

6 OBLIGATORIOS, 3 OLVIDADOS Y 1 INVISIBLE

Los 9 básicos, la ISO 27001 y lo que tu empresa probablemente no está viendo

Carlos De Ferrari Lead GRC
Felipe Zepeda Expert GRC

2º Gobierno de Seguridad e IA



¿QUÉ SON?

9

**Medidas de seguridad simples
contra los ataques más comunes**
Sin grandes inversiones

2024

La Ley Marco de Ciberseguridad crea
la ANCI



2026

La ANCI publica las 9 medidas de
seguridad y propone que 6 sean
obligatorias

LOS 9 BÁSICOS, EN SIMPLE

CisoServiceChile

90%

de los incidentes de efecto significativo reportados a la ANCI en 2025 se podrían haber evitado con 6 medidas básicas

No hablamos de tecnología cara. Hablamos de lo básico, bien hecho y demostrable.



MANTEN TU MANO LEVANTA SI...

Y bájala apenas tu respuesta sea "no" o "no sé"

01

Tu empresa usa MFA en las cuentas críticas

02

Podrías mostrarle hoy la evidencia a un fiscalizador, en menos de una hora

03

Sabes qué herramientas de IA usó tu equipo esta semana y con qué datos

TU SEMÁFORO DE LOS 9 BÁSICOS

Califica cada uno mentalmente.



01

Actualizar



02

Capacitar



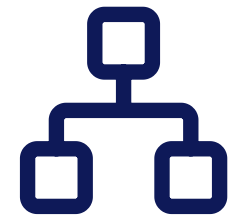
03

Minimizar
privilegios



04

Respaldar



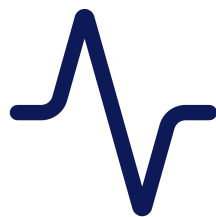
05

Asegurar redes



06

Asegurar
equipos



07

Monitorear en
tiempo real



08

Usar MFA



09

Gestor de
contraseñas

¿Cómo lo calificas?



Verde

Lo tengo y lo puedo demostrar



Amarillo

Lo tengo, pero no podría
demostrarlo hoy



Rojo

No lo tengo o no lo sé

Parte 1

6 OBLIGATORIOS

LO QUE SE VA A EXIGIR

LA PREGUNTA QUE TE VAN A HACER

Cada básico tiene un control ISO 27001 y una pregunta incómoda detrás



Actualizar

“¿Cuál fue el último parche crítico y cuántos días tardaste?”



Capacitar

“¿Cómo sabes que la capacitación cambió algo?”



Respaldar

“¿Cuándo fue tu última restauración probada?”



Asegurar equipos

“¿Cuántos equipos tienes y cuáles no están protegidos?”



Usar MFA

“¿Qué cuentas quedaron fuera del MFA, y por qué?”



Gestor de contraseñas

“¿Dónde vive hoy la contraseña del administrador?”

CisoServiceChile



TENERLO $\neq$ DEMOSTRARLO

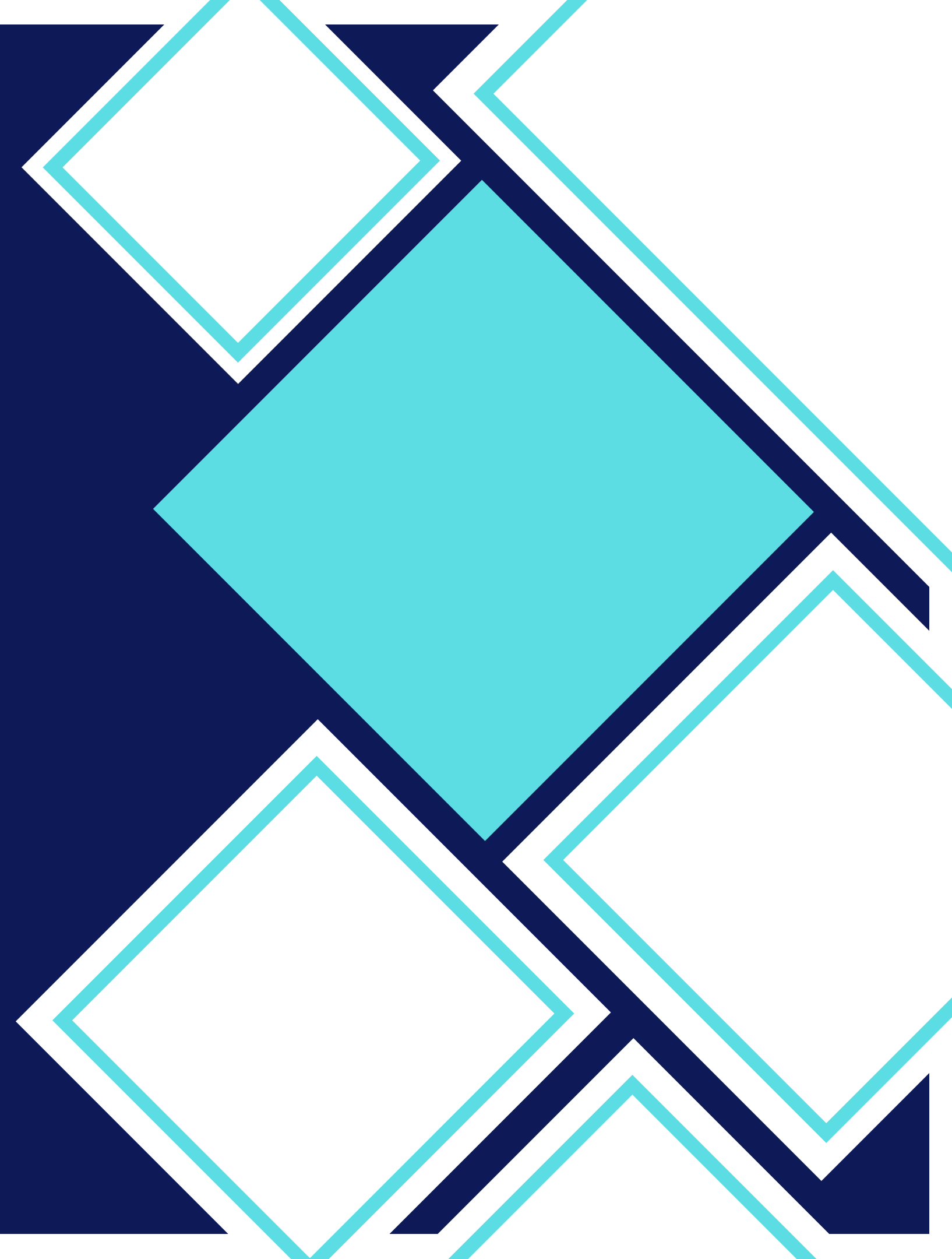
Política Registro Evidencia

Consulta ANCI 2026: 2 de cada 3 se declaran maduros...
...pero la mayoría no tiene respaldo documental

Parte 2

3 OLVIDADOS

Fuera de la propuesta obligatoria
¿o no?



¿OLVIDADOS? NO PARA LOS OIV

Fuera de la norma de los 6, pero ya exigidos a los operadores vitales desde diciembre de 2025



PRIVILEGIOS

Solo el acceso necesario

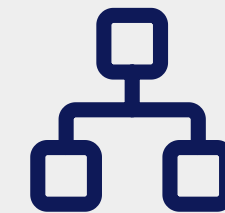
Instrucción N° 4: Restringir accesos y cambiar credenciales administrativas



MONITOREO

Si no lo ves, no existe

Instrucción N° 4: Herramientas de detección y contención



REDES

Segmentar para contener

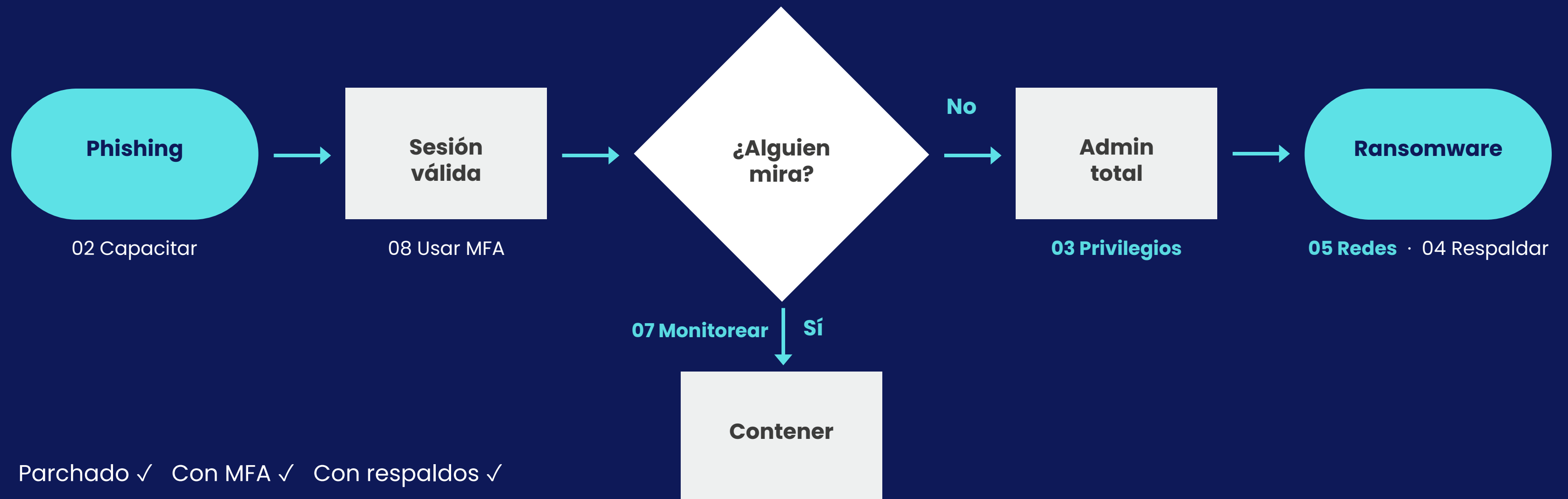
Instrucción N° 4: Cortafuegos con bloqueo por defecto y segmentación

915 organizaciones en el primer listado oficial de OIV. Si eres proveedor de una de ellas, esto también te llega.

CREDENCIAL VÁLIDA

CisoServiceChile

Un ataque que pasa los 6 obligatorios



Parte 3

1 INVISIBLE

SHADOW AI



Comercial

Contratos y propuestas en un chatbot



Recursos Humanos

CV y datos de personas



Finanzas

Planillas, sueldos y proveedores

SHADOW AI

No es un problema de TI

Ley 21.719 · 1 dic 2026

Un dato personal en un chatbot
ya es un problema legal

CÓMO ROMPE LOS BÁSICOS

No es un básico más:
rompe los que ya tienes

Privilegios → agentes con acceso total a correo y archivos

Capacitación → datos sensibles pegados en un chat público

Monitoreo → tráfico hacia IA sin ninguna visibilidad

MFA → cuentas personales fuera del SSO corporativo

LO QUE CUESTA LO INVISIBLE

Informe IBM Cost of a Data Breach 2025

1 de 5

Organizaciones reportó una brecha vinculada a Shadow AI

+USD 670 mil

Costo adicional por brecha con alto uso de Shadow AI

63%

De las organizaciones con brechas no tenía gobierno de IA o lo estaba desarrollando

Desde el 1 de diciembre de 2026, pegar datos personales en un chat es tratamiento de datos bajo la Ley 21.719.

ISO 27001

Seguridad de la información

- 4 Contexto
- 5 Liderazgo
- 6 Riesgos
- 7 Apoyo
- 8 Operación
- 9 Evaluación
- 10 Mejora

Anexo A: 93 controles



ISO 42001

Sistemas de IA

- 4 Contexto
- 5 Liderazgo
- 6 Riesgos
- 7 Apoyo
- 8 Operación
- 9 Evaluación
- 10 Mejora

Anexo A: 38 controles

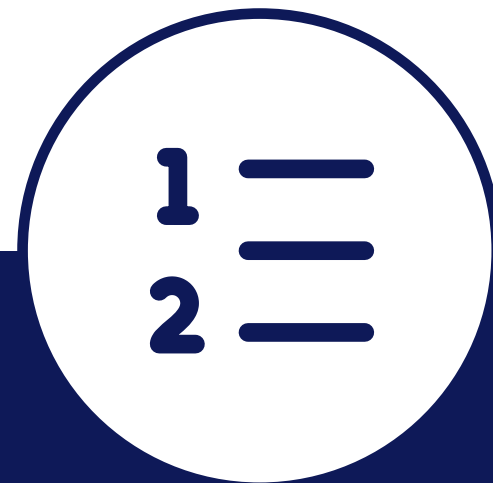
UN SISTEMA, NO PARCHES

DE CUMPLIR A ESTAR SEGURO



DIAGNOSTICAR

Los 6: brechas y evidencia



PRIORIZAR

Los 3: plan por riesgo



IMPLEMENTAR

El 1: IA gobernada



SOSTENER

Un SGSI que lo demuestra

CisoServiceChile



¿CUÁL ES TU PUNTO CIEGO?

La IA ya está en tu empresa. ¿Está en tu SGSI?

Te ayudamos a encontrarlo • CisoServiceChile

9 BÁSICOS × ISO 27001

BÁSICO ANCI	CONTROLES ISO 27001:2022	OBLIGATORIO*
Actualizar	Gestión de vulnerabilidades técnicas	Sí
Capacitar	Concienciación y formación	Sí
Minimizar privilegios	Derechos de acceso privilegiado	No
Respaldar	Respaldo de la información	Sí
Asegurar redes	Seguridad de redes	No
Asegurar equipos	Dispositivos de usuario final	Sí
Monitorear en tiempo real	Actividades de monitoreo	No
Usar MFA	Autenticación segura	Sí
Gestor de contraseñas	Información de autenticación	Sí