones para aplicar correcciones.

Gestor de Riesgos / CISO

- ✓ Aprobación del plan y de las **políticas** de gestión de **vulnerabilidades.**
- ✓ Revisión de reportes **ejecutivos** y **evolución** del **riesgo**.
- ✓ Aceptación formal del **riesgo residual** cuando una **vulnerabilidad** no puede ser corregida.

Entregables y Coordinación del Servicio

Al finalizar cada evaluación, **PentaSec** entrega **información clara** y accionable que permite a la organización **comprender los riesgos** identificados y tomar decisiones informadas para su remediación.

Entregables del servicio

Informe de hallazgos

Documento detallado con las vulnerabilidades, identificadas, evidencia técnica, validación de explotación cuando aplica y recomendaciones específicas de remediación.

Resumen ejecutivo

Síntesis orientada a la dirección que presenta el nivel de riesgo, los hallazgos más relevantes y las prioridades de remediación.

Anexos técnicos

Información técnica complementaria para los equipos responsables de implementar las acciones correctivas.

Entregables del cliente

Autorización formal de pruebas

El cliente debe proporcionar la autorización escrita para el inicio de las actividades.

Obligaciones del cliente

Acceso controlado a la infraestructura

Se debe habilitar acceso VPN para el consultor asignado, con un perfil que permita alcanzar los hosts definidos en el alcance de la evaluación.

Elaboración de Planes de Remediación

Transformamos los hallazgos de seguridad en acciones concretas de corrección.

PentaSec analiza cada vulnerabilidad identificada y construye un **plan de remediación priorizado**, alineado al riesgo y a la criticidad de los activos.

Escaneos Automatizados

Evaluaciones internas y externas para detectar vulnerabilidades técnicas.

Auditorías de Configuración Segura

Revisión de configuraciones frente a estándares como **CIS Benchmark**.

Alertas y avisos de fabricantes

Seguimiento de vulnerabilidades críticas y zero-days publicadas por proveedores.

Clasificación y Priorización de Vulnerabilidades

Priorizamos lo que realmente representa riesgo para su organización.

PentaSec analiza cada hallazgo en su contexto real, priorizando las acciones que realmente pueden impactar a la organización.

Factores que analizamos

Gravedad Técnica (CVSS)

Análisis del nivel técnico según estándares internacionales

Probabilidad Exploit

Si existen exploits públicos o evidencia de ataques en curso.

Criticidad del Activo

Si el sistema afecta operación, servicios, o datos sensibles.

Nivel de Exposición

Si el activo está expuesto a internet, en red interna o aislado.

Modelo de Priorización

CRÍTICA	ALTA	MEDIA	BAJA
Exploits públicos en sistemas expuestos a internet. Acción inmediata.	Vulnerabilidades severas en activos internos críticos.	Vulnerabilidades de riesgo moderado en entornos internos.	Hallazgos con bajo riesgo en entornos aislados.

Ventanas de Remediación (SLAs)

Para reducir el riesgo de forma efectiva, es fundamental **definir** tiempos claros para la corrección de vulnerabilidades.

PentaSec establece **ventanas de remediación** alineadas a la **prioridad del riesgo,** permitiendo que las organizaciones atiendan primero lo que realmente puede **impactar** su **operación.**

Tiempos máximos de remediación

CRÍTICA
Corrección prioritaria.

Hasta 30 días.

ALTA
Vulnerabilidades relevantes en activos críticos.

Hasta 90 días.

MEDIA
Riesgo moderado en activos internos.

Hasta 120 días.

BAJA
Hallazgos de bajo impacto o informativos.

Opcional

CRÍTICA	ALTA	MEDIA	BAJA
Corrección prioritaria.	Hasta **90 días.**	Hasta **120 días.**	**Opcional**

PentaSec
Cybersecurity

SOLICITE UNA PRUEBA DE CONCEPTO DE HARDENIZACIÓN Y VULNERABILIDADES

Demostramos cómo **fortalecer su infraestructura** y **reducir riesgos** con **controles técnicos verificables.**

IDENTIFICACIÓN
DE VULNERABILIDADES REALES

En servidores, endpoints, red e IoT.

APLICACIÓN DE **HARDENIZACIÓN**
BASADA EN **CIS BENCHMARK**

Configuraciones **seguras** y mejores prácticas.

VALIDACIÓN TÉCNICA
DEL IMPACTO EN LA **REDUCCIÓN**
DE SUPERFICIE DE ATAQUE

MENOR RIESGO | **MEJOR CUMPLIMIENTO** | **MAYOR VISIBILIDAD**

SOLICITE UNA **PRUEBA DE CONCEPTO INICIAL**

CONTÁCTENOS **HOY**

https//www.pentasec.net/contacto/