

Las 7 Capas de Ciberseguridad que ISO 27001 convierte en un sistema

Implementadas con inteligencia artificial. La matriz completa que entregamos a los asistentes: amenazas reales, controles ISO 27001 y las herramientas de IA que aceleran la implementación.

La matriz completa

Toca cualquier capa para ir directo a su ficha — amenaza, controles ISO 27001 e IA que la resuelve.

7

Seguridad Humana

El 95% de las brechas comienza con un error humano — la capa más crítica y la más difícil de parchear

[Ver ficha >](#)

6

Seguridad de Datos

El activo más valioso — clasificarlo, cifrarlo y controlar quién lo toca es el núcleo de ISO 27001

[Ver ficha >](#)

5

Seguridad de Aplicaciones

El 60% de los ataques explota vulnerabilidades en código — la IA analiza miles de líneas en segundos

[Ver ficha >](#)

4

Seguridad de Endpoints

Cada laptop, celular o tablet es una puerta de entrada que el antivirus tradicional ya no cierra

[Ver ficha >](#)

3

Seguridad de Red

Una vez dentro de la red, el atacante se mueve lateralmente — la IA detecta anomalías en tiempo real

[Ver ficha >](#)

2

Seguridad Perimetral

El borde de la red ya no existe como antes — el perímetro ahora es identidad, no dirección IP

[Ver ficha >](#)

1

Seguridad Física

La brecha más obvia y la más ignorada — entrar al edificio y conectar un USB supera toda defensa digital

[Ver ficha >](#)

 **Matriz
resumen**

 **Por qué
ISO 27001 une todo**





Seguridad Humana

El 95% de las brechas comienza con un error humano — la capa más crítica y la más difícil de parchear



[Índice](#)

EL PROBLEMA REAL

- Un empleado hace clic en un email de phishing y entrega sus credenciales
- Un empleado con acceso activo filtra datos antes de irse
- Contraseñas reutilizadas en múltiples sistemas corporativos
- Deepfakes de voz usados en fraude al CFO ("CEO Fraud")

CONTROLES ISO 27001

A.6.1

A.6.2

A.6.3

A.6.5

A.8.25

LO QUE APRENDES EN EL CURSO

Diseñar programas de concienciación + política de usuario final

IA QUE LO RESUELVE

KnowBe4 / Proofpoint

Simulaciones de phishing con IA adaptativa según el perfil del empleado

UEBA (Splunk / Sentinel)

Detecta comportamientos anómalos antes de que ocurra el incidente

ChatGPT / Gemini

Genera microtrainings personalizados por rol en minutos

6

Seguridad de Datos

El activo más valioso — clasificarlo, cifrarlo y controlar quién lo toca es el núcleo de ISO 27001



[← Índice](#)

EL PROBLEMA REAL

- Datos críticos sin clasificar — nadie sabe qué información es sensible
- Backups que nunca se prueban y fallan al momento de recuperar
- Archivos confidenciales enviados por email sin cifrar
- Datos de clientes accesibles por cualquier empleado sin necesidad

CONTROLES ISO 27001

A.8.1

A.8.2

A.8.10

A.12.3

A.18.1

LO QUE APRENDES EN EL CURSO

Clasificación de activos · Inventario ISO 27001 · Esquemas de cifrado



IA QUE LO RESUELVE

Microsoft Purview

Clasificación automática con ML: detecta PII y datos regulados

Forcepoint DLP

Bloquea transferencias anómalas con análisis de contexto por IA

AWS Macie / Azure Info Protection

Descubre y protege datos sensibles en la nube

EL PROBLEMA REAL

- APIs sin autenticación expuestas a internet sin que nadie lo sepa
- Inyecciones SQL en formularios web no revisados
- Librerías de código desactualizadas con CVEs críticos conocidos
- Tokens de API hardcodeados en repositorios públicos

CONTROLES ISO 27001

A.14.1

A.14.2

A.12.6

A.8.26

LO QUE APRENDES EN EL CURSO

OWASP Top 10 · DevSecOps · Gestión de vulnerabilidades técnicas

IA QUE LO RESUELVE

GitHub Advanced Security + Copilot

Escanea código en tiempo real, detecta secrets antes del merge

Snyk / Veracode

SAST/DAST con IA que prioriza vulnerabilidades por impacto real

Cloudflare WAF

WAF con ML que aprende patrones de ataque y bloquea variantes nuevas

4

Seguridad de Endpoints

Cada laptop, celular o tablet es una puerta de entrada que el antivirus tradicional ya no cierra



[< Índice](#)

EL PROBLEMA REAL

- Equipos sin actualizar — vulnerabilidades conocidas desde meses
- Empleados en home office conectados a redes domésticas sin seguridad
- USBs con malware conectados en la oficina sin restricciones
- Celulares personales con acceso a correo corporativo sin MDM

CONTROLES ISO 27001

A.8.1

A.12.1

A.12.6

A.8.19

A.8.22

LO QUE APRENDES EN EL CURSO

Políticas de hardening · Gestión de parches · Control de dispositivos



IA QUE LO RESUELVE

CrowdStrike Falcon / SentinelOne

EDR con IA que detiene ransomware en milisegundos, sin firmas

Microsoft Intune

Compliance automatizado: si no cumple la política, no accede

Automox

Parcheo automático que prioriza qué actualizar primero según riesgo

EL PROBLEMA REAL

- Red plana sin segmentación — un dispositivo comprometido llega a todo
- Logs guardados pero nunca revisados — el ataque lleva meses activo
- Servidores expuestos directamente a internet sin DMZ
- WiFi corporativo compartido con visitantes sin segmentación

CONTROLES ISO 27001

A.13.1

A.13.1.3

A.12.4

A.8.20

A.8.21

LO QUE APRENDES EN EL CURSO

Segmentación · Logging · Gestión de incidentes de red

IA QUE LO RESUELVE

Microsoft Sentinel / Splunk SIEM

Correlaciona millones de eventos de red con ML

Darktrace NDR

Aprende el comportamiento normal de la red y alerta anomalías

Cisco AI Network Analytics

Microsegmentación automática basada en comportamiento real

2

Seguridad Perimetral

El borde de la red ya no existe como antes — el perímetro ahora es identidad, no dirección IP



[< Índice](#)

EL PROBLEMA REAL

- Firewall configurado hace años sin actualizar reglas
- VPN sin MFA — una credencial robada da acceso total
- Empleados en cloud (M365, Salesforce) sin control perimetral tradicional
- Ataques DDoS que tumban el sitio web en horas pico

CONTROLES ISO 27001

A.13.1.1

A.13.2

A.8.20

A.9.4

LO QUE APRENDES EN EL CURSO

Arquitectura Zero Trust · Control de acceso · Gestión de identidad

IA QUE LO RESUELVE

Palo Alto NGFW (AI threat prevention)

Bloquea amenazas zero-day con ML entrenado globalmente

Zscaler Zero Trust Exchange

Reemplaza la VPN con acceso basado en identidad y contexto

Cloudflare DDoS Protection

Mitiga ataques automáticamente en menos de 3 segundos



Seguridad Física

La brecha más obvia y la más ignorada — entrar al edificio y conectar un USB supera toda defensa digital



[Índice](#)

EL PROBLEMA REAL

- Persona no autorizada entra siguiendo a un empleado ("tailgating")
- Servidor en una bodega sin control de temperatura ni acceso biométrico
- Tarjetas de acceso de exempleados nunca desactivadas
- Documentos impresos con información confidencial en la basura

CONTROLES ISO 27001

A.11.1

A.11.1.2

A.11.2

A.7.1

A.11.1.7

LO QUE APRENDES EN EL CURSO

Controles físicos ISO 27001 · Política de acceso · Auditoría física

IA QUE LO RESUELVE

Verkada AI CCTV

Detecta tailgating y objetos olvidados en tiempo real

HID + Reconocimiento facial

Control biométrico que detecta intentos de suplantación

ChatGPT / Gemini

Genera política de visitantes y checklist de auditoría física

Matriz completa · Las 7 capas de un vistazo

El mapa de ruta hacia ISO 27001 — amenaza principal, controles y la IA que acelera cada capa.



[Índice](#)

Capa	Amenaza principal 2026	Controles ISO 27001	IA que lo resuelve
7 · Humana	Phishing con deepfakes · CEO Fraud · Insider	A.6.3 · A.7.1	KnowBe4 · UEBA · ChatGPT
6 · Datos	Exfiltración a IA pública · Shadow IT · Ransomware	A.8.1 · A.8.2 · A.18.1	Purview · Macie · Forcepoint
5 · Aplicaciones	APIs expuestas · Librerías vulnerables · Inyecciones	A.14.1 · A.12.6 · A.14.2	GitHub Sec · Snyk · WAF ML
4 · Endpoints	Ransomware · Equipos sin parches · Robo de dispositivos	A.12.6 · A.8.19 · A.8.22	CrowdStrike · Intune · Automox
3 · Red	Movimiento lateral · Tráfico C2 · MITM	A.13.1 · A.12.4 · A.8.20	Sentinel · Darktrace · Cisco AI
2 · Perimetral	Bypassing VPN · DDoS · Zero-day exploits	A.13.1.1 · A.9.4 · A.13.2	Palo Alto · Zscaler · Cloudflare
1 · Física	Tailgating · USB malicioso · Robo de hardware	A.11.1 · A.11.2 · A.7.1	Verkada · HID · Gemini

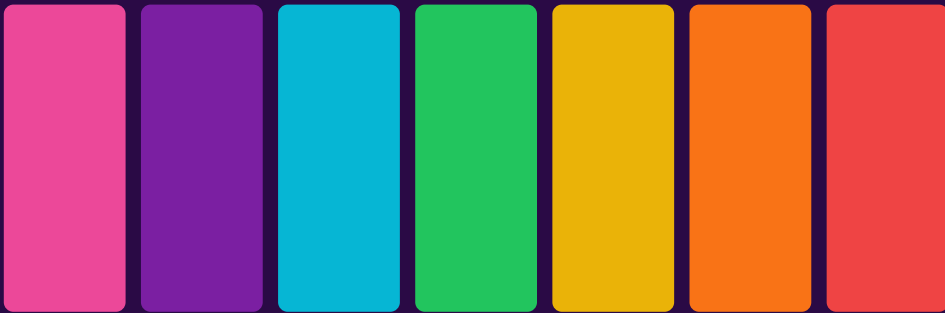
 **La tesis:** ninguna empresa puede contratar un especialista para cada capa. Un profesional certificado entiende las 7 de forma integrada — y la IA hace la implementación alcanzable.

Por qué ISO 27001 es la capa que une todo



[< Índice](#)

SIN ISO 27001 — 7 islas de seguridad



Cada capa se protege por separado, sin criterio común ni responsable claro.

CON ISO 27001 — un sistema de gestión



Gobierna las 7 con un solo sistema: qué controles aplicar, quién responde, cómo se audita.

Ciberseguridad NIST sabe qué proteger en cada capa. **ISO 27001** sabe cómo gobernarlo. Con **IA** se implementa en semanas, no meses.





¿Dudas o quieres profundizar en tu empresa?

Escríbenos por WhatsApp o [visita itservice.com.co](https://visita.itservice.com.co)
— un asesor te responde sin presión, a tu ritmo.



+57 3175889547

Gracias por acompañarnos

Esta matriz es tuya para guardar y compartir. Si quieres ver cómo se aplica exactamente a tu empresa, con gusto lo conversamos — sin compromiso.

Siguientes pasos de certificación, si quieres ir más allá:

Lead Cybersecurity NIST · perfil gobernanza y gestión

ISO 27001 Auditor Líder · perfil gobernanza y gestión

ISO 27001 Auditor Interno · perfil gobernanza y gestión

[< Volver al índice de la matriz](#)

