cloudcomputing

Estrategias prácticas, victorias rápidas y ejemplos del mundo real para una Gestión de Acceso Privilegiado (PAM) exitosa.

Cómo Planificar **Para PAM**

Índice

Índice

10

Victorias rápidas para reforzar la implantación de PAM

11

Evaluación y transición de las soluciones PAM

12

Caso práctico - Cómo previene PAM las amenazas internas y externas

13

Conclusión - El futuro de PAM en Ciberseguridad

14

Ponte en contacto

01

¿Por qué este ebook?

Lo que aprenderá

Este libro electrónico ofrece una visión completa de cómo la gestión de acceso privilegiado (PAM) puede proteger los activos más valiosos de su organización, especialmente en el contexto de los entornos de trabajo modernos, como los equipos remotos.

Exploramos cómo PAM no sólo protege contra las amenazas de ciberseguridad, sino que también actúa como un habilitador de negocios, impulsando la eficiencia, la innovación y el cumplimiento. Descubrirá estrategias prácticas para mitigar los riesgos, adaptar PAM al trabajo remoto e implantar la seguridad Zero Trust.

El libro electrónico también aborda los mitos más comunes sobre PAM y proporciona pasos prácticos para crear una estrategia PAM sólida, donde se incluyen los logros rápidos para fortalecer su postura de seguridad.

Tanto si se trata de una pequeña como de una gran empresa, esta guía le proporcionará los conocimientos necesarios para mejorar la ciberseguridad de su organización y proteger sus activos más valiosos.

Sobre el autor

cloudcomputing

Este libro ha sido elaborado por el equipo de Cloudcomputing.

Con 14 años de experiencia guiando a las organizaciones a través de complejos viajes de identidad, Cloudcomputing se ha establecido como una autoridad en ciberseguridad y en asegurar la fuerza más fundamental en los negocios: la confianza.

Aportamos valor tangible a través de la Identidad Moderna, la Movilidad y la Seguridad, y la Consultoría Cibernética, abordando los desafíos únicos a los que se enfrentan las organizaciones de diversos sectores.

Identidad moderna

Más que seguridad, nuestro enfoque proporciona una ventaja estratégica. No solo protege los activos clave y salvaguarda a las partes interesadas, sino que también agiliza el acceso, fomenta el cumplimiento normativo e impulsa la transformación digital.

Movilidad y seguridad

A medida que aumenta la movilidad en las operaciones empresariales, también lo hacen los retos de gestionar las identidades y el acceso en entornos móviles.
Ayudamos a las organizaciones a implantar estrategias, tecnologías y políticas para proteger dispositivos, aplicaciones y datos, garantizando la seguridad, la conformidad y la productividad.

Consultoría en ciberseguridad

Nuestros consultores aportan una gran experiencia y conocimiento del sector. Nuestro enfoque de la consultoría en ciberseguridad va más allá de los métodos tradicionales, incorporando tecnologías de vanguardia y las mejores prácticas para hacer frente a la evolución del panorama. Esta postura proactiva ayuda a las organizaciones a mantenerse a la vanguardia.

Gestión de acceso privilegiado

Como socio certificado de Delinea, Cloudcomputing implementa soluciones PAM preparadas para la nube y de nivel empresarial que sitúan el acceso privilegiado en el centro de las estrategias de ciberseguridad.

02

Introducción a la Gestión de Acceso Privilegiado (PAM)

¿Qué es la Gestión de Acceso Privilegiado (PAM)?

La Gestión de Acceso Privilegiado (PAM) es una práctica crítica de ciberseguridad diseñada para gestionar, supervisar y asegurar el acceso a los sistemas y datos más sensibles de una organización.

Las cuentas privilegiadas, que tienen derechos de acceso elevados, controlan funciones esenciales dentro de la infraestructura informática.

Estas cuentas incluyen usuarios administrativos, cuentas de servicio y administradores del sistema que pueden realizar acciones críticas como cambiar la configuración del sistema o acceder a datos confidenciales..

Sin una gestión adecuada, estas cuentas plantean riesgos significativos, incluido el potencial de uso indebido interno o de ciberataques externos.

PAM ayuda a mitigar estos riesgos aplicando controles estrictos, auditando el acceso y garantizando que sólo las personas o servicios autorizados tengan acceso privilegiado cuando sea necesario.

Por qué es importante la PAM en el panorama actual de la ciberseguridad

El entorno de la ciberseguridad es más complejo y hostil que nunca. Los ciberdelincuentes tienen como objetivo las cuentas privilegiadas por el alto nivel de acceso que proporcionan.

Una sola cuenta privilegiada comprometida puede dar lugar a infracciones devastadoras, pérdidas financieras y daños a la reputación.

En este contexto, el PAM ya no es sólo una medida de ciberseguridad, sino una herramienta empresarial estratégica que favorece la eficacia operativa, el cumplimiento de la normativa y la innovación.

Al salvaguardar las cuentas privilegiadas, PAM ayuda a las organizaciones a reducir el riesgo, mantener la confianza con las partes interesadas y adoptar con confianza la transformación digital.

Razones clave por las que el PAM es esencial:

- **Protege los activos críticos**

  Las cuentas con privilegios controlan el acceso a los sistemas y datos más sensibles.

- **Reduce el riesgo de amenazas internas**

  Una supervisión adecuada de las cuentas privilegiadas minimiza el riesgo de uso indebido interno.

- **Defiende contra ciberataques externos**

  PAM implementa fuertes medidas de seguridad como la autenticación multifactor y el acceso con mínimos privilegios para evitar accesos no autorizados.

- **Respalda el cumplimiento de la normativa**

  Muchas normativas, como GDPR e HIPAA, exigen estrictos controles de acceso para los datos sensibles.

Principales ventajas de PAM para las empresas

Mientras que la ciberseguridad se considera a menudo una práctica defensiva, **el PAM actúa como facilitador del negocio**, ayudando a las organizaciones a alcanzar sus objetivos estratégicos. Cómo lo hace:

1. **Aceleración de la transformación digital**
   PAM garantiza un acceso seguro a las nuevas herramientas digitales, lo que facilita a las empresas la integración de tecnologías modernas y el mantenimiento de la competitividad.

2. **Mejora de la eficiencia operativa**
   La automatización de los controles de acceso mediante PAM reduce la carga manual de los equipos de TI, disminuye los errores humanos y libera recursos para tareas más estratégicas.

3. **Mejora de la agilidad y la innovación**
   Con un acceso seguro a los sistemas, los equipos pueden innovar sin comprometer la seguridad, lo que hace que la organización sea más ágil y reaccione mejor a los cambios.

4. **Apoyo al cumplimiento y la gobernanza**
   PAM proporciona registros de auditoría detallados que garantizan que las empresas cumplen las normativas del sector y las normas de cumplimiento.

5. **Reducción de los costes del seguro de ciberseguridad**
   Una estrategia PAM sólida demuestra la madurez de la ciberseguridad, reduciendo potencialmente las primas de los ciberseguros y contribuyendo a una respuesta más rápida ante incidentes.

Resumen de los puntos clave

- **La Gestión de Acceso Privilegiado (PAM)** es esencial para proteger las cuentas privilegiadas que tienen acceso elevado a sistemas y datos críticos.
- **PAM es más que una medida de ciberseguridad;** actúa como un facilitador de negocios, apoyando la transformación digital, el cumplimiento y la eficiencia operativa.
- **Las cuentas con privilegios son los principales objetivos** tanto de las amenazas internas como de los ciberataques externos, por lo que su protección es crucial.
- **Una estrategia PAM sólida** incluye la aplicación de privilegios mínimos, la implantación de autenticación multifactor y la provisión de registros de auditoría detallados para garantizar la seguridad y el cumplimiento de la normativa.

En el próximo capítulo, exploraremos cómo PAM va más allá de la seguridad, actuando como catalizador del crecimiento empresarial, la eficiencia operativa y la innovación.

03

El papel de PAM como facilitador del negocio

La Gestión de Accesos Privilegiados (PAM) suele considerarse una medida de ciberseguridad, pero tiene un valor mucho más estratégico.

Además de proteger las cuentas confidenciales, PAM puede ser una herramienta empresarial fundamental que impulse el crecimiento, la eficacia y la innovación.

En este capítulo, exploraremos las diversas formas en que PAM ayuda a las organizaciones a alcanzar sus objetivos empresariales.

1. Acelerar la transformación digital

La transformación digital es una prioridad absoluta para las empresas que buscan seguir siendo competitivas en un mundo impulsado por la tecnología.
PAM desempeña un papel fundamental a la hora de garantizar que las organizaciones puedan adoptar nuevas herramientas y plataformas de forma segura, sin poner en peligro los datos confidenciales.

- **Integración segura de nuevas herramientas:** PAM proporciona acceso seguro a nuevas aplicaciones y sistemas, evitando que usuarios no autorizados exploten estas herramientas.
- **Mitigación de riesgos durante la transición:** PAM ayuda a garantizar que las transformaciones digitales - como las migraciones a la nube - sean seguras, reduciendo el riesgo de brechas durante el periodo de transición.
- **Apoyo al trabajo remoto:** A medida que las organizaciones adoptan el trabajo remoto y los entornos basados en la nube, PAM permite el acceso seguro de los empleados que trabajan desde cualquier lugar.

2. Mejorar la eficiencia operativa

PAM automatiza muchos de los procesos implicados en la gestión de accesos privilegiados, reduciendo la carga de trabajo manual de los equipos de TI.
Esto permite a las empresas funcionar con mayor eficacia y al personal informático centrarse en iniciativas estratégicas.

- **Automatización de los controles de acceso:** PAM automatiza el aprovisionamiento y desaprovisionamiento de acceso, minimizando la intervención humana y reduciendo los errores.
- **Reducción de la carga de TI:** Con la gestión automatizada de credenciales, los equipos de TI ya no necesitan rotar manualmente las contraseñas o aprobar las solicitudes de acceso, liberando recursos para otros proyectos.
- **Minimización de los errores humanos:** La automatización también reduce la probabilidad de cometer errores en la gestión de los permisos de acceso, lo que mejora aún más la seguridad y la estabilidad operativa.

3. Mejorar la agilidad y la innovación

La agilidad es clave para seguir siendo competitivos, especialmente en sectores que experimentan rápidos cambios tecnológicos.
PAM dota a las organizaciones de mayor flexibilidad, ya que les permite **ampliar o reducir rápidamente la escala sin perder la seguridad**.

- **Escalado rápido y seguro:** Tanto si se añaden nuevos usuarios, sistemas o dispositivos a la red, PAM permite a las empresas escalar de forma segura.
- **Alentador de la innovación:** Al asegurar el acceso a sistemas experimentales o sensibles, PAM permite a los equipos probar nuevas tecnologías y flujos de trabajo sin exponer a la organización a riesgos innecesarios.
- **Fomento de la colaboración:** El acceso seguro de socios y contratistas externos permite a las organizaciones colaborar de forma más eficaz al tiempo que protegen los activos críticos.

4. Apoyo al cumplimiento y la gobernanza

El cumplimiento de la normativa es una preocupación clave para organizaciones de sectores como las finanzas, la sanidad y la administración pública.
PAM ayuda a cumplir estos requisitos proporcionando un control y supervisión detallados del acceso privilegiado.

- **Registros de Auditoría Detallados:** PAM proporciona una visibilidad completa de quién accedió a qué, cuándo y por qué, lo cual es crucial para cumplir normas de conformidad como GDPR, HIPAA y SOX.
- **Garantizar el Cumplimiento de la Normativa:** Gracias a la estricta aplicación de las políticas de acceso de PAM, las organizaciones pueden demostrar el cumplimiento de los marcos normativos.
- **Refuerzo de la Gobernanza:** PAM apoya la gobernanza garantizando que sólo el personal autorizado tenga acceso a los sistemas sensibles, con aprobaciones y solicitudes de acceso rastreadas y documentadas.

5. Reducir los Costes de los Seguros de Ciberseguridad

Con el creciente coste de los seguros de ciberseguridad, **demostrar madurez en ciberseguridad puede dar lugar a primas reducidas**.
PAM desempeña un papel vital en el fortalecimiento de la postura de seguridad de una organización y puede ayudar a reducir los costes de los seguros.

- **Demostrar la madurez de la seguridad:** PAM muestra a las aseguradoras que una organización ha implementado fuertes controles de acceso, reduciendo la probabilidad de una brecha.
- **Respuesta más rápida ante incidentes:** En caso de infracción, PAM proporciona pruebas forenses cruciales que ayudan a responder con rapidez y eficacia, reduciendo los daños potenciales.
- **Proporcionar pruebas clave para las reclamaciones:** Los registros de acceso detallados y las auditorías generadas por PAM pueden respaldar las reclamaciones de seguros al proporcionar pruebas de los protocolos de seguridad y las mitigaciones aplicadas.

Resumen de los puntos clave

- **PAM es un potente habilitador de negocio,** no solo una medida de ciberseguridad. Ayuda a las organizaciones a navegar con seguridad por la transformación digital, mejorar la eficiencia operativa y fomentar la innovación.
- **La automatización de los controles de acceso** mediante PAM reduce la carga informática y minimiza los errores humanos, liberando recursos para iniciativas estratégicas.
- **PAM mejora la agilidad,** permitiendo a las empresas ampliar o reducir su tamaño de forma segura, al tiempo que favorece la colaboración y la innovación.
- **El cumplimiento de la normativa** se simplifica con los registros de auditoría detallados de PAM y la aplicación estricta de las políticas de acceso.
- **Las organizaciones pueden reducir potencialmente los costes del seguro de ciberseguridad** demostrando su madurez en ciberseguridad a través de PAM, lo que ayuda a mitigar los riesgos y permite una respuesta más rápida a los incidentes.

En el próximo capítulo, profundizaremos en las amenazas de ciberseguridad más comunes que tienen como objetivo las cuentas privilegiadas y cómo una estrategia PAM robusta puede neutralizar estos riesgos.

04

Amenazas de ciberseguridad comunes dirigidas a cuentas con privilegios

Las cuentas con privilegios representan los puntos de acceso más sensibles y potentes dentro de la infraestructura informática de una organización.

Estas cuentas son objetivos frecuentes de los ciberdelincuentes porque pueden abrir la puerta a sistemas y datos críticos.

En este capítulo, exploraremos las amenazas de ciberseguridad más comunes que tienen como objetivo las cuentas privilegiadas y cómo estos riesgos pueden comprometer toda la postura de seguridad de una organización.

1. Compromiso de credenciales

Amenaza: Los atacantes suelen aprovecharse de contraseñas débiles o reutilizadas para obtener acceso no autorizado a cuentas privilegiadas. La vulneración de las credenciales suele lograrse mediante métodos como el phishing, los ataques de fuerza bruta o el relleno de credenciales, en los que se reutilizan contraseñas previamente vulneradas.

Factores clave que contribuyen a la amenaza	Impact	Mitigación sugerida
• Contraseñas débiles o fáciles de adivinar • Reutilización de contraseñas en varias cuentas • Falta de autenticación multifactor (MFA)	• Acceso no autorizado a sistemas críticos • Filtraciones de datos • Escalada de privilegios para obtener un acceso más amplio	→ Imponer **la autenticación multi-factor (MFA)** para todas las cuentas privilegiadas → Implemente **la rotación automática de contraseñas** para actualizar periódicamente las credenciales

2. Acceso no autorizado

Amenaza: Los usuarios no autorizados pueden intentar acceder a cuentas privilegiadas saltándose los controles de acceso.

Essa amenaza suele producirse cuando las prácticas de gestión de accesos son insuficientes, lo que permite a personas acceder a sistemas a los que no deberían.

Factores clave que contribuyen a la amenaza	Impacto	Mitigación sugerida
• Aplicación deficiente del principio del menor privilegio • Cuentas con privilegios excesivos • Controles de acceso inadecuados	• Manipulación no autorizada de datos • Sabotaje del sistema • Acciones internas maliciosas	→ Aplicar **controles de acceso de privilegio mínimo**, garantizando que los usuarios sólo tengan el access mínimo necesario. → Implantar el **aprovisionamiento Just-in-Time (JIT)**, concediendo acceso temporal sólo cuando sea necesario.

3. Movimiento lateral

Amenaza: Después de obtener el acceso inicial, los atacantes intentan el movimiento lateral dentro de la red para comprometer sistemas adicionales. Esta es una táctica común utilizada en las amenazas persistentes avanzadas (APT), donde los atacantes amplían su control y buscan más datos sensibles.

Factores clave que contribuyen a la amenaza	Impacto	Mitigación sugerida
• Deficiente segmentación de la red • Falta de supervisión de las actividades de las cuentas privilegiadas • Cuentas de usuario con privilegios excesivos	• Los atacantes obtienen el control de múltiples sistemas • Mayor dificultad para aislar y responder a las infracciones	→ Implantar **la segmentación de la red** para limitar los movimientos de los atacantes. → Realizar **una supervisión continua** de las cuentas privilegiadas para detectar actividades sospechosas.

4. Escalada de privilegios

Amenaza: La escalada de privilegios se produce cuando los atacantes aprovechan vulnerabilidades o configuraciones erróneas para elevar sus permisos de una cuenta de usuario normal a una cuenta administrativa o privilegiada. Esto les da un mayor control sobre los sistemas críticos.

Factores clave que contribuyen a la amenaza	Impacto	Mitigación sugerida
• Privilegios mal configurados • Vulnerabilidades sin parchear • Control deficiente de los cambios de privilegios	• Los atacantes obtienen el control total de los sistemas clave • Los datos y configuraciones críticos están expuestos	→ **Limitar los derechos administrativos** sólo a los usuarios esenciales → **Auditar y revisar** periódicamente los **cambios de privilegios**

5. Ataques de *phishing* selectivo

Amenaza: Los atacantes diseñan sofisticadas campañas de phishing dirigidas a usuarios privilegiados para robar sus credenciales. Estos ataques de phishing suelen imitar fuentes de confianza, lo que facilita que los usuarios compartan involuntariamente su información de inicio de sesión.

Factores clave que contribuyen a la amenaza	Impacto	Mitigación sugerida
• Falta de concienciación de los usuarios en materia de seguridad • Dependencia excesiva de la autenticación de un solo factor • Mecanismos de detección de phishing deficientes	• Compromiso de cuentas privilegiadas • Acceso no autorizado a sistemas sensibles • Robo o destrucción de datos	→ Impartir **formación sobre seguridad** a todos los usuarios, especialmente a los privilegiados. → Implantar **soluciones avanzadas de protección contra el phishing** (por ejemplo, filtrado de correo electrónico, escaneado de enlaces).

6. Explotación de vulnerabilidades

Amenaza: Los atacantes suelen explotar vulnerabilidades de software no parcheadas para obtener acceso privilegiado a los sistemas. Estas vulnerabilidades pueden existir en aplicaciones, sistemas operativos o dispositivos de red, lo que proporciona a los atacantes una forma de eludir las medidas de seguridad normales.

Factores clave que contribuyen a la amenaza	Impacto	Mitigación sugerida
• Retraso en las actualizaciones y los parches de *software* • Sistemas heredados inseguros • Falta de procesos de gestión de vulnerabilidades	• Compromiso total del sistema • Ejecución remota de código con privilegios administrativos	→ Implantar **procesos regulares de gestión de parches** para mantener los sistemas actualizados. → **Exploración de vulnerabilidades** para identificar y corregir las deficiencias de seguridad.

7. Ataques internos

Amenaza: Los intrusos con acceso legítimo a cuentas privilegiadas pueden abusar de su acceso con fines maliciosos, ya sea en beneficio propio o por coacción. Las amenazas internas son de las más difíciles de detectar porque el individuo ya goza de confianza dentro del sistema.

Factores clave que contribuyen a la amenaza	Impacto	Mitigación sugerida
• Falta de supervisión de las actividades privilegiadas • No hay separación de funciones • Registro y auditoría insuficientes	• Robo, destrucción o manipulación de datos • Pérdidas financieras • Daños a la reputación	→ **Segregación de funciones** para garantizar que ningún usuario tenga control sobre los procesos críticos. → Implantar **auditorías y registros continuos** de las actividades privilegiadas.

8. Cuentas de servicio no gestionadas

Amenaza: Las cuentas de servicio suelen pasarse por alto, a pesar de tener privilegios elevados. Estas cuentas, que se utilizan para ejecutar aplicaciones y procesos, pueden convertirse en un riesgo importante si no se gestionan o supervisan.

Factores clave que contribuyen a la amenaza	Impacto	Mitigación sugerida
• Falta de visibilidad de las cuentas de servicio • Falta de rotación o seguridad de las credenciales de las cuentas de servicio • Cuentas de servicio con privilegios excesivos	• Los atacantes obtienen el control de las funciones críticas del sistema • Manipulación o destrucción de datos	→ **Descubrir y gestionar de forma centralizada las cuentas de servicio.** → **Rote** periódicamente **las credenciales de las cuentas de servicio** y aplique estrictos controles de acceso.

Resumen de los puntos clave

- **Compromiso de credenciales**: PAM evita el robo de credenciales mediante la aplicación de MFA y la rotación periódica de contraseñas.
- **Acceso no autorizado**: El acceso con mínimos privilegios y el aprovisionamiento JIT limitan la exposición a usuarios no autorizados.
- **Movimiento lateral**: La segmentación de la red y la supervisión continua impiden que los atacantes se propaguen por los sistemas.
- **Escalada de privilegios**: Los estrictos controles de privilegios y las auditorías periódicas impiden a los atacantes elevar sus permisos.
- ***Phishing* selectivo**: la formación en materia de seguridad y las defensas avanzadas contra el *phishing* protegen a los usuarios con privilegios del robo de credenciales.
- **Explotación de vulnerabilidades**: La aplicación periódica de parches y la exploración de vulnerabilidades cierran brechas que los atacantes pueden aprovechar para obtener acceso privilegiado.
- **Ataques internos**: La segregación de funciones y el registro de actividades ayudan a detectar y mitigar las actividades internas maliciosas.
- **Cuentas de servicio no gestionadas**: Una gestión adecuada de las cuentas de servicio garantiza que estas cuentas, a menudo olvidadas, no se conviertan en vectores de ataque.

A continuación, profundizaremos en **cómo PAM mitiga estos riesgos para las cuentas privilegiadas** y garantiza un entorno seguro.

05

Cómo PAM mitiga los riesgos de las cuentas con privilegios

La gestión de accesos privilegiados (PAM) desempeña un papel crucial en la protección de las organizaciones frente a las ciberamenazas dirigidas a las cuentas privilegiadas.

Mediante la aplicación de estrategias eficaces, PAM mitiga los riesgos asociados con el acceso no autorizado, el compromiso de credenciales y las amenazas internas.

Este capítulo explora los métodos clave que emplea PAM para asegurar el acceso privilegiado.

1. Aplicación de los Privilegios Mínimos y Aprovisionamiento *Just-in-Time*

Control de acceso de mínimo privilegio

- Garantiza que los usuarios tengan sólo los permisos mínimos necesarios para realizar sus tareas
- Reduce el riesgo de uso accidental o malintencionado de privilegios

Aprovisionamiento *Just-in-Time* (JIT)

- Concede acceso privilegiado sólo cuando es necesario y lo revoca inmediatamente después de su uso.
- Limita el plazo durante el cual se pueden explotar las credenciales.

2. Control y Auditoría Continuos

Supervisión en tiempo real

- Rastrea continuamente las actividades de los usuarios en cuentas privilegiadas para identificar comportamientos sospechosos
- Alerta a los equipos de seguridad de cualquier anomalía para su investigación inmediata

Capacidades de auditoría

- Mantiene registros detallados de todas las actividades de acceso privilegiado, apoyando el cumplimiento y las investigaciones forenses.
- Las auditorías periódicas ayudan a las organizaciones a garantizar el cumplimiento de las políticas de seguridad y a identificar áreas de mejora.

3. Autenticación Multifactor (MFA)

Capa de seguridad mejorada

- Requiere que los usuarios proporcionen múltiples formas de verificación antes de acceder a cuentas privilegiadas.
- Reduce significativamente el riesgo de acceso no autorizado, incluso si las credenciales están en peligro.

Métodos de autenticación flexibles

- Admite varias opciones de MFA, que incluyen biométrica, tokens y verificación por SMS.
- Puede adaptarse a las necesidades de la organización para mejorar la experiencia del usuario.

4. Rotación automática de credenciales y gestión de contraseñas

Rotación regular de credenciales

- Automatiza el proceso de cambio de contraseñas de las cuentas privilegiadas a intervalos regulares.
- Reduce la probabilidad de que las credenciales se vean comprometidas al minimizar la ventana de exposición.

Gestión segura de contraseñas

- Aplica políticas de contraseñas seguras, incluidos requisitos de complejidad y contraseñas únicas para cada cuenta.
- Utiliza bóvedas seguras para almacenar y gestionar las contraseñas, impidiendo el acceso no autorizado.

Resumen de los puntos clave

- PAM mitiga los riesgos de las cuentas privilegiadas mediante el **acceso con menos privilegios** y estrategias de **aprovisionamiento *Just-In-Time***.
- **La supervisión y auditoría continuas** ayudan a identificar actividades sospechosas y a garantizar el cumplimiento de la normativa.
- **La autenticación multifactor (MFA)** añade una capa crítica de seguridad contra el acceso no autorizado.
- **La rotación automatizada de credenciales y la gestión de contraseñas** reducen la exposición y mejoran la seguridad general.

En el próximo capítulo, vamos a explorar **la relación crítica** entre la Gestión de Acceso Privilegiado (PAM) y la Arquitectura Zero Trust (ZTA).

06

PAM y Arquitectura Zero Trust

A medida que evolucionan las amenazas a la ciberseguridad, los modelos tradicionales de seguridad de redes que asumen que todo dentro de la red es de confianza ya no son suficientes.

Este cambio ha llevado al auge de la **Arquitectura Zero Trust (ZTA)**, que adopta el enfoque de "nunca confíes, siempre verifica".

La gestión de accesos privilegiados (PAM) es un componente crítico de cualquier estrategia de Zero Trus, ya que **garantiza la gestión y el control seguros de los accesos privilegiados, que suelen ser el objetivo principal de los ciberataques.**

En este capítulo, exploraremos cómo PAM soporta y habilita los principios Zero Trust para mejorar la seguridad en toda la red.

¿Qué es la Arquitectura Zero Trust?

La Arquitectura Zero Trust (ZTA) es un marco de seguridad que asume que ninguna entidad, ya sea dentro o fuera de la red, es de confianza automática. Cada solicitud de acceso debe ser autenticada, autorizada y validada continuamente en función de niveles de riesgo dinámicos.

- **"Nunca confíes, verifica siempre"**
  Todas las solicitudes de acceso se autentican continuamente, independientemente de su origen.
- **Microsegmentación**
  Las redes se dividen en zonas más pequeñas para minimizar el movimiento lateral.
- **Acceso con mínimos privilegios**
  Los usuarios y sistemas sólo reciben el acceso mínimo necesario durante el menor tiempo posible.
- **Supervisión continua**
  El acceso y las actividades se supervisan continuamente para identificar cualquier comportamiento inusual.

El papel de PAM en la Arquitectura Zero Trust

PAM desempeña un papel clave en la aplicación de los principios Zero Trust, en particular cuando se trata de proteger las cuentas privilegiadas.

Los usuarios con privilegios, como los administradores, tienen acceso a sistemas críticos, lo que los convierte en objetivos de gran valor para los atacantes.

Así es como PAM apoya el Zero Trust.

1. Aplicación del acceso con privilegios mínimos

Uno de los principales pilares de Zero Trust es el Acceso con Mínimos Privilegios, lo que significa que los usuarios deben tener sólo los permisos mínimos necesarios para completar sus tareas.

PAM se encarga de ello gestionando y controlando las cuentas privilegiadas de forma que se reduzca el riesgo de uso indebido.

- **Control de acceso granular**: PAM garantiza que el acceso esté limitado a sistemas, datos o recursos específicos en función del rol del usuario.
- **Control de acceso basado en roles (RBAC)**: A los usuarios se les asignan funciones específicas con derechos de acceso predefinidos, lo que garantiza que nadie tenga privilegios excesivos.
- **Acceso limitado en el tiempo**: La provisión *Just-In-Time* (JIT) garantiza que el acceso se conceda sólo cuando sea necesario y por una duración limitada.

---

2. Autenticación y autorización continuas

En Zero Trust, **la autenticación y la autorización** no son eventos puntuales, sino procesos continuos.

PAM apoya esto verificando continuamente la identidad del usuario y los permisos de acceso durante toda la sesión.

- **Autenticación multifactor (MFA)**: PAM aplica la MFA a los usuarios con privilegios, exigiendo múltiples formas de verificación de identidad.
- **Supervisión continua de las sesiones**: Las sesiones con privilegios se supervisan activamente, y cualquier comportamiento inusual o de riesgo se marca para su revisión.
- **Controles de acceso dinámicos**: Los privilegios de acceso pueden ajustarse en tiempo real en función de factores de riesgo como la ubicación, el dispositivo o el comportamiento del usuario.

---

3. Provisión de acceso *Just-in-Time* (JIT)

El aprovisionamiento Just-in-Time (JIT) es una característica crítica tanto en PAM como en Zero Trust.

Al conceder **acceso sólo cuando es necesario** y revocarlo automáticamente después de su uso, PAM reduce significativamente la superficie de ataque.

- **Acceso privilegiado temporal**: PAM permite conceder acceso privilegiado sólo durante la duración de una tarea específica, después de lo cual se revoca.
- **Reduce el tiempo de exposición**: Al minimizar el tiempo que un usuario tiene acceso privilegiado, PAM limita la ventana de oportunidad para un ataque.
- **Revocación automática de acceso:** Una vez finalizada la tarea, PAM revoca automáticamente los privilegios sin necesidad de intervención manual.

---

4. Control y auditoría continuos

En un entorno de Zero Trust, **la supervisión y auditoría continuas** de las cuentas y actividades privilegiadas son esenciales.

PAM proporciona información detallada sobre quién ha accedido a qué, cuándo y cómo, lo que permite a las organizaciones mantener una visibilidad total.

- **Grabación y auditoría de sesiones**: PAM registra todas las sesiones privilegiadas, lo que facilita la revisión de las actividades para el cumplimiento y la seguridad.
- **Alertas en tiempo real**: PAM proporciona alertas inmediatas ante cualquier actividad sospechosa, como intentos de acceso no autorizados o comportamientos inusuales durante una sesión privilegiada.
- **Informes exhaustivos**: PAM genera registros e informes de auditoría detallados, garantizando que todas las actividades privilegiadas están bien documentadas para el cumplimiento de normativas y los análisis forenses.

Cómo Soporta PAM la Autenticación y Autorización Continuas

En un entorno de Zero Trust, la **autenticación y autorización continuas** significan que la identidad del usuario se verifica durante toda la sesión, no sólo al iniciar sesión. Esto es crucial para detectar y responder a actividades sospechosas en tiempo real.

- **Autenticación adaptativa**
  Las soluciones PAM ajustan los requisitos de autenticación en función del contexto, como la ubicación, el dispositivo o el nivel de riesgo.
- **Tiempo de espera de sesión y re-autenticación**
  PAM puede pedir a los usuarios que vuelvan a autenticarse si su sesión se queda inactiva o si detecta un comportamiento arriesgado.
- **Aislamiento de sesiones**
  PAM aísla las sesiones privilegiadas del resto de la red, evitando el movimiento lateral si se produce un acceso no autorizado.

Alcanzar Plenamente el Zero Trust con PAM

Lograr **plenamente el Zero Trust** requiere implantar controles y procesos que verifiquen continuamente el acceso de los usuarios, supervisen la actividad y restrinjan los permisos.

PAM desempeña un papel fundamental en este sentido:

- **Eliminación de la confianza implícita**: PAM aplica el principio de "nunca confíes, siempre verifica", incluso para los usuarios que ya están dentro de la red.
- **Control de acceso dinámico**: PAM ajusta dinámicamente los privilegios de los usuarios en función del análisis contextual de riesgos, evitando la escalada de accesos.
- **Integración con otras herramientas de seguridad**: PAM se integra con soluciones de seguridad como los sistemas SIEM (Security Information and Event Management) y las herramientas de detección de amenazas, garantizando una visibilidad total de la seguridad.
- **Mitigación proactiva de riesgos**: Con funciones como el acceso JIT, la supervisión continua y MFA, PAM mitiga activamente los riesgos y apoya los principios de Zero Trust.

Ventajas de Integrar PAM con la Arquitectura Zero Trust

Al integrar PAM en una estrategia de Zero Trust, las organizaciones pueden mejorar significativamente su postura de seguridad y proteger mejor sus cuentas privilegiadas y sistemas críticos.

- **Postura de seguridad mejorada**: PAM garantiza que incluso si un atacante consigue acceder a la red, no podrá explotar las cuentas privilegiadas.
- **Superficie de ataque minimizada**: El acceso JIT y las políticas de mínimos privilegios reducen los posibles puntos de entrada de los atacantes.
- **Cumplimiento mejorado**: La supervisión continua, la grabación de sesiones y la auditoría ayudan a cumplir los requisitos normativos y de conformidad.
- **Respuesta más rápida ante incidentes**: Las alertas en tiempo real y la supervisión de sesiones permiten detectar y responder rápidamente a las amenazas, minimizando los daños potenciales.

Resumen de los puntos clave

- **La Arquitectura Zero Trust (ZTA)** se basa en el principio de "nunca confíes, siempre verifica", que exige autenticación y autorización constantes.
- **PAM apoya el Zero Trust** al imponer el acceso de mínimo privilegio, autenticar continuamente a los usuarios, proporcionar acceso JIT y supervisar todas las actividades privilegiadas.
- **La autenticación multifactor (MFA)** y el **control de acceso basado en roles (RBAC)** son funciones clave de PAM que se ajustan a los principios zero trust.
- **La supervisión y auditoría continuas** garantizan que las cuentas con privilegios se controlan adecuadamente y se protegen de las amenazas internas y externas.
- La integración de PAM con Zero Trust mejora la seguridad, minimiza la superficie de ataque y proporciona una mayor visibilidad de las actividades privilegiadas.

En el próximo capítulo, vamos a explorar cómo PAM está evolucionando para afrontar los retos del **trabajo remoto**, garantizando el acceso seguro y la protección de las cuentas privilegiadas en un entorno de trabajo distribuido.

07

Adaptar PAM a la Era del Trabajo a Distancia

Adaptar las estrategias de PAM al trabajo remoto implica abordar superficies de ataque ampliadas, gestionar TI sombra, proteger los dispositivos y mitigar las amenazas internas.

Mediante la implantación de soluciones como la MFA, el acceso JIT, la seguridad de los terminales, la supervisión continua y la formación de los empleados, las organizaciones pueden proteger eficazmente el acceso privilegiado en un entorno de trabajo remoto.

En este capítulo, exploraremos cómo el cambio al trabajo remoto ha cambiado el panorama de la ciberseguridad e introducido nuevos retos en la seguridad de los accesos privilegiados.

Principales retos a la hora de proteger el acceso privilegiado de equipos remotos

El cambio al trabajo remoto ha introducido varios retos para asegurar el acceso privilegiado. Afrontar estos retos es crucial para mantener una ciberseguridad sólida.

Estos son los principales retos a los que se enfrentan las organizaciones:

1. Superficie de ataque ampliada

Aumento de los puntos de entrada	Más puntos finales significan una mayor superficie de ataque, lo que dificulta la protección de todos los puntos de acceso.
Entornos de red diversos	El trabajo remoto implica condiciones de red y posturas de seguridad variables, lo que complica el control de acceso.

2. TI sombra

Herramientas no autorizadas	Los empleados pueden utilizar herramientas y aplicaciones no autorizadas, saltándose los protocolos de seguridad oficiales.
Falta de visibilidad	La dificultad para supervisar y controlar el software no autorizado aumenta los riesgos de seguridad.

3. Falta de seguridad física

Vulnerabilidad de los dispositivos	Los dispositivos remotos son más propensos al robo o al acceso no autorizado en comparación con los entornos de oficina seguros.
Protección de datos	Garantizar la protección de los datos cuando se accede a ellos desde ubicaciones menos seguras es todo un reto.

4. Amenazas internas

Reducción de la supervisión	Con menos supervisión directa, aumenta el riesgo de amenazas internas o de uso indebido de accesos privilegiados.
Supervisión del comportamiento	La visibilidad limitada de las actividades de los empleados puede dificultar la detección y respuesta a comportamientos maliciosos.

Soluciones probadas para la implantación remota de PAM

Para hacer frente a los retos que plantea el trabajo remoto, las organizaciones necesitan implantar soluciones eficaces para la Gestión de Acceso Privilegiado (PAM). Aquí tiene algunas estrategias probadas para mejorar el PAM de los equipos remotos:

Solución	Acción
Implantar la autenticación multifactor (MFA)	Exigir MFA para todas las cuentas privilegiadas para añadir una capa adicional de seguridad y dificultar el acceso no autorizado.
Aprovisionamiento *Just-in-Time* (JIT)	Conceda acceso privilegiado sólo cuando sea necesario y revóquelo inmediatamente después de su uso. Así se limita el riesgo de uso no autorizado fuera del horario laboral.
Aplique la seguridad de los puntos finales	Asegúrese de que todos los dispositivos remotos cumplen las normas de seguridad antes de concederles acceso. Esto incluye software antivirus y parches de seguridad actualizados.
Supervisar y auditar el acceso remoto	Rastree y audite continuamente el acceso remoto privilegiado para detectar y responder rápidamente a las amenazas potenciales.
Educar a los trabajadores	Impartir formación sobre los riesgos del trabajo a distancia y las mejores prácticas de seguridad para garantizar que los empleados son conscientes de las posibles amenazas y de cómo mitigarlas.

La Importancia de la Seguridad de los Terminales y la Supervisión del Acceso Remoto

A medida que el trabajo remoto se convierte en la norma, la seguridad de los terminales y la supervisión del acceso remoto se han convertido en componentes cruciales de una sólida estrategia de gestión de acceso privilegiado (PAM).

A continuación se explica por qué estos aspectos son vitales y cómo contribuyen a la ciberseguridad general.

Seguridad de terminales: La primera línea de defensa

La seguridad de los terminales se refiere a la protección de los dispositivos de los usuarios finales, como portátiles, ordenadores de sobremesa, teléfonos inteligentes y tablets, que se conectan a la red de su organización.

Estos dispositivos suelen ser los puntos de entrada de las ciberamenazas, por lo que su seguridad es primordial.

Por qué es importante la seguridad de los terminales

- **Reducción de la vulnerabilidad:** Los dispositivos remotos suelen estar expuestos a diversas amenazas, como *malware*, ataques de *phishing* y accesos no autorizados. Garantizar la seguridad de estos dispositivos reduce el riesgo de que se vean comprometidos y utilizados como puntos de entrada para ataques.
- **Cumplimiento y control**: Muchas normas reglamentarias exigen que las organizaciones apliquen medidas de seguridad en los terminales. El cumplimiento de estas normas es esencial para evitar problemas legales y mantener la confianza.
- **Protección contra el robo de datos**: La seguridad de los puestos finales ayuda a proteger los datos confidenciales frente al acceso o el robo por parte de personas no autorizadas, especialmente cuando los empleados trabajan desde distintas ubicaciones.

Componentes clave de la seguridad de los puntos finales

- **Antivirus y Antimalware**: Instale y actualice regularmente *software* antivirus para detectar y neutralizar amenazas maliciosas.
- **Cifrado**: Cifre los datos en los puntos finales para garantizar que, aunque se pierda o roben un dispositivo, los datos permanezcan protegidos.
- **Gestión de parches:** Actualice y parche periódicamente los sistemas operativos y las aplicaciones para solucionar vulnerabilidades y fallos de seguridad.
- **Controles de acceso**: Implanta métodos de autentic ación fuertes y restringe el acceso a datos sensibles en función de las funciones y necesidades de los usuarios.

Supervisión del acceso remoto: Visibilidad y respuesta

La supervisión del acceso remoto implica el seguimiento y análisis de las actividades realizadas por los usuarios que acceden a la red de la organización de forma remota. Una supervisión eficaz ayuda a detectar, investigar y responder a posibles incidentes de seguridad.

Por qué es crucial supervisar el acceso remoto

- **Detección temprana de amenazas**: La supervisión continua permite detectar en tiempo real actividades sospechosas o anomalías, que pueden indicar una brecha de seguridad o un acceso no autorizado.
- **Respuesta a incidentes: La rápida identificación de incidentes de seguridad permite una respuesta rápida, minimizando los daños potenciales y reduciendo el tiempo de recuperación.**
- **Cumplimiento y auditoría**: La supervisión y el registro periódicos de las actividades de acceso remoto garantizan que las organizaciones cumplan los requisitos normativos y pueden proporcionar informes detallados para las auditorías.

Aspectos clave de la supervisión del acceso remoto

- **Alertas en tiempo real**: Configura alertas para actividades inusuales, como intentos de acceso fuera del horario normal o desde lugares desconocidos.
- **Grabación de sesiones**: Grabe las sesiones de acceso remoto para revisar y analizar las acciones de los usuarios, garantizando el cumplimiento de la normativa e investigando incidentes si necesario.
- **Registro de actividades**: Mantenga registros completos de todas las actividades de acceso remoto, incluidos los intentos de inicio de sesión, el acceso a archivos y los cambios realizados, para respaldar las investigaciones forenses y las comprobaciones de cumplimiento.
- **Análisis del comportamiento**: Utilice análisis de comportamiento para detectar desviaciones del comportamiento normal de los usuarios, lo que puede ayudar a identificar cuentas comprometidas o amenazas internas.

Resumen de los puntos clave

En este capítulo, hemos explorado cómo adaptar las estrategias de Gestión de Acceso Privilegiado (PAM) para hacer frente a los desafíos únicos que plantea el entorno de trabajo remoto:

- **Superficie de ataque ampliada:** Más puntos finales aumentan la complejidad de la seguridad.
- **TI Sombra:** las herramientas no autorizadas pueden eludir los controles de seguridad.
- **Seguridad física:** Los dispositivos remotos son más vulnerables.
- **Amenazas internas:** La reducción de la supervisión aumenta el riesgo.

Al abordar estos retos con las soluciones propuestas, las organizaciones pueden gestionar eficazmente el acceso privilegiado en un entorno de trabajo remoto, garantizando tanto la seguridad como la productividad.

- **MFA**: Añade seguridad adicional a las cuentas privilegiadas.
- **Acceso JIT**: Limita el acceso sólo a los momentos necesarios.
- **Seguridad para puntos finales**: Protege los dispositivos con antivirus y cifrado.
- **Supervisión**: Rastrea y audita las actividades de acceso remoto.
- **Formación**: Educa a los empleados en las mejores prácticas de seguridad.

Proteger los dispositivos que se conectan a la red de la organización es crucial para prevenir las ciberamenazas, garantizar el cumplimiento de la normativa y salvaguardar los datos. Las medidas clave incluyen software antivirus, cifrado, gestión de parches y controles de acceso. La supervisión eficaz del acceso remoto es vital para la detección temprana de amenazas, la respuesta a incidentes y el cumplimiento de las normativas. Las prácticas esenciales incluyen alertas en tiempo real, grabación de sesiones, registro de actividades y análisis de comportamiento.

En el próximo capítulo, clarificamos mitos y conceptos erróneos sobre PAM, proporcionando claridad sobre su papel e implementación.

08

Mitos sobre PAM

La gestión de acceso privilegiado (PAM) es un componente crucial de las estrategias modernas de ciberseguridad, pero **hay varios conceptos erróneos que impiden a las organizaciones aprovechar plenamente su potencial.**

En este capítulo, desmontamos los mitos más comunes en torno a PAM, explicaremos la realidad detrás de estos conceptos erróneos y destacaremos los beneficios de una estrategia PAM bien implementada.

Mito 1

PAM es sólo para grandes empresas

La realidad: Aunque las soluciones PAM se asocian a menudo con las grandes organizaciones, este mito pasa por alto la creciente necesidad de las pequeñas y medianas empresas (PYMES) de proteger sus datos críticos. Las ciberamenazas se dirigen a empresas de todos los tamaños, y los atacantes suelen buscar organizaciones más pequeñas con menos recursos de seguridad.

Puntos clave

Las PYME son tan vulnerables a los ciberataques como las grandes empresas.	Las soluciones PAM pueden ser escalables y adaptarse a las necesidades de las organizaciones más pequeñas.	Las rentables herramientas PAM basadas en la nube la hacen accesible para empresas con presupuestos limitados.

Mito 2

La implantación de PAM es demasiado compleja

La realidad: La implantación de PAM puede parecer desalentadora, pero las soluciones PAM modernas están diseñadas pensando en la facilidad de uso y despliegue. Estas soluciones suelen ofrecer directivas preconfiguradas, plantillas y funciones de automatización que facilitan el proceso y reducen el consumo de recursos.

Puntos clave

Las plataformas PAM modernas son fáciles de usar y ofrecen implantaciones guiadas.

La automatización y las plantillas preconfiguradas reducen la necesidad de configuraciones manuales.

Muchos proveedores ofrecen asistencia al cliente y formación para simplificar el proceso de implantación.

Mito 3

PAM reduce la productividad al restringir el acceso

La realidad: Aunque PAM impone controles de acceso más estrictos, en realidad puede mejorar la productividad al agilizar la gestión de accesos. Con PAM, los usuarios pueden acceder a los recursos que necesitan de forma más rápida y segura, sin comprometer la seguridad de la organización.

Puntos clave

PAM automatiza los controles de acceso, reduciendo la carga de los equipos informáticos.

El acceso Just-in-Time (JIT) garantiza que los usuarios sólo tengan privilegios cuando sea necesario.

La autenticación multifactor (MFA) mejora la seguridad sin añadir fricciones significativas a la experiencia del usuario.

Mito 4

PAM sólo es necesario para los administradores de TI

La realidad: Aunque PAM es fundamental para los administradores de TI que gestionan cuentas privilegiadas, también se aplica a una amplia gama de roles y funciones dentro de una organización. Cualquier empleado, contratista o usuario externo con acceso elevado supone un riesgo potencial si no se gestiona adecuadamente.

Puntos clave

PAM se extiende a ejecutivos, proveedores externos y entornos en la nube.	Las cuentas de servicio y las entidades no humanas también requieren una gestión de acceso privilegiada.	Las amenazas internas son una preocupación importante, y PAM ayuda a mitigar este riesgo en varios tipos de usuarios.

Mito 5

PAM por sí solo puede proteger todas las cuentas con privilegios

La realidad: PAM es una parte esencial de una estrategia de seguridad más amplia, pero no se debe confiar en ella como único mecanismo de defensa. Funciona mejor cuando se integra con otras medidas de seguridad como la segmentación de la red, la protección de puntos finales y la Arquitectura Zero Trust.

Puntos clave

PAM refuerza la seguridad, pero debe combinarse con otras herramientas de ciberseguridad.

Los principios de Zero Trust, la supervisión de la red y las auditorías periódicas complementan a PAM para ofrecer una defensa integral.

Los programas continuos de formación y concienciación sobre seguridad son necesarios para garantizar que todos los empleados entienden y siguen las mejores prácticas.

Resumen de los puntos clave

- **La implantación de PAM no tiene por qué ser compleja**: las herramientas modernas ofrecen automatización y configuraciones simplificadas, lo que facilita su despliegue.
- **PAM mejora la productividad**: gracias a funciones como el aprovisionamiento Just-in-Time y MFA, agiliza los flujos de trabajo y mejora la seguridad.
- **PAM no sólo se aplica a los administradores de TI**, sino también a una gran variedad de usuarios, como ejecutivos, proveedores externos y cuentas de servicio.
    - **PAM debe formar parte de una estrategia de seguridad global**: funciona mejor cuando se integra con otras herramientas y prácticas, como el Zero Trust y la protección de puntos finales.

A continuación, nos adentraremos en "**Creación de una estrategia integral de PAM: Una lista de comprobación práctica**", donde describiremos los pasos clave para desarrollar un sólido enfoque de PAM adaptado a las necesidades de su organización.

09

Creación de una Estrategia Global de PAM

Lista de Comprobación Práctica

Una estrategia sólida de Gestión de Acceso Privilegiado (PAM) es esencial para proteger los sistemas y datos más confidenciales de su organización.

En este capítulo, le guiaremos a través de la creación de una estrategia integral de PAM mediante una práctica lista de comprobación.

Seguir estos pasos le ayudará a reforzar su postura de seguridad y a reducir el riesgo de infracciones relacionadas con cuentas privilegiadas.

1. Identificar y Proteger todas las Cuentas con Privilegios

El primer paso para construir una estrategia PAM es identificar todas las cuentas privilegiadas dentro de su organización, incluyendo usuarios humanos, cuentas de servicio y entidades no humanas como aplicaciones.

Puntos de acción

- Realice una auditoría de descubrimiento para identificar todas las cuentas privilegiadas.
- Clasifique estas cuentas en función del nivel de acceso y de los riesgos asociados.
- Proteja todas las cuentas privilegiadas con contraseñas fuertes y únicas.

2. Implantar la Autenticación Multifactor (MFA)

La MFA añade una capa esencial de protección al exigir múltiples formas de verificación antes de conceder acceso a cuentas privilegiadas.

Puntos de acción

- Imponga MFA para todas las cuentas con privilegios.
- Utilice MFA tanto para usuarios internos como remotos.
- Garantizar que las soluciones de MFA se integran perfectamente en los flujos de trabajo existentes.

3. Aplicar el Principio de Mínimo Privilegio (PoLP)

El Principio de Mínimo Privilegio (PoLP) garantiza que los usuarios tengan el nivel mínimo de acceso necesario para realizar sus tareas, lo que reduce la superficie de ataque.

Puntos de acción

- Revise y restrinja los niveles de acceso de todos los usuarios en función de sus funciones laborales.
- Implantar el control de acceso basado en roles (RBAC) para simplificar la gestión de los derechos de acceso.
- Audite continuamente los permisos para asegurarse de que siguen siendo adecuados a lo largo del tiempo.

4. Automatizar la Gestión y Rotación de Contraseñas

La gestión manual de contraseñas puede dar lugar a errores humanos y lagunas de seguridad. Automatizar la rotación de contraseñas de cuentas privilegiadas ayuda a mitigar los riesgos de credenciales comprometidas.

Puntos de acción

- Establezca una rotación automática de contraseñas para todas las cuentas con privilegios.
- Asegúrese de que las políticas de rotación de contraseñas cumplen las normas de seguridad de su organización.
- Utilice soluciones de almacenamiento de contraseñas para guardar y gestionar las credenciales de forma segura.

5. Imponer el Aprovisionamiento *Just-in-Time (JIT)*

El aprovisionamiento **Just-in-Time (JIT)** limita el tiempo durante el cual las cuentas privilegiadas tienen acceso elevado, reduciendo la ventana de oportunidad para que los atacantes exploten las cuentas.

Puntos de acción

- Implantar el aprovisionamiento JIT para sistemas críticos y datos sensibles.
- Limite la duración del acceso elevado y revoque una vez finalizadas las tareas.
- Configure la caducidad automática de los privilegios cuando no se utilicen.

6. Supervisar y Auditar las Actividades Privilegiadas

La supervisión y auditoría periódicas de las actividades privilegiadas son esenciales para detectar comportamientos sospechosos y garantizar el cumplimiento de las políticas de seguridad.

Puntos de acción

- Permitir la supervisión continua de las sesiones privilegiadas.
- Establezca alertas automáticas para detectar actividades inusuales o infracciones de las políticas.
- Revisar periódicamente los registros de auditoría para garantizar el cumplimiento de los requisitos internos y normativos.

7. Eduque y Forme a sus Trabajadores

Una plantilla bien informada es crucial para el éxito de su estrategia PAM. Los empleados y administradores deben comprender su papel en el mantenimiento de la seguridad y cómo afecta PAM a sus operaciones diarias.

Puntos de acción

- Impartir periódicamente sesiones de formación sobre las mejores prácticas y protocolos de seguridad de la PAM.
- Asegúrese de que los usuarios conocen los ataques de phishing, la gestión de credenciales y los métodos de acceso seguro.
- Mantener informado al personal de los cambios en las políticas y procedimientos de PAM.

8. Revisar y Actualizar Periódicamente las Políticas de la PAM

Su estrategia PAM debe evolucionar con las necesidades de su organización y el cambiante panorama de las amenazas. Las revisiones y actualizaciones periódicas garantizan la eficacia de las políticas.

Puntos de acción

- Programar revisiones periódicas de las políticas y prácticas de PAM.
- Actualizar las políticas de PAM en respuesta a los cambios tecnológicos, los procesos empresariales o los requisitos normativos.
- Evalúe continuamente la eficacia de sus herramientas de PAM y realice los ajustes necesarios.

Resumen de los puntos clave

- **Identifique y proteja todas las cuentas privilegiadas** para garantizar una protección completa.
- **Implemente la MFA** para una capa adicional de seguridad.
- **Aplique el Principio de Mínimo Privilegio (PoLP)** para minimizar el acceso excesivo.
- **Automatice la gestión y rotación de contraseñas** para reducir los errores manuales.
- **Aplique el aprovisionamiento *Just-in-Time* (JIT)** para limitar la duración del acceso privilegiado.
- **Supervise y audite las actividades privilegiadas** para detectar a tiempo comportamientos sospechosos.
- **Eduque y forme a su personal** para mejorar la concienciación sobre la seguridad y el cumplimiento de las mejores prácticas.
- **Revise y actualice periódicamente las políticas PAM** para mantener su estrategia de seguridad alineada con la evolución de las amenazas.

En el próximo capítulo, vamos explorar "**Ganancias rápidas para fortalecer su implementación de PAM**", destacando los pasos accionables que puede tomar de inmediato para mejorar su estrategia de PAM y mejorar la seguridad.

10

Victorias rápidas para reforzar la implantación de PAM

Reforzar su estrategia de Gestión de Acceso Privilegiado (PAM) no siempre requiere grandes revisiones o proyectos a largo plazo.

Pequeños cambios estratégicos pueden tener un gran impacto en la seguridad de su organización.

En este capítulo, nos centraremos en algunos logros rápidos que pueden mejorar rápidamente su implementación de PAM.

1. Rote periódicamente las credenciales privilegiadas

La rotación automática de contraseñas es una de las formas más sencillas de mejorar la seguridad rápidamente.

Las contraseñas obsoletas o estáticas son vulnerables a los ataques, especialmente si se comparten entre varios usuarios o no se han actualizado con regularidad.

Puntos de acción

- Establezca una rotación automática de contraseñas para todas las cuentas con privilegios.
- Asegúrese de que las contraseñas se rotan con frecuencia para minimizar el riesgo de compromiso.
- Guarde las contraseñas rotadas de forma segura en una cámara acorazada de contraseñas.

2. Implantar el aprovisionamiento *Just-in-Time (JIT)*

Los controles de aprovisionamiento Just-in-Time (JIT) pueden minimizar rápidamente la ventana de oportunidad para los atacantes concediendo acceso sólo cuando sea necesario. Se trata de una forma eficaz de reducir los privilegios permanentes innecesarios y mitigar los riesgos de uso indebido de credenciales.

Puntos de acción

- Establezca políticas de aprovisionamiento JIT para conceder acceso privilegiado sólo cuando sea necesario.
- Revocar el acceso automáticamente una vez finalizada la tarea.
- Utilice el ECI tanto para entidades humanas como no humanas, como las cuentas de servicio.

3. Imponer la Autenticación Multifactor (MFA)

Añadir la autenticación multifactor (MFA) es una forma sencilla pero potente de proteger las cuentas privilegiadas.

MFA ayuda a evitar el acceso no autorizado incluso si las credenciales están en peligro, añadiendo una capa crucial de defensa.

Puntos de acción

- Aplique MFA a todas las cuentas privilegiadas de la organización.
- Integre la MFA en las herramientas de acceso remoto y otras aplicaciones críticas.
- Utilice opciones de MFA basadas tanto en hardware como en software en función del caso de uso.

4. Supervisar y Auditar las Actividades Privilegiadas

La supervisión y auditoría continuas son esenciales para detectar a tiempo comportamientos sospechosos.

Una forma rápida de conseguirlo es configurar alertas en tiempo real para cualquier actividad anormal relacionada con cuentas privilegiadas.

Puntos de acción

- Activar la supervisión continua de todas las sesiones privilegiadas.
- Establezca alertas para detectar anomalías, como horas de acceso o ubicaciones geográficas inusuales.
- Revise periódicamente los registros de auditoría y adopte las medidas correctoras necesarias.

5. Aplicar el Principio de Mínimo Privilegio (PoLP)

Aplicar el Principio de Mínimo Privilegio (PoLP) en toda la organización es una buena práctica fundamental.

Los usuarios, las aplicaciones y los sistemas deben tener sólo el acceso mínimo necesario para realizar sus funciones.

Puntos de acción

- Realice una revisión de los accesos para identificar a los usuarios con permisos excesivos.
- Ajuste los privilegios para que los usuarios sólo tengan el nivel mínimo de acceso requerido para su función.
- Implantar el control de acceso basado en funciones (RBAC) para agilizar la gestión de privilegios.

6. Centralizar la Gestión de las Cuentas de Servicio

Las cuentas de servicio suelen pasarse por alto, pero pueden plantear importantes riesgos de seguridad si no se gestionan.

Al centralizar la gestión de estas cuentas, se puede reforzar rápidamente la seguridad.

Puntos de acción

- Descubra y centralice todas las cuentas de servicio en su sistema PAM.
- Automatice la gestión y la rotación de las credenciales de las cuentas de servicio.
- Asegúrese de que las cuentas de servicio se incluyen en acceso JIT y en auditoría de políticas.

7. Eduque a su equipo sobre las mejores prácticas en materia de PAM

Impartir una formación rápida y específica a sus empleados puede reforzar significativamente la implantación de su PAM.

Todos los miembros de la organización deben comprender la importancia de proteger las cuentas privilegiadas.

Puntos de acción

- Organizar un taller o una sesión de formación sobre las mejores prácticas en materia de PAM.
- Asegúrese de que los empleados comprenden su papel en el mantenimiento de la seguridad de los accesos privilegiados.
- Céntrese en áreas como la MFA, la gestión segura de contraseñas y la concienciación sobre la suplantación de identidad.

A continuación, nos enfocamos en **"Evaluación y Transición de Soluciones PAM"**, donde exploramos cómo evaluar su sistema PAM actual y realizar una transición sin problemas a una solución moderna que se adapte a las necesidades de seguridad en evolución de su organización.

11

Evaluación y transición de las soluciones PAM

A medida que las organizaciones crecen y las necesidades de seguridad evolucionan, se hace evidente la necesidad de reevaluar y, potencialmente, cambiar a una solución de gestión de acceso privilegiado (PAM) más adecuada.

En este capítulo, exploraremos los motivos para considerar nuevas soluciones PAM, en particular Delinea, destacamos las características clave de las herramientas PAM modernas y ofrecemos orientación para planificar una transición sin problemas.

1. Evaluación de su solución PAM actual

Antes de decidirse por una nueva herramienta de PAM, es crucial evaluar a fondo los puntos fuertes y las limitaciones de su sistema actual.

Esto le ayudará a identificar carencias y áreas de mejora.

Puntos clave de la evaluación

- **Experiencia del usuario:** ¿El sistema actual es fácil de usar o requiere un esfuerzo manual excesivo?
- **Escalabilidad**: ¿Puede gestionar las crecientes necesidades de acceso privilegiado a medida que crece su organización?
- **Capacidades de la nube:** ¿Se integra perfectamente con la infraestructura en la nube?
- **Funciones de seguridad:** ¿Es compatible con protocolos de seguridad modernos como la autenticación multifactor (MFA), el aprovisionamiento Just-in-Time (JIT) y la auditoría robusta?

2. ¿Por qué cambiar a Delinea?

A medida que su organización crece y las necesidades de seguridad evolucionan, es posible que necesite una mayor escalabilidad, funciones de nube mejoradas o una interfaz más fácil de usar.

Recomendamos cambiar a Delinea. Delinea ofrece un enfoque más moderno, flexible y fácil de usar para la Gestión de Acceso Privilegiado. Cambiar de CyberArk a Delinea puede parecer complejo, pero con el enfoque adecuado resultará sencillo y beneficioso.

Delinea ofrece la flexibilidad y las prestaciones necesarias para satisfacer estas exigencias modernas.

- **Escalabilidad mejorada:** Delinea está diseñado para adaptarse a los entornos empresariales modernos, proporcionando flexibilidad para adaptarse al crecimiento y a las cambiantes necesidades de seguridad.
- **Interfaz fácil de usar**: Ofrece un diseño intuitivo que simplifica la gestión y mejora la experiencia del usuario, facilitando a los equipos informáticos su implantación y mantenimiento.
- **Amplias capacidades en la nube:** Admite el acceso seguro de usuarios remotos sin necesidad de VPN, por lo que resulta ideal para los entornos de trabajo híbridos actuales.
- **Opciones de integración sólidas:** Se integra fácilmente con los marcos y herramientas de seguridad existentes, lo que garantiza una transición más fluida y una postura de seguridad global mejorada.

3. Identificación de las Características Clave de una Solución PAM Moderna

A la hora de seleccionar una nueva solución PAM, es esencial asegurarse de que satisface sus necesidades actuales y futuras. Estas son las características clave que debe buscar:

Características imprescindibles

- **Facilidad de implantación**: Una nueva solución PAM debe ser fácil de implantar con el mínimo trastorno.
- **Integración en la nube**: La integración perfecta con servicios en la nube como AWS, Azure y Google Cloud es fundamental.
- **Experiencia del usuario**: Asegúrese de que la interfaz sea intuitiva tanto para los administradores como para los usuarios finales.
- **Controles de seguridad exhaustivos**: Funciones avanzadas como la rotación automática de contraseñas, MFA y la supervisión de sesiones no son negociables.
- **Visibilidad en tiempo real**: Las alertas inmediatas y los informes detallados son esenciales para responder rápidamente a los incidentes.

4. Planificación de una Transición Fluida a una Nueva Solución de PAM

El cambio a una nueva solución PAM puede parecer desalentador, pero con un enfoque estratégico, el proceso puede ser fluido y eficaz.

Pasos clave de la transición

- **Desarrolle un plan de migración**: Cree un plan detallado que incluya plazos, hitos clave y recursos necesarios.
- **Transferencia de datos y copia de seguridad**: Garantice una migración de datos segura y sin fisuras, incluidos los almacenes de credenciales, los permisos de usuario y las políticas de acceso.
- **Minimizar el tiempo de inactividad**: Planifique la transición durante periodos de baja actividad para minimizar el impacto en las operaciones diarias.

- **Probar el nuevo sistema**: Lleve a cabo una fase de pruebas exhaustiva para identificar posibles problemas antes de la implantación completa.
- **Formación de usuarios**: Ofrezca formación completa a administradores y usuarios finales para garantizar una adopción sin problemas.

5. Retorno de la Inversión a Largo Plazo de las Soluciones PAM Modernas

Invertir en una nueva solución PAM puede reportar importantes beneficios a largo plazo. Aunque puede suponer un coste inicial, la mejora de la seguridad, la flexibilidad y la eficiencia operativa suelen proporcionar un fuerte retorno de la inversión (ROI).

Beneficios de la transición

- **Mayor seguridad:** Las soluciones PAM modernas ofrecen controles de seguridad más avanzados, lo que reduce el riesgo de infracciones.
- **Productividad mejorada**: Las funciones de automatización reducen la carga de trabajo manual, lo que permite a los equipos de TI centrarse en tareas estratégicas.
- **Escalabilidad**: A medida que su organización crece, las soluciones PAM modernas pueden escalarse fácilmente para gestionar usuarios y recursos adicionales.
- **Rentabilidad**: Las herramientas modernas suelen reducir los costes de mantenimiento continuo al agilizar la gestión y reducir los riesgos.

Resumen de los puntos clave

- **Evalúe su solución PAM actual** para identificar las carencias en materia de seguridad, escalabilidad y facilidad de uso.
- **Identifique características clave** como la integración en la nube, la facilidad de despliegue y los protocolos de seguridad avanzados para una solución PAM moderna.
- **Desarrolle un plan de migración** que incluya la transferencia de datos, pruebas y formación exhaustiva para garantizar una transición sin problemas.
- **Considere el retorno de la inversión a largo plazo**, que incluye una mayor seguridad, una mayor escalabilidad y una reducción de los costes operativos.

A continuación, exploraremos un **"Caso práctico: Cómo PAM Previene las Amenazas Internas y Externas"**, donde ejemplos reales demostrarán el poder de PAM para mitigar los riesgos tanto internos como externos de las cuentas privilegiadas.

12

Caso práctico - Cómo previene PAM las amenazas internas y externas

En este capítulo, exploramos un ejemplo de cómo una sólida estrategia de Gestión de Acceso Privilegiado (PAM) mitiga eficazmente las amenazas internas y externas.

Dado que las cuentas con privilegios son el principal objetivo de los ciberataques, PAM desempeña un papel fundamental a la hora de evitar accesos no autorizados, proteger datos confidenciales y garantizar el cumplimiento de las normativas de seguridad.

Visión general de la Organización

Tamaño
Más de 5.000 empleados

Sector
Servicios financieros

Reto

La organización se enfrentaba a riesgos crecientes de ciberataques externos y amenazas internas, especialmente con el trabajo remoto que complicaba el panorama de la seguridad.

Solución PAM

Implantación de una moderna plataforma PAM para proteger el acceso privilegiado interno y externo.

Identificación de las Principales Amenazas

La organización identificó dos vectores de amenaza principales:

Amenazas externas

Los atacantes externos se dirigían a cuentas privilegiadas utilizando técnicas como el phishing, el robo de credenciales y la explotación de vulnerabilidades no parcheadas.

Riesgos identificados

- Compromiso de credenciales a través de correos electrónicos de *phishing*.
- Ataques de escalada de privilegios.
- Explotación de cuentas de servicio para obtener acceso no autorizado.

Amenazas internas

Los usuarios internos, incluidos empleados y contratistas, planteaban riesgos potenciales debido al exceso de privilegios, el uso indebido del acceso administrativo y la falta de supervisión de las actividades internas.

Riesgos identificados

- Los usuarios con privilegios hacen un uso indebido de las credenciales para acceder a datos sensibles.
- Uso compartido no autorizado de credenciales privilegiadas.
- Falta de responsabilidad por las acciones administrativas.

Cómo Abordó PAM las Amenazas Externas

PAM proporcionaba varias capas de defensa contra las amenazas externas:

- **Autenticación multifactor (MFA)**
  Los atacantes externos que intentaban comprometer cuentas privilegiadas fueron bloqueados por la implementación de MFA para todos los usuarios privilegiados, evitando el acceso no autorizado incluso si las credenciales fueron robadas.
- **Rotación automática de contraseñas**
  PAM rota automáticamente las contraseñas privilegiadas de forma regular, reduciendo la ventana de oportunidad para que los atacantes utilicen credenciales comprometidas.
- **Aprovisionamiento *Just-in-Time* (JIT)**
  El acceso externo a sistemas críticos se concedía sólo cuando era necesario, minimizando la exposición a sistemas privilegiados y garantizando que el acceso se revocaba inmediatamente después de su uso.
- **Supervisión y grabación de sesiones**
  PAM permitió la monitorización en tiempo real de las sesiones privilegiadas, detectando cualquier comportamiento anómalo y permitiendo al equipo de seguridad tomar medidas inmediatas cuando fuera necesario.

Cómo Abordó la PAM las Amenazas Internas

Para las amenazas internas, PAM permitió un control más estricto y una mejor visibilidad de los accesos privilegiados:

- **Aplicación del Principio del Menor Privilegio**
  PAM aplicó el principio de mínimo privilegio, garantizando que los empleados sólo tuvieran acceso a los recursos que necesitaban para realizar sus funciones laborales, reduciendo el riesgo de uso indebido.
- **Segregación de Funciones**
  La organización implantó controles de acceso basados en roles (RBAC) para segregar funciones, evitando que un único usuario tuviera un control excesivo sobre sistemas críticos.
- **Registros de Auditoría y Supervisión Continua**
  PAM generó registros de auditoría detallados de todos los accesos y actividades privilegiadas. Esta visibilidad permitió a la organización supervisar de cerca las actividades internas e identificar rápidamente cualquier acción no autorizada o sospechosa.

- **Prohibición de Compartir Credenciales**
  PAM aplicó políticas que prohibían compartir credenciales de cuentas privilegiadas, garantizando que cada evento de acceso pudiera ser rastreado hasta un individuo específico.

Resultados y beneficios

Tras la implantación de PAM, la organización experimentó mejoras significativas tanto en seguridad como en eficacia operativa:

- **Reducción de los Incidentes de Seguridad**
  Las brechas externas dirigidas a cuentas privilegiadas se redujeron en un 75%, gracias a medidas de autenticación más estrictas y a la supervisión en tiempo real.
- **Cumplimiento Mejorado**
  La organización superó con facilidad las auditorías normativas gracias a las detalladas funciones de registro e informes de PAM, que garantizaban la trazabilidad de todas las acciones privilegiadas.
- **Mayor Productividad**
  La gestión automatizada del acceso y la rotación de contraseñas redujeron la carga de trabajo manual del equipo de TI, lo que les permitió centrarse en iniciativas más estratégicas.
- **Prevención de Amenazas Internas**
  El uso indebido de privilegios por parte de usuarios internos se mitigó mediante estrictos controles de acceso y una supervisión continua, lo que permitió mejorar la rendición de cuentas.

Resumen de los puntos clave

- **Las amenazas externas**, como el robo de credenciales y la escalada de privilegios, se mitigaron mediante la autenticación multifactor, la rotación de contraseñas y la supervisión de sesiones.
- **Las amenazas internas** se abordaron mediante la aplicación de los privilegios mínimos, la segregación de funciones y la supervisión continua de las actividades privilegiadas.
- **Los resultados fueron los siguientes**: reducción de los incidentes de seguridad, mejora del cumplimiento de la normativa y aumento de la productividad.

A continuación, exploraremos la "**Conclusión: El futuro de PAM en la ciberseguridad**", donde analizaremos las tendencias emergentes, la evolución del papel de PAM y cómo las organizaciones pueden prepararse para el futuro de la gestión de accesos privilegiados.

13

Conclusión - El futuro de PAM en Ciberseguridad

De cara a 2025 y más allá, la importancia de la Gestión de Accesos Privilegiados (PAM) en el panorama de la ciberseguridad está llamada a crecer significativamente.

Este capítulo explora la creciente relevancia de la PAM, su evolución junto con las tecnologías emergentes y los próximos pasos a seguir para las organizaciones que pretenden mejorar su postura de ciberseguridad.

La creciente importancia de PAM en 2025 y más allá

Ciberamenazas crecientes	Con ciberataques cada vez más sofisticados, PAM es esencial para proteger las cuentas privilegiadas, que son los principales objetivos de los ***hackers***.
Cumplimiento de la normativa	A medida que se endurecen las normativas en torno a la protección de datos y la privacidad, las organizaciones deben implantar estrategias eficaces de PAM para cumplir los requisitos de conformidad.
Trabajo remoto e híbrido	La continuación de modelos de trabajo remotos e híbridos requiere soluciones PAM robustas que aseguren el acceso desde diversas ubicaciones y dispositivos.

Cómo sigue evolucionando el PAM con las nuevas tecnologías

Integración con marcos de Zero Trust

PAM se alineará cada vez más con los principios de Zero Trust, centrándose en la verificación continua de usuarios y dispositivos independientemente de su ubicación en la red.

Adopción de IA y aprendizaje automático

La incorporación de IA mejorará la capacidad de PAM para detectar anomalías, agilizar la gestión del acceso de los usuarios y automatizar los protocolos de respuesta.

Soluciones nativas de la nube

A medida que las organizaciones se trasladan a la nube, las soluciones PAM diseñadas específicamente para entornos en la nube serán cruciales para mantener un acceso seguro.

Análisis del comportamiento de los usuarios

La supervisión del comportamiento de los usuarios a través de análisis ayudará a identificar patrones inusuales, ayudando a prevenir amenazas internas y accesos no autorizados.

Próximos pasos para las organizaciones que deseen reforzar la ciberseguridad

Evaluar las soluciones actuales de PAM	Evalúe la eficacia de las herramientas de PAM existentes e identifique áreas de mejora o actualización a sistemas más avanzados.
Implemente programas de formación exhaustivos	Forme periódicamente a los empleados en las mejores prácticas de seguridad y en la importancia de PAM para proteger los datos sensibles.
Adopte un enfoque proactivo	Supervisar y adaptar continuamente las estrategias de PAM para responder a las nuevas amenazas y a los cambios en el panorama de la organización.
Fomentar la colaboración entre departamentos	Fomente la cooperación entre los equipos de TI, seguridad y cumplimiento para crear un enfoque unificado de la gestión del acceso privilegiado.

Resumen de los puntos clave

- **La importancia de la PAM** seguirá creciendo a medida que aumenten las ciberamenazas y las exigencias normativas en los próximos años.
- **Las tecnologías emergentes**, como la IA, los marcos de zero trust y las soluciones en la nube, están transformando las prácticas de las PAM.
- Las organizaciones deben **dar los siguientes pasos**, como evaluar las soluciones PAM, implantar programas de formación y fomentar la colaboración para mejorar su postura de ciberseguridad.

En conclusión

El futuro de PAM no es sólo cuestión de tecnología; se trata de crear una cultura de seguridad que dé prioridad a la protección de los accesos privilegiados como componente vital de cualquier estrategia de ciberseguridad.

A medida que las organizaciones asuman estos cambios, estarán mejor equipadas para navegar por las complejidades del panorama digital.

14

Ponte en contacto

Entendemos que cada organización tiene sus propios retos y necesidades en materia de ciberseguridad. Por eso estamos aquí para ayudar.

Si tiene alguna pregunta, necesita más orientación o está listo para dar los siguientes pasos en el fortalecimiento de su estrategia de PAM, le invitamos a ponerse en contacto con nosotros.

Conéctese con nosotros

Para obtener asistencia personalizada y asesoramiento experto, póngase en contacto con:

Fernando Carvalho
Director de Movilidad y Seguridad

No dude en ponerse en contacto con nosotros. Juntos podemos construir un futuro más seguro para su organización.