

28 COMPROBACIONES

Kit de Autodiagnóstico de Exposición Privilegiada

Haz visibles cuentas, accesos, terceros y sesiones que podrían estar quedando fuera de control.

Incluye

- Checklist ejecutivo en 7 dimensiones
- Mapa rápido de identidades y accesos
- Matriz de evidencias y preparación
- Plan de acción a 30, 60 y 90 días
- Plantilla Excel editable

Una revisión útil antes de elegir tecnología

Completa el kit con Seguridad, Infraestructura, IAM, Operaciones y, cuando corresponda, Auditoría o Compliance.

Objetivo

Detectar señales de exposición y reunir la información necesaria para decidir qué corregir primero, qué validar con evidencia y qué merece un análisis más profundo.

No necesitas disponer ya de una plataforma PAM.

No escribas contraseñas, secretos, tokens ni información sensible en este documento.

Datos de la revisión

ORGANIZACIÓN

RESPONSABLE

FECHA

SCOPE INICIAL

Qué contiene el kit

01

Checklist

28 comprobaciones
en siete dimensiones.

02

Inventario

Personas, cuentas,
terceros, secretos y
activos.

03

Evidencias

Qué puedes
demostrar hoy y qué
falta localizar.

04

Prioridades

Acciones inmediatas,
a 60 días y a 90 días.

Importante

Este autodiagnóstico ofrece una orientación inicial. No es una certificación, un benchmark ni una probabilidad de incidente. El PAES se reserva al Privileged Access Exposure Assessment de NexTReT, con scope y evidencia revisados.

Completa el kit en cuatro pasos

Usa la respuesta que mejor representa el scope revisado. Si no puedes confirmarla, marca “No lo sé”: la falta de visibilidad también es una señal.

1

Delimita el scope

Empieza por un grupo manejable: activos críticos, un dominio, un proveedor o un caso de uso.

2

Responde con evidencia

Distingue lo que está implantado y probado de lo que solo está documentado o declarado.

3

Registra los gaps

Lleva al Excel cada respuesta parcial, no controlada o desconocida.

4

Prioriza por fases

Define acciones a 30, 60 y 90 días y asigna un responsable.

Leyenda de respuestas

- **Controlado** El control opera de forma consistente y existe evidencia actual.
- **Parcial** Existe una base, pero la cobertura es incompleta, manual o irregular.
- **No controlado** El control no está implantado o no cubre el scope revisado.
- **No lo sé** No hay visibilidad o no se puede localizar evidencia suficiente.

Consejo: una respuesta “Controlado” sin evidencia localizable debe revisarse antes de darla por cerrada.

1. Inventario e identificación

Personas, cuentas no humanas, propietarios, activos y cuentas huérfanas.

EVIDENCIAS ÚTILES

Export de directorios, CMDB, inventario PAM/IAM, listado de cuentas locales, tickets de alta y baja.

01 ¿Existe un inventario actualizado de identidades y cuentas privilegiadas, humanas y no humanas, en los entornos relevantes?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

02 ¿Cada cuenta privilegiada tiene propietario, finalidad, alcance y relación con los activos que administra?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

03 ¿Se identifican y revisan cuentas compartidas, por defecto, de emergencia, inactivas y potencialmente huérfanas?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

04 ¿Los privilegios se retiran o ajustan cuando cambia el rol, finaliza una relación laboral o termina un servicio externo?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

2. Credenciales y secretos

Custodia, exposición, rotación y ciclo de vida de contraseñas, claves, tokens y certificados.

EVIDENCIAS ÚTILES

Política de credenciales, vault, configuraciones de rotación, repositorios de secretos, muestras de cuentas de servicio.

05 ¿Las credenciales privilegiadas se custodian en mecanismos aprobados, sin depender de documentos, scripts, correo o conocimiento personal?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

06 ¿Las contraseñas y secretos se rotan con una frecuencia definida y, cuando corresponde, después de cada uso?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

07 ¿Claves, tokens, certificados y credenciales de cuentas de servicio están inventariados y tienen un ciclo de vida gestionado?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

08 ¿El uso de credenciales compartidas puede atribuirse a una persona concreta y se evita la reutilización innecesaria?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

3. Autorización y mínimo privilegio

Roles, segregación, aprobación, acceso temporal y privilegios permanentes.

EVIDENCIAS ÚTILES

Matriz de roles, grupos administrativos, flujos de aprobación, accesos temporales, revisiones y excepciones.

09 ¿Las tareas administrativas se realizan con cuentas nominativas separadas de las cuentas de uso diario?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

10 ¿Los roles y permisos limitan el alcance a lo estrictamente necesario, evitando privilegios amplios por defecto?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

11 ¿La concesión de privilegios requiere aprobación y una justificación técnica o de negocio verificable?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

12 ¿Se utiliza acceso temporal o elevación bajo demanda y se controla el acceso de emergencia?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

4. Autenticación y contexto

MFA, identidad individual, dispositivo, ubicación y condiciones de acceso.

EVIDENCIAS ÚTILES Políticas MFA, acceso condicional, configuración de protocolos, excepciones y registros de autenticación.

13 ¿El acceso privilegiado exige MFA de forma consistente en los sistemas y casos de uso relevantes?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

14 ¿Se consideran contexto y riesgo, como dispositivo, ubicación, red, horario o protocolo, antes de permitir el acceso?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

15 ¿Cada administrador y tercero utiliza una identidad individual, evitando cuentas genéricas para autenticarse?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

16 ¿Los protocolos heredados, cuentas técnicas y excepciones que pueden eludir controles están identificados y revisados?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

5. Control de sesión

Aislamiento, monitorización, grabación, comandos, alertas y terminación.

EVIDENCIAS ÚTILES

Registros de sesión, grabaciones, alertas, integración SIEM, reglas de comando y procedimientos de terminación.

17 ¿Las sesiones privilegiadas se intermedian o aíslan cuando el nivel de criticidad lo requiere?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

18 ¿Las sesiones sobre activos críticos quedan registradas o grabadas y pueden localizarse de forma ágil?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

19 ¿Existen alertas y capacidad de respuesta ante comandos anómalos, elevaciones inesperadas o accesos fuera de contexto?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

20 ¿La evidencia conecta identidad, aprobación, credencial, activo, inicio y fin de sesión y acciones realizadas?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

6. Terceros y acceso remoto

Identidad, alcance, ventana temporal, revocación y trazabilidad de proveedores.

EVIDENCIAS ÚTILES

Inventario de proveedores, patrocinadores internos, contratos, VPN/ZTNA, ventanas de acceso y bajas.

21 ¿Todos los proveedores con acceso privilegiado están inventariados y cuentan con un responsable interno?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

22 ¿Su acceso está limitado a activos, tareas y ventanas temporales concretas y se habilita solo cuando es necesario?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

23 ¿La revocación se ejecuta con rapidez cuando termina el contrato, cambia el personal o deja de existir la necesidad?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

24 ¿Las sesiones de terceros aplican MFA, registro y revisión con criterios equivalentes a los accesos internos?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

7. Gobierno y operación

Políticas, revisiones, evidencias, runbooks, métricas, integraciones y mejora continua.

EVIDENCIAS ÚTILES

Política PAM, RACI, recertificaciones, runbooks, SLAs, métricas, informes de excepción y comités de revisión.

25 ¿Existe una política aprobada para accesos privilegiados que define roles, excepciones y acceso de emergencia?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

26 ¿Se realizan recertificaciones periódicas y revisiones de cuentas huérfanas, inactivas o con privilegios excesivos?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

27 ¿Hay responsables, runbooks y niveles de servicio para onboarding, rotación, incidencias y evidencias de auditoría?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

28 ¿Se revisan métricas de cobertura, antigüedad, excepciones, fallos de control y adopción para impulsar mejoras?

☐ Controlado ☐ Parcial ☐ No controlado ☐ No lo sé

EVIDENCIA, EXCEPCIÓN O SIGUIENTE PASO

Convierte respuestas en decisiones

No sumes respuestas para crear un PAES. Usa este semáforo para localizar señales y decidir qué validar primero.

Prioridad inmediata	Validación necesaria	Base a mantener
Credenciales expuestas, cuentas huérfanas, accesos indefinidos, ausencia de MFA o sesiones críticas sin trazabilidad.	Controles manuales, excepciones, cobertura desigual o evidencia difícil de localizar.	Control consistente, propietario claro, revisión periódica y evidencia actual disponible.

Semáforo por dimensión

Marca el estado que mejor resume cada dimensión y registra la principal señal.

Inventario e identificación	☐ Base	☐ Validar	☐ Prioridad	
Credenciales y secretos	☐ Base	☐ Validar	☐ Prioridad	
Autorización y mínimo privilegio	☐ Base	☐ Validar	☐ Prioridad	
Autenticación y contexto	☐ Base	☐ Validar	☐ Prioridad	
Control de sesión	☐ Base	☐ Validar	☐ Prioridad	
Terceros y acceso remoto	☐ Base	☐ Validar	☐ Prioridad	
Gobierno y operación	☐ Base	☐ Validar	☐ Prioridad	

Siguiente paso recomendado

Pasa las señales rojas y ámbar al Plan de 90 días del Excel y asigna propietario, fecha y evidencia esperada.

Empieza por los accesos más sensibles

Este mapa sirve para delimitar el scope. Utiliza la plantilla Excel para mantener el inventario completo y priorizado.

Seis tipos que conviene localizar

Administradores
Dominio, cloud, red, bases de datos, aplicaciones y OT.

Cuentas de servicio
Procesos, integraciones, tareas programadas y automatizaciones.

Terceros
Proveedores, soporte remoto, mantenimiento y proyectos.

Cuentas compartidas
Genéricas, locales, de equipo y de emergencia.

Secretos
Claves API, tokens, certificados, SSH y credenciales embebidas.

Activos críticos
Sistemas cuya administración puede afectar operación o datos sensibles.

Muestra de inventario

Identidad / cuenta	Tipo	Activo / entorno	Propietario	Señal prioritaria

No registres secretos: anota únicamente el tipo, la ubicación de custodia y su propietario.

Evidencia que puedes demostrar hoy

Una política indica intención. La evidencia operativa demuestra que el control se aplica, se revisa y deja trazabilidad.

EVIDENCIA	ESTADO	PROPIETARIO / UBICACIÓN
Inventario de cuentas y propietarios	☐ Disponible ☐ Parcial ☐ No	
Matriz de roles y grupos privilegiados	☐ Disponible ☐ Parcial ☐ No	
Política de accesos privilegiados	☐ Disponible ☐ Parcial ☐ No	
Configuración MFA y acceso condicional	☐ Disponible ☐ Parcial ☐ No	
Flujos de aprobación y accesos temporales	☐ Disponible ☐ Parcial ☐ No	
Registros o grabaciones de sesión	☐ Disponible ☐ Parcial ☐ No	
Inventario de terceros y fechas de baja	☐ Disponible ☐ Parcial ☐ No	
Recertificaciones, excepciones y métricas	☐ Disponible ☐ Parcial ☐ No	

Regla práctica

Clasifica la evidencia como actual y verificable, documentada pero no comprobada, declarada o desconocida. Evita considerar un control como cerrado si no puedes localizar una prueba suficiente.

El Excel incluye una matriz ampliada para registrar fuente, fecha, responsable y siguiente revisión.

Construye un plan a 30, 60 y 90 días

Empieza por reducir exposición inmediata, luego estabiliza el control y finalmente convierte la mejora en operación repetible.

0-30 días | Contener

Retirar accesos innecesarios, bloquear cuentas huérfanas, corregir secretos expuestos, acotar terceros y activar controles básicos.

ACCIONES, RESPONSABLE Y EVIDENCIA ESPERADA

31-60 días | Estructurar

Completar inventario, definir propietarios, formalizar aprobaciones, priorizar activos y diseñar el primer scope PAM.

ACCIONES, RESPONSABLE Y EVIDENCIA ESPERADA

61-90 días | Operar

Implantar o ampliar controles, automatizar rotaciones, registrar sesiones, recertificar accesos y establecer métricas.

ACCIONES, RESPONSABLE Y EVIDENCIA ESPERADA

Prioriza por impacto y exposición, no por facilidad.

La plantilla Excel permite asignar impacto, esfuerzo, propietario, fecha y estado.

Llega al Assessment con mejor contexto

No necesitas tener todas las respuestas. El objetivo es identificar qué sabemos, qué debemos verificar y dónde empezar.

Antes de la sesión

- ☐ Define un scope inicial: activos, entorno, proveedor o caso de uso.
- ☐ Invita a Seguridad y al responsable técnico del scope.
- ☐ Reúne el inventario disponible, aunque esté incompleto.
- ☐ Localiza políticas, revisiones, tickets, logs o capturas relevantes.
- ☐ Selecciona dos o tres situaciones reales de acceso privilegiado.
- ☐ Anota las decisiones que necesitas poder tomar al terminar.

Pregunta de decisión

¿Qué acceso te resultaría más difícil reconstruir y demostrar hoy ante una investigación o auditoría?

PRIVILEGED ACCESS EXPOSURE ASSESSMENT

Convierte señales dispersas en una hoja de ruta.

NexTReT revisa el scope, la calidad de evidencia y las siete dimensiones para construir una lectura ejecutiva y un primer plan de acción.

RESERVA TU ASSESSMENT

Más información: nextret.net

© NexTReT. Documento de trabajo orientativo. No incluyas credenciales ni secretos.