Roadmap de Hardening Transversal – Análisis, Priorización e Implementación

1. Contexto y Enfoque General

El presente documento consolida el análisis del proceso de hardening transversal definido para la organización, alineado a CIS Controls v8, ISO/IEC 27002 y al Scope de Hardening entregado.

- **CIS Controls v8** son un conjunto de **18 controles prioritarios**, enfocados en **reducir riesgo real** de forma práctica y medible.

    - CIS 1 – Inventario y Control de Activos Empresariales
        - Establece la necesidad de identificar y mantener actualizado el inventario de todos los activos tecnológicos que soportan el negocio.
    - CIS 2 – Inventario y Control de Activos de Software
        - Busca asegurar que solo software autorizado y conocido esté instalado en la organización.
    - CIS 3 – Protección de Datos
        - Define controles para proteger información sensible durante su almacenamiento, procesamiento y transmisión.
    - CIS 4 – Gestión de Configuración Segura
        - Establece configuraciones base seguras para sistemas y aplicaciones.
    - CIS 5 – Gestión de Cuentas
        - Asegura que las cuentas de usuario y servicio estén controladas, justificadas y actualizadas.
    - CIS 6 – Gestión de Accesos
        - Define cómo se asignan y revisan permisos de acceso, aplicando el principio de mínimo privilegio.
    - CIS 7 – Gestión Continua de Vulnerabilidades
        - Busca identificar, priorizar y corregir vulnerabilidades técnicas de forma sistemática.
    - CIS 8 – Gestión de Logs y Monitoreo
        - Asegura que eventos relevantes de seguridad sean registrados y monitoreados.
    - CIS 9 – Protección de Email y Navegadores
        - Reduce riesgos asociados a phishing, malware y navegación insegura.
    - CIS 10 – Protección contra Malware
        - Establece controles para prevenir, detectar y responder a software malicioso.

    - CIS 11 – Recuperación de Datos

        - Asegura la existencia de respaldos confiables y probados.
    - CIS 12 – Seguridad de Infraestructura de Red
        - Define controles para proteger redes, segmentar tráfico y limitar accesos.
    - CIS 13 – Monitoreo y Defensa de Red
        - Permite detectar comportamientos anómalos dentro de la red.
    - CIS 14 – Concientización y Capacitación
        - Promueve una cultura de seguridad entre los usuarios.
    - CIS 15 – Gestión de Proveedores
        - Controla riesgos derivados de terceros y proveedores.
    - CIS 16 – Seguridad de Aplicaciones
        - Busca asegurar el desarrollo y operación segura de aplicaciones.
    - CIS 17 – Gestión de Respuesta a Incidentes
        - Define cómo detectar, responder y recuperarse de incidentes de seguridad.
    - CIS 18 – Pruebas de Penetración
        - Evalúa la efectividad de los controles mediante pruebas controladas.

ISO/IEC 27002 – RESUMEN POR DOMINIO

ISO/IEC 27002 define controles de seguridad organizacionales, técnicos y humanos, orientados a gobierno y cumplimiento.

A.5 – Controles Organizacionales

Establecen políticas, roles, responsabilidades y gobierno de la seguridad.
Da marco formal al hardening y su sostenibilidad.

A.6 – Controles de Personas

Regula seguridad antes, durante y después de la relación laboral.
Controla riesgos asociados a usuarios y privilegios.

A.7 – Controles Físicos

Protege instalaciones, salas críticas y activos físicos.
Fundamental en CPD, salas SCADA y subestaciones.

A.8 – Controles Tecnológicos

Incluye hardening técnico de sistemas, redes, aplicaciones y datos.
Donde se materializa la mayor parte del hardening.

A.8.1 – Control de Accesos

Define reglas de acceso lógico y autenticación.
Aplica mínimo privilegio y control de identidades.

A.8.2 – Criptografía

Asegura uso adecuado de cifrado para proteger información.
En tránsito y en reposo.

A.8.3 – Seguridad de Operaciones

Incluye gestión de cambios, parches, backups y monitoreo.
Asegura estabilidad operativa del hardening.

A.8.4 – Seguridad de Comunicaciones

Protege redes y flujos de información.
Segmentación, firewalls y VPN.

A.8.5 – Seguridad del Ciclo de Vida de Sistemas

Cubre desarrollo, pruebas y cambios en aplicaciones.
Evita introducir riesgos en nuevos sistemas.

A.8.6 – Gestión de Incidentes

Define procesos para gestionar eventos de seguridad.
Complementa CIS 17.

A.8.7 – Continuidad del Negocio

Asegura resiliencia ante fallas o incidentes graves.
DRP, backups y pruebas periódicas.

Plan de ejecución:

Step 1: SERVIDORES WINDOWS (AD / APP / FILE / INFRA)

Análisis

- Versión de SO (2016 / 2019 / 2022)
- Rol del servidor (AD, File, App, Infra)
- Dependencias:
    - .NET Framework
    - PowerShell
    - SMB
- GPO existentes
- Servicios legacy

Riesgos eventuales

- Aplicaciones legacy incompatibles con CIS Level 2
- Scripts que requieren privilegios elevados
- Dependencia de NTLM / SMBv1
- Bloqueo de servicios por hardening agresivo

Incompatibilidades comunes

- .NET antiguo vs TLS 1.2+
- Aplicaciones hardcodeadas con rutas protegidas
- Software que no soporta UAC o BitLocker

Gestión del cambio

- Piloto por **tipo de rol** (no por servidor)
- Validación con dueño de aplicación
- Ventana de cambio aprobada
- Plan de rollback documentado

Ejecución

- CIS Benchmark Level 1 (baseline)
- MFA para cuentas administrativas
- BitLocker + Secure Boot
- Deshabilitación de servicios innecesarios
- Logging centralizado (SIEM)

Step 2: SERVIDORES LINUX (APP / DB / INFRA)

Análisis

- Distro y versión (RHEL, Ubuntu, SUSE)
- Kernel y parches
- Librerías críticas:
    - glibc
    - OpenSSL
- Servicios activos
- Usuarios con sudo

Riesgos eventuales

- Apps incompatibles con OpenSSL actualizado
- Servicios ejecutándose como root
- Scripts legacy que fallan con permisos restringidos

Incompatibilidades comunes

- OpenSSL ≥ 1.1 vs apps antiguas
- SELinux rompiendo aplicaciones mal diseñadas
- Firewall local bloqueando puertos hardcodeados

Gestión del cambio

- Hardening en ambiente espejo
- Pruebas funcionales
- Validación con equipo APP
- Ventana de cambio controlada

Ejecución

- CIS Benchmark Linux
- SSH hardening
- Mínimo privilegio
- Firewall local activo
- Auditoría y logs

Step 3: BASES DE DATOS (Oracle / SQL Server / PostgreSQL)

🔍 **Análisis**

- Motor y versión
- Clientes DB conectados
- Usuarios y roles
- Métodos de autenticación
- Backups actuales

Riesgos eventuales

- Aplicaciones con cuentas compartidas
- Clientes antiguos sin soporte TLS
- Queries con permisos excesivos

Incompatibilidades comunes

- Drivers antiguos vs TLS fuerte
- Apps que no soportan rotación de credenciales
- Backups que fallan por cambios de permisos

Gestión del cambio

- Pruebas en QA
- Migración progresiva de cuentas
- Validación con APP owners

Ejecución

- Roles mínimos
- Cifrado en tránsito
- Auditoría de accesos
- Backups inmutables

Step 4: SERVIDORES DE APLICACIÓN (JAVA / .NET / WEB)

Análisis

- Runtime (JDK, .NET)
- Librerías y frameworks
- Puertos expuestos
- Métodos de autenticación

Riesgos eventuales

- Apps no compatibles con TLS fuerte
- Escritura en rutas bloqueadas
- Dependencias hardcodeadas

Incompatibilidades comunes

- JDK antiguo
- Frameworks sin soporte
- Librerías no parcheadas

Gestión del cambio

- Pruebas DEV / QA
- Ajustes de configuración
- Coordinación con ventanas de negocio

Ejecución

- TLS fuerte
- Restricción de puertos
- Allow-listing
- Hardening del runtime

Step 5: SERVIDORES CLOUD / VIRTUALIZACIÓN

Análisis

- Tipo de servicio (IaaS / PaaS)
- IAM asociado
- Imágenes base
- Pipelines CI/CD

Riesgos eventuales

- Cambios manuales fuera de IaC
- Drift de configuración
- Secrets expuestos

Incompatibilidades comunes

- Scripts no versionados
- Imágenes base antiguas
- Políticas IAM demasiado amplias

Gestión del cambio

- Cambios vía IaC
- Pull Request + aprobación
- Validación automatizada

Ejecución

- IAM mínimo privilegio
- Imágenes endurecidas
- Logging nativo
- Backups automáticos

MATRIZ DE RIESGOS TRANSVERSALES

Riesgo	**Impacto**
Incompatibilidad de librerías	Caída de aplicaciones
Hardening sin piloto	Interrupción de servicio
Cambios sin gestión	Incidentes operacionales
Drift post-hardening	Pérdida de control
MFA sin comunicación	Rechazo de usuarios

ROADMAP TEMPORAL (ALINEADO AL DOCUMENTO)

Etapa	Foco	Duración
Análisis	Inventario + dependencias	3–4 semanas
Resultados	Validación ejecutiva	1 semana
Gestión del cambio	Pilotos + comunicación	2–3 semanas
Ejecución Ola 1	Identidades, backups, endpoints	4 semanas
Ejecución Ola 2	Servidores, DB, SIEM	3–4 semanas
Ejecución Ola 3	Cloud, allow-list, madurez	2–4 semanas

DOTACIÓN DE PROFESIONALES POR ETAPA (sugerido):

Etapa	Perfiles	Cantidad
Análisis	SA, SO, IAM, DB, NET, PM	5–6
Resultados	SA, PM	2
Gestión del cambio	SA, OT, PM	3
Ejecución Ola 1	SO, IAM, DB, NET, SOC	5
Ejecución Ola 2	SO, DB, NET, SOC	4
Ejecución Ola 3	DevSecOps, SO, SOC	3

Tabla de roles por función:

Rol	Nombre Completo	Responsabilidades Principales
SA	Security Architect (Arquitecto de Ciberseguridad)	Diseña la estrategia de hardening, prioriza riesgos, define controles de seguridad, valida decisiones técnicas y es responsable final del proyecto ante la organización.
SO	Especialista en Sistemas Operativos (Windows / Linux)	Ejecuta el hardening de servidores y endpoints, aplica baselines de seguridad, configura sistemas operativos de forma segura y valida compatibilidad con aplicaciones.
IAM	Especialista en Identidades y Accesos	Gestiona cuentas de usuario y servicio, implementa MFA, aplica mínimo privilegio, revisa accesos y reduce riesgos asociados a credenciales y permisos excesivos.
DB	Especialista en Bases de Datos	Protege las bases de datos mediante control de accesos, cifrado, auditoría, segregación de roles y definición de políticas de respaldo y recuperación.
NET	Especialista de Redes	Diseña y ejecuta controles de red, segmentación, firewalls, VPN y comunicaciones seguras, reduciendo la superficie de ataque y controlando el tráfico.
SOC	Ingeniero de Seguridad Operacional (SOC / SIEM)	Implementa monitoreo, centraliza logs, configura alertas de seguridad y apoya la detección temprana y respuesta ante incidentes.

Rol	Nombre Completo	Responsabilidades Principales
DevSecOps	Ingeniero DevSecOps	Integra seguridad en infraestructura cloud, automatización, CI/CD e Infraestructura como Código (IaC), asegurando que los controles de seguridad se apliquen de forma consistente y escalable.
OT	Ingeniero OT / Automatización Industrial	Valida cambios en sistemas industriales, SCADA y OT, asegurando que el hardening no afecte la continuidad operacional ni la seguridad física.
PM	Project Manager / Gestor del Cambio	Planifica, coordina y controla el proyecto, gestiona tiempos, dependencias, comunicación, ventanas de cambio y asegura una implementación ordenada y sin impactos no planificados.

Roles con cruce RACI por etapa

La matriz RACI asigna responsabilidades claras a cada rol en las distintas etapas del proyecto de hardening, asegurando ejecución ordenada, reducción de conflictos, trazabilidad de decisiones y control efectivo del riesgo, donde R = Responsible, A = Accountable, C=Consulted, I = informed.

Etapa 1 Análisis:

Actividad	SA	SO	IAM	DB	NET	SOC	OT	PM
Inventario de activos	A	C	C	C	C	I	C	R
Análisis de accesos y privilegios	A	C	R	C	I	I	C	I
Análisis de configuraciones (baseline)	A	R	C	C	C	I	C	I
Análisis de redes y segmentación	A	I	I	I	R	I	C	I
Matriz de criticidad	A	I	I	I	I	I	C	I

Etapa 2 Entrega de resultados:

Actividad	SA	SO	IAM	DB	NET	SOC	OT	PM
Informe ejecutivo	A	I	I	I	I	I	I	R
Presentación a gerencia	A	I	I	I	I	I	C	R
Aprobación del roadmap	A	C	C	C	C	I	C	R

Etapa 3 Gestión del Cambio:

Actividad	SA	SO	IAM	DB	NET	SOC	OT	PM
Evaluación impacto operacional	A	C	C	C	C	I	R	I
Definición ventanas de cambio	A	I	I	I	I	I	C	R
Plan de comunicación	A	I	I	I	I	I	I	R

Actividad	SA	SO	IAM	DB	NET	SOC	OT	PM
Pilotos técnicos	A	R	R	R	R	C	C	I

Etapa 4 1era Implementación (critico):

Actividad	SA	SO	IAM	DB	NET	SOC	OT	PM
MFA y mínimo privilegio	A	I	R	I	I	I	C	I
Hardening endpoints	A	R	C	I	I	C	C	I
Backups inmutables	A	C	C	R	I	I	I	I
Accesos remotos seguros	A	I	C	I	R	I	C	I

Etapa 5 2da Implementación (critico):

Actividad	SA	SO	IAM	DB	NET	SOC	OT	PM
Baselines servidores	A	R	C	I	I	C	C	I
Hardening bases de datos	A	I	C	R	I	C	I	I
Gestión de parches	A	R	I	C	I	I	C	I
Logging y SIEM	A	C	C	C	C	R	I	I
Segmentación de red	A	I	I	I	R	I	C	I

Etapa 6 3era Implementación (critico):

Actividad	SA	SO	IAM	DB	NET	SOC	OT	PM
Gestión de vulnerabilidades	A	R	I	C	C	R	I	I
Allow-listing aplicaciones	A	R	I	I	I	I	C	I
Hardening cloud avanzado	A	C	C	I	C	C	I	I
Gestión formal de cambios	A	I	I	I	I	I	I	R