NexTReT

Executive Outlook Series

CISO Outlook 2027

Las 10 prioridades de ciberresiliencia, visibilidad y cumplimiento que marcarán la agenda ejecutiva

Briefing estratégico para evaluar si tu organización puede detectar, responder, recuperarse y demostrar control ante amenazas, auditorías y presión regulatoria.

MANIFIESTO EJECUTIVO

La ciberseguridad entra en una nueva fase: demostrar resiliencia

> **Prevenir ya no basta. Hay que detectar, contener, responder, recuperar y demostrar.**

El entorno de riesgo actual exige una evolución estratégica. La ciberseguridad deja de medirse por lo que evita y empieza a evaluarse por lo que la organización es capaz de soportar, gestionar y demostrar ante cualquier amenaza.

Las organizaciones deben acreditar su capacidad de visibilidad, respuesta, recuperación y gobierno. La resiliencia no es un estado, es una práctica continua que debe ser gestionada, probada y evidenciada.

RESUMEN EJECUTIVO

10 prioridades para una agenda CISO más ejecutiva, medible y resiliente

01

Resiliencia

La ciberseguridad se medirá cada vez más por la capacidad de operar y recuperarse.

02

Visibilidad

Sin visibilidad continua, no hay respuesta eficaz ni reporting ejecutivo fiable.

03

Identidad

Usuarios, máquinas, terceros y agentes de IA amplían el plano de control.

04

Evidencia

Cumplimiento significa demostrar controles, responsables y brechas.

05

Recuperación

Tener backup no equivale a poder restaurar servicios críticos a tiempo.

06

IA

La IA añade nuevos riesgos de datos, permisos, agentes y gobierno.

La agenda CISO 2027 se articula alrededor de una pregunta:
¿podemos demostrar control real sobre nuestros riesgos críticos?

EVOLUCIÓN DEL ROL CISO

De proteger sistemas a sostener confianza, continuidad y evidencia

El rol del CISO evoluciona desde la gestión táctica de controles hacia un liderazgo que habilita resiliencia, decisiones y confianza.

ANTES

- Herramientas desplegadas
- Controles por dominio
- Cumplimiento periódico
- Revisión reactiva de incidentes
- Reporting limitado a indicadores técnicos
- Seguridad entendida como barrera

AHORA

- Visibilidad continua
- Priorización por impacto
- Evidencia viva de cumplimiento
- Recuperación probada
- Gobierno de identidad, terceros e IA
- Seguridad entendida como resiliencia

El CISO deja de ser sólo el responsable de bloquear amenazas y pasa a ser un garante de resiliencia digital.

TRES PREGUNTAS EJECUTIVAS

01 | ¿Qué riesgos pueden afectar al negocio de forma material?

02 | ¿Qué capacidades reales tenemos para detectarlos, contenerlos y recuperarnos?

03 | ¿Qué evidencias podemos mostrar ante dirección, clientes, auditores o reguladores?

CONTEXTO ESTRATÉGICO

Cinco fuerzas que redefinen la ciberseguridad empresarial

01

Ransomware y extorsión digital

Siguen poniendo a prueba continuidad, disponibilidad y recuperación.

02

Regulación y responsabilidad ejecutiva

ENS, NIS2, DORA e ISO elevan la exigencia de evidencia y gobierno.

03

IA, shadow AI y agentes autónomos

Los usos de IA avanzan más rápido que los controles de seguridad y gobierno.

04

Complejidad cloud, identidad y terceros

SaaS, cloud y proveedores TIC amplían el perímetro real del riesgo.

05

Exigencia de recuperación y evidencia

La resiliencia debe probarse, no sólo declararse.

> Estas cinco fuerzas obligan a cambiar la conversación: de reducir exposición a construir una **capacidad demostrable de resiliencia**.

FRAMEWORK ESTRATÉGICO

Cyber Resilience Priority Framework

NexTReT propone un marco práctico para separar tendencias interesantes de prioridades que deberían entrar en roadmap, presupuesto o conversación ejecutiva.

01 Impacto ejecutivo

Continuidad, reputación, cumplimiento o Dirección.

02 Urgencia 2027

Presión regulatoria, amenaza, auditoría o presupuesto.

03 Brecha habitual

Frecuencia de inmadurez en organizaciones reales.

04 Capacidad de acción

Diagnóstico, mejora u operación concreta.

05 Convertir en acción

Decisiones, responsables, roadmap y seguimiento.

METODOLOGÍA

Cómo se puntúan las prioridades

El framework puntúa cada prioridad en cinco dimensiones para traducir la agenda 2027 en una hoja de ruta accionable.

Dimensión	Pregunta que responde
Impacto ejecutivo	¿Puede afectar continuidad, reputación, cumplimiento, clientes o Dirección?
Urgencia 2027	¿Debe entrar en roadmap, presupuesto o auditoría en los próximos meses?
Brecha habitual	¿Es frecuente encontrar inmadurez en esta área?
Capacidad de acción	¿Se puede diagnosticar, mejorar u operar de forma concreta?
Convertir en acción	¿Puede traducirse en decisiones, responsables, roadmap y seguimiento medible?

21-25
Prioridad crítica

17-20
Prioridad estratégica

13-16
Prioridad emergente

<13
Seguimiento

El valor del framework está en conectar la conversación técnica, ejecutiva y de acción.

En la siguiente página mostramos el ranking para 2027

RANKING GENERAL

Las 10 prioridades CISO 2027 según impacto y urgencia

01	Ransomware resilience	25/25
02	Security visibility & SIEM/SOC	25/25
03	Regulatory resilience	24/25
04	Recovery assurance	24/25
05	Identity, PAM & Zero Trust	23/25
06	AI security governance	22/25
07	Third-party ICT risk	21/25
08	AI-enabled SOC automation	21/25
09	Digital service observability	19/25
10	Crypto-agility	17/25

Las cuatro primeras prioridades combinan impacto ejecutivo alto, urgencia inmediata y capacidad clara de convertirse en assessment o proyecto.

MATRIZ DE PRIORIZACIÓN

Qué actuar ahora, qué planificar y qué monitorizar

Enfoca tu estrategia donde más importa

PRIORIDAD 01

Resiliencia frente a ransomware

El ransomware ya no es sólo un problema de endpoint. Es una prueba de continuidad, recuperación y gobierno.

1. Qué cambia en 2027

- Los ataques buscan continuidad del negocio, no sólo cifrado de datos.
- Los atacantes explotan privilegios y cuentas para moverse lateralmente.
- Los backups aislados y probados son ahora un requisito, no una opción.

2. Riesgo de no actuar

Una falsa sensación de seguridad puede llevar a un bloqueo operativo total, pérdida de ingresos, impacto reputacional y sanciones regulatorias. La recuperación sin preparación es lenta, costosa y, en muchos casos, imposible.

3. Preguntas clave

- ¿Conocemos nuestros activos críticos y dependencias?
- ¿Detectamos comportamientos de cifrado a tiempo?
- ¿Aplicamos el mínimo privilegio de forma efectiva?
- ¿Podemos restaurar sin pagar ni negociar?

4. Acciones 90 días

- Identificar dependencias críticas y escenarios de interrupción.
- Revisar exposición de endpoints, accesos remotos y cuentas privilegiadas.
- Validar backups: aislamiento, integridad y pruebas de restauración.
- Ejecutar ejercicio de mesa con TI, legal, comunicación y negocio.

ASSESSMENT RECOMENDADO

Ransomware Readiness Assessment

Evalúa su preparación frente a ransomware y su capacidad de recuperar operaciones críticas sin pagar rescates.

PRIORIDAD 02

Visibilidad continua y SIEM/SOC moderno

No se puede responder a lo que no se ve.

1. Qué cambia en 2027

- La visibilidad debe conectar endpoint, identidad, red, cloud y aplicaciones.
- Importa más la calidad de la correlación que el volumen de eventos.
- El reporting ejecutivo debe traducir señales técnicas en decisiones.

2. Riesgo de no actuar

Los incidentes pueden permanecer invisibles, la respuesta se ralentiza y la organización pierde capacidad para explicar qué ocurrió, qué activos se vieron afectados y qué controles fallaron.

3. Preguntas clave

- ¿Qué fuentes críticas están integradas?
- ¿Dónde tenemos huecos de visibilidad?
- ¿Las alertas están priorizadas por riesgo?
- ¿Podemos generar reporting útil para Dirección?

4. Acciones 90 días

- Mapear logs y telemetría crítica.
- Identificar huecos de integración.
- Definir casos de uso prioritarios.
- Revisar reglas, falsos positivos y KPIs.

ASSESSMENT RECOMENDADO

Security Visibility Assessment

Evalúa si tu organización dispone de visibilidad suficiente para detectar, priorizar y responder.

PRIORIDAD 03

Cumplimiento ENS/NIS2/DORA con evidencia

Cumplir no es suficiente si no se puede demostrar de forma continua.

1. Qué cambia en 2027

- El cumplimiento exige controles, responsables y evidencias vivas.
- La conversación pasa de documentación a gobierno continuo.
- Dirección y auditoría esperan trazabilidad y reporting claro.

2. Riesgo de no actuar

Las brechas de cumplimiento pueden traducirse en sanciones, retrasos en auditorías, pérdida de contratos y dificultades para demostrar diligencia ante un incidente o regulador.

3. Preguntas clave

- ¿Qué marcos nos aplican realmente?
- ¿Tenemos mapa de controles y evidencias?
- ¿Quién es responsable de cada control?
- ¿Qué brechas requieren remediación inmediata?

4. Acciones 90 días

- Ejecutar gap analysis inicial.
- Mapear controles y evidencias.
- Clasificar brechas por impacto.
- Definir responsables y plan de remediación.

ASSESSMENT RECOMENDADO

Auditoría Express ENS/NIS2

Identifica brechas, prioriza acciones y construye una hoja de ruta realista de cumplimiento.

PRIORIDAD 04

Backup inmutable y recuperación verificable

Tener backup no significa poder recuperarse.

1. Qué cambia en 2027

- La conversación pasa de copias disponibles a recuperación verificable.
- Los backups deben resistir ransomware y sabotaje.
- RPO/RTO reales deben probarse, no asumirse.

2. Riesgo de no actuar

La falsa sensación de seguridad puede ocultar copias incompletas, restauraciones lentas o backups afectados por el propio incidente, comprometiendo la continuidad del negocio.

3. Preguntas clave

- ¿Cuándo probamos la última restauración?
- ¿Qué RPO/RTO son reales?
- ¿Existen copias aisladas o inmutables?
- ¿Qué dependencias frenarían la recuperación?

4. Acciones 90 días

- Inventariar sistemas críticos y políticas.
- Validar RPO/RTO por servicio.
- Ejecutar pruebas de restauración.
- Revisar aislamiento, inmutabilidad y retención.

ASSESSMENT RECOMENDADO

Backup Health Check

Verifica si tus copias son suficientes, recuperables y resistentes frente a ransomware o disrupción.

PRIORIDAD 05

Identidad, accesos, PAM y Zero Trust

La identidad ya es infraestructura crítica.

1. Qué cambia en 2027

- La identidad es el nuevo plano de control.
- PAM se vuelve clave para privilegios, terceros y cuentas de servicio.
- Zero Trust reduce la confianza implícita y exige verificación continua.

2. Riesgo de no actuar

Privilegios excesivos, MFA incompleto, accesos de terceros sin revisión y cuentas huérfanas pueden facilitar intrusiones, movimiento lateral y abuso de automatizaciones.

3. Preguntas clave

- ¿Inventariamos identidades humanas y no humanas?
- ¿Qué accesos privilegiados revisamos hoy?
- ¿MFA cubre accesos críticos?
- ¿Los terceros tienen propietario y caducidad?

4. Acciones 90 días

- Inventariar privilegios y cuentas de servicio.
- Revisar accesos de terceros.
- Validar MFA y acceso condicional.
- Reducir privilegios excesivos y definir alertas.

ASSESSMENT RECOMENDADO

Identity & Privileged Access Risk Review

Evalúa exposición asociada a identidades, privilegios, MFA, accesos críticos y PAM.

PRIORIDAD 06

Gobierno de IA, shadow AI y agentes autónomos

El riesgo de IA no está sólo en el modelo.

1. Qué cambia en 2027

- La IA amplía la superficie de riesgo antes que los modelos de gobierno.
- Los agentes heredan permisos, datos y acciones sobre sistemas reales.
- El shadow AI puede crecer más rápido que las políticas internas.

2. Riesgo de no actuar

La organización puede exponer datos sensibles, habilitar automatizaciones no autorizadas y perder trazabilidad sobre qué herramientas de IA usan sus equipos y con qué permisos.

3. Preguntas clave

- ¿Qué herramientas IA se utilizan hoy?
- ¿Qué datos se comparten?
- ¿Qué agentes tienen permisos sobre sistemas internos?
- ¿Existen políticas y registros suficientes?

4. Acciones 90 días

- Inventariar herramientas y casos de uso.
- Clasificar datos expuestos.
- Definir política de uso aceptable.
- Revisar permisos, logs y monitorización.

ASSESSMENT RECOMENDADO

AI Security Readiness Review

Identifica usos de IA, riesgos de datos, brechas de gobierno y controles necesarios.

PRIORIDAD 07

Riesgo de terceros y proveedores TIC críticos

El perímetro de riesgo ya incluye dependencias externas.

1. Qué cambia en 2027

- Cloud, SaaS y proveedores forman parte del perímetro real.
- DORA y NIS2 elevan la exigencia sobre terceros críticos.
- La dependencia operativa debe medirse y gobernarse.

2. Riesgo de no actuar

La organización puede sufrir caídas de servicio, exposición de datos, dependencia excesiva o falta de evidencias sobre proveedores que hoy sostienen procesos críticos.

3. Preguntas clave

- ¿Qué proveedores TIC son realmente críticos?
- ¿Qué accesos y datos manejan?
- ¿Exigimos evidencias mínimas de seguridad?
- ¿Tenemos plan si un proveedor falla?

4. Acciones 90 días

- Identificar proveedores TIC críticos.
- Clasificar dependencias por impacto.
- Revisar accesos, datos y evidencias.
- Definir requisitos y contingencias.

ASSESSMENT RECOMENDADO

Third-Party ICT Risk Review

Evalúa dependencias, accesos, evidencias y continuidad asociada a proveedores críticos.

PRIORIDAD 08

SOC con automatización e IA operativa

El SOC debe evolucionar de centro de alertas a sistema de respuesta priorizada.

1. Qué cambia en 2027

- El SOC debe orientarse a valor operativo, no sólo a volumen.
- La automatización reduce ruido y acelera decisiones.
- La IA ayuda a priorizar y asistir el triage.

2. Riesgo de no actuar

Sin priorización ni automatización, el SOC se satura, aumentan los falsos positivos y se ralentiza la capacidad de contener incidentes relevantes.

3. Preguntas clave

- ¿Qué alertas son ruido recurrente?
- ¿Qué casos de uso están priorizados?
- ¿Qué respuestas podemos automatizar?
- ¿Qué KPIs ve Dirección?

4. Acciones 90 días

- Revisar reglas y falsos positivos.
- Priorizar casos de uso de mayor impacto.
- Definir runbooks de respuesta.
- Establecer KPIs y reporting ejecutivo.

ASSESSMENT RECOMENDADO

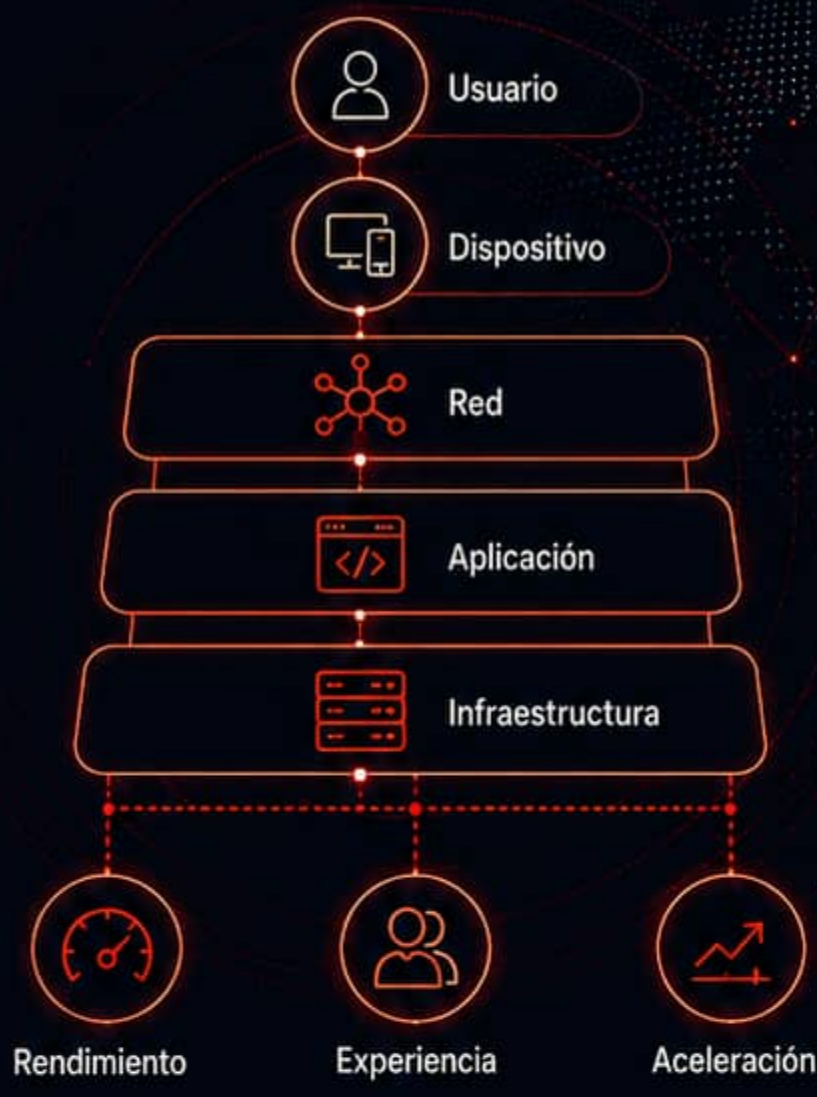
SOC Maturity Review

Evalúa madurez SOC, automatización, calidad de alertas y capacidad de respuesta.

PRIORIDAD 09

Observabilidad, rendimiento y experiencia digital

La resiliencia también se mide en la experiencia real de usuarios, aplicaciones y red.



1. Qué cambia en 2027

- La observabilidad conecta experiencia, red, apps e infraestructura.
- La degradación invisible impacta continuidad y negocio.
- Rendimiento y aceleración entran en la agenda ejecutiva.

2. Riesgo de no actuar

Los fallos de experiencia, latencia o bajo rendimiento pueden escalar sin visibilidad suficiente y afectar productividad, clientes o servicios críticos.

3. Preguntas clave

- ¿Qué servicios digitales son críticos?
- ¿Detectamos degradaciones antes que el usuario?
- ¿Qué ocurre entre red, app e infraestructura?
- ¿Podemos correlacionar experiencia e impacto?

4. Acciones 90 días

- Identificar journeys y servicios críticos.
- Definir métricas de experiencia real.
- Revisar degradaciones recurrentes.
- Priorizar mejoras por impacto de negocio.

ASSESSMENT RECOMENDADO

Digital Experience & Network Observability Assessment

Identifica degradaciones, latencia y riesgos operativos en servicios digitales críticos.

PRIORIDAD 10

Preparación post-cuántica y criptoagilidad

No será el proyecto más urgente para todos, pero sí una señal de madurez futura.

1. Qué cambia en 2027

- La prioridad es construir inventario y criterio.
- Importa entender datos sensibles de larga duración.
- La criptoagilidad exige coordinación con proveedores.

2. Riesgo de no actuar

La organización puede llegar tarde a una transición compleja y no entender qué sistemas, datos o dependencias requieren preparación anticipada.

3. Preguntas clave

- ¿Qué criptografía usamos hoy?
- ¿Qué datos deben seguir protegidos durante años?
- ¿Qué proveedores gestionan cifrado crítico?
- ¿Tenemos hoja de ruta de criptoagilidad?

4. Acciones 90 días

- Identificar sistemas con criptografía crítica.
- Clasificar datos sensibles de larga duración.
- Revisar proveedores y dependencias.
- Definir un roadmap inicial.

ASSESSMENT RECOMENDADO

Crypto-Agility Roadmap

Construye una primera visión de exposición criptográfica y pasos de preparación futura.

PRIORIDADES

Las prioridades no son silos: forman una cadena de resiliencia

Prevenir, detectar, contener, responder, recuperar y demostrar.

PREVENIR	DETECTAR	CONTENER	RESPONDER	RECUPERAR	DEMOSTRAR
Reducimos la probabilidad de incidente	Obtenemos visibilidad y contexto	Limitamos el impacto y el alcance	Actuamos rápido y con coordinación	Restauramos confiabilidad y continuidad	Probamos y evidenciamos cumplimiento
• Identidad y PAM • Zero Trust y acceso mínimo • Gestión de vulnerabilidades • Seguridad en terceros TIC	• SIEM/SOC moderno • Observabilidad unificada • Detección con IA y comportamiento • Inteligencia de amenazas	• Segmentación y microsegmentación • Control de accesos en tiempo real • Aislamiento de activos críticos • Playbooks de contención	• Automatización del SOC • SOAR y orquestación • Gestión de incidentes • Comunicación y crisis	• Backup inmutable y verificable • Planes de recuperación • Pruebas y ejercicios • Resiliencia de negocio	• Cumplimiento ENS/NIS2/DORA • Auditoría continua • Trazabilidad y evidencia • Reporting ejecutivo

CAPACIDADES TRANSVERSALES QUE HACEN POSIBLE LA CADENA

IA y agentes autónomos | Personas, cultura y roles | Nube segura y soberana | Automatización y orquestación | Métricas, KPIs y mejora continua | Criptoagilidad y resiliencia cuántica

La ciberresiliencia real aparece cuando estas capacidades se conectan.

PRÓXIMO PASO

De prioridad ejecutiva a diagnóstico accionable

Cada prioridad debe traducirse en una brecha identificable, un diagnóstico concreto y un plan de acción.

Prioridad	Pregunta ejecutiva	Diagnóstico recomendado
1 Ransomware	¿Podríamos detectar, contener y recuperar un ataque?	Ransomware Readiness Assessment
2 Visibilidad y SIEM/SOC	¿Estamos viendo las señales críticas?	Security Visibility Assessment
3 Cumplimiento	¿Podemos demostrar control ante auditoría o regulador?	Auditoría Express ENS/NIS2
4 Backup y recuperación	¿Nuestros backups son realmente recuperables?	Backup Health Check
5 Identidad, accesos y PAM	¿Quién puede acceder a qué y con qué privilegios?	Identity & Privileged Access Risk Review
6 IA y shadow AI	¿Qué usos de IA existen y qué riesgos generan?	AI Security Readiness Review
7 Terceros TIC	¿Qué proveedores pueden afectar continuidad o cumplimiento?	Third-Party ICT Risk Review
8 SOC + automatización	¿Qué parte del SOC es ruido y qué parte genera respuesta útil?	SOC Maturity Review
9 Observabilidad y rendimiento	¿Qué degradaciones afectan servicios críticos?	Digital Experience & Network Observability Assessment
10 Criptoagilidad	¿Qué datos y sistemas requieren preparación futura?	Crypto-Agility Roadmap

Una prioridad bien definida debe traducirse en diagnóstico, decisión y seguimiento.

AUTOEVALUACIÓN

Cyber Resilience Priority Score

Una autoevaluación inicial para identificar exposición, madurez parcial y oportunidades de mejora.

0–39
Exposición alta
Riesgos significativos y controles insuficientes.

40–69
Madurez parcial
Controles básicos, con brechas relevantes.

70–84
Resiliencia razonable
Controles adecuados, con mejoras necesarias.

85–100
Resiliencia avanzada
Controles sólidos y capacidad adaptativa.

Cómo funciona

- 0 puntos: no existe o no se ha revisado
- 5 puntos: existe parcialmente
- 10 puntos: está implantado, probado y documentado

La pregunta clave no es sólo qué puntuación obtienes, sino qué prioridad deberías revisar primero.

CHECKLIST

Autoevaluación rápida

Responde No, Parcialmente o Sí para cada una de las 10 prioridades.

1. ¿Hemos evaluado la exposición real frente a ransomware?

○ No ○ Parcialmente ○ Sí

2. ¿Tenemos visibilidad centralizada sobre eventos críticos?

○ No ○ Parcialmente ○ Sí

3. ¿Podemos demostrar evidencias de cumplimiento?

○ No ○ Parcialmente ○ Sí

4. ¿Hemos probado restauración y recuperación?

○ No ○ Parcialmente ○ Sí

5. ¿Controlamos accesos críticos, MFA y PAM?

○ No ○ Parcialmente ○ Sí

6. ¿Tenemos visibilidad y políticas sobre IA y shadow AI?

○ No ○ Parcialmente ○ Sí

7. ¿Evaluamos de forma estructurada el riesgo de terceros TIC?

○ No ○ Parcialmente ○ Sí

8. ¿El SOC prioriza y automatiza parte de la respuesta?

○ No ○ Parcialmente ○ Sí

9. ¿Monitorizamos experiencia real, red, apps y servicios críticos?

○ No ○ Parcialmente ○ Sí

10. ¿Existe un roadmap de ciberresiliencia 2027 priorizado?

○ No ○ Parcialmente ○ Sí

No sustituye una auditoría técnica; ayuda a identificar por dónde empezar.

INTERPRETACIÓN

Qué significa tu score

El valor no está sólo en la cifra final,
sino en identificar qué prioridad revisar primero.

MENOR MADUREZ — MAYOR MADUREZ

0–39 | 40–69 | 70–84 | 85–100

0–39
Exposición alta

Priorizar un diagnóstico inicial y acciones de corto plazo.

- Riesgo elevado de incidentes y disrupciones.
- Brechas críticas en múltiples dominios.
- Requiere foco inmediato y recursos dedicados.

40–69
Madurez parcial

Convertir brechas críticas en un plan priorizado.

- Capacidades presentes pero inconsistentes.
- Dependencias y controles que limitan la resiliencia.
- Enfoque en fortalecer detección y recuperación.

70–84
Resiliencia razonable

Validar puntos críticos antes del roadmap 2027.

- Base sólida con algunos riesgos residuales.
- Procesos definidos pero con variabilidad.
- Asegurar cobertura, pruebas y medición continua.

85–100
Resiliencia avanzada

Optimizar, automatizar y reforzar evidencias.

- Capacidades robustas y basadas en datos.
- Automatización y mejora continua en marcha.
- Mantener ventajas y prepararse para lo inesperado.

PREGUNTAS QUE REVELAN PATRONES

¿Puntuamos bajo en detección?

¿La recuperación no está probada?

¿Hay brechas de identidad o PAM?

¿La IA se usa sin gobierno?

DE PREOCUPACIÓN A ACCIÓN

Roadmap 90 días

(ORIENTATIVO - EJEMPLO)

Una secuencia práctica para pasar de brechas críticas a un roadmap 2027.

Semanas 1–2

Inventario, visibilidad y activos críticos

- Identificar sistemas, datos y dependencias.
- Mapear fuentes de visibilidad.
- Revisar proveedores TIC y accesos críticos.

Semanas 3–4

Brechas, riesgos y quick wins

- Evaluar ransomware, SIEM y backup.
- Revisar cumplimiento, identidad y PAM.
- Priorizar quick wins de alto impacto.

Mes 2

Remediación priorizada y pruebas

- Mejorar detección y reducir privilegios.
- Probar restauración y runbooks.
- Formalizar evidencias iniciales.

Mes 3

Roadmap ejecutivo y seguimiento

- Asignar responsables e inversiones.
- Definir KPIs y reporting.
- Construir él roadmap CISO 2027.

El objetivo no es hacerlo todo a la vez, sino empezar por el riesgo con mayor impacto.

DECISION TREE

¿Por dónde empezar?

Un árbol de decisión para identificar el diagnóstico más útil según tu situación actual.

No todas las organizaciones deben empezar por lo mismo; deben empezar por el riesgo que más condiciona negocio, cumplimiento o continuidad.

ECOSISTEMA NEXTRET

Capacidades conectadas para ejecutar la agenda CISO 2027

La ciberresiliencia no se construye con iniciativas aisladas, sino con capacidades integradas.

Cyber Resilience

1. **Ransomware & XDR**
   SentinelOne
   Protección preventiva, detección y respuesta ante amenazas avanzadas.

2. **Cumplimiento & Evidencias**
   ENS / NIS2 / DORA
   Alinear, evidenciar y demostrar cumplimiento normativo.

3. **Backup & Recuperación**
   Backup Health Check
   Asegurar recuperabilidad, resiliencia y continuidad operativa.

4. **Visibilidad & SOC**
   SIEM / Wazuh / SOC
   Visibilidad completa, contexto y capacidades de detección.

5. **Identity & PAM**
   IAM / PAM / MFA / privilegios
   Gestionar identidades, accesos privilegiados y mínimo privilegio.

6. **Observabilidad & Rendimiento**
   Riverbed / experiencia / red
   Experiencia digital óptima y rendimiento de red con visibilidad real.

7. **Third-Party ICT Risk**
   Dependencias críticas
   Visibilidad y gestión del riesgo de proveedores y terceros.

8. **Managed Services / Roadmap**
   Operación, seguimiento y mejora continua
   Acompañamiento experto para ejecutar, operar y evolucionar.

NexTReT conecta diagnóstico, implantación y operación para convertir prioridades en capacidades reales.

SIGUIENTE PASO

Convierte estas prioridades en un roadmap accionable

Te ayudamos a traducir exposición, brechas y urgencias en una secuencia clara de decisiones.

1. Identificar la prioridad correcta

Entendemos tu contexto, riesgos clave y presiones que más impactan.

2. Activar el assessment adecuado

Ejecutamos el diagnóstico más útil para tu situación actual.

3. Definir roadmap y quick wins

Priorizamos acciones, capacidades y próximos pasos con impacto medible.

Escanea para solicitar una sesión ejecutiva de priorización.*

*Gratuita. Sin Compromiso.

La diferencia entre una preocupación difusa y una estrategia real está en cómo se prioriza, se diagnostica y se ejecuta.