Eleven Paths

Claves para implantar una Identidad Digital Corporativa 360

Un desafío que no se debe retrasar

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

Resumen ejecutivo

En los últimos años, y en paralelo a los procesos acelerados de transformación digital corporativa, un gran problema ha ido creciendo inadvertidamente en las estructuras fundamentales de toda organización.

Nos referimos a los inconvenientes derivados de una **gestión ineficiente de las identidades y el acceso** que, por un lado, lastran la productividad y merman la expansión del negocio y, por otro, afectan de manera significativa a la seguridad de la organización.

Factores causantes de los problemas relativos a la gestión de identidad:

- Evolución tecnológica no planificada basada en soluciones parciales y aisladas.
- El crecimiento inorgánico corporativo y el retraso de la integración de los directorios de identidades.
- Falta de procesos estándar de gestión del ciclo de vida y una política de roles y autorizaciones.
- Demora en implantar medidas correctivas e implantar una estrategia corporativa de identidad.

Este *paper* se inicia con la descripción de los problemas generados por una gestión ineficiente de la Identidad corporativa para a continuación describir un modelo de gobierno de la identidad basado en la metodología de CARTA de Gartner. Por último, se detallan las características que debe tener una solución completa de gestión de identidades y acceso.

01

Retos en la gestión de la identidad corporativa

02. Seguridad

- **Acumulación excesiva e innecesaria de privilegios** debido a cambios de rol de personal interno.
- Credenciales de **accesos privilegiados vulnerables** puesto que sus contraseñas no son custodiadas debidamente.
- **Incapacidad de auditar los accesos** privilegiados.
- La carencia de un **proceso de baja automatizado** implica un riesgo importante de robo de información confidencial o sabotaje.
- La no implantación de una **política de contraseñas rigurosa** facilita el robo de credenciales.
- Robos de **credenciales de bots o dispositivos IoT** no incluidos en el plan de gobierno de la identidad.

01. Productividad y Negocio

- **Retrasos** en provisión de nuevos empleados.
- Equipos de recursos humanos o TI ocupados en **tareas repetitivas y de escaso valor.**
- Incoherencias en el organigrama que implican **demoras en las autorizaciones de accesos** a recursos corporativos.
- **Desatención de tareas** de identidad más relevantes y de visión estratégica.
- Existencia de un alto número de **cuentas huérfanas** lo que implica gasto en licenciamiento innecesario
- **Riesgo de fraude** mediante credenciales de desarrollo o pruebas no adecuadamente custodiadas.

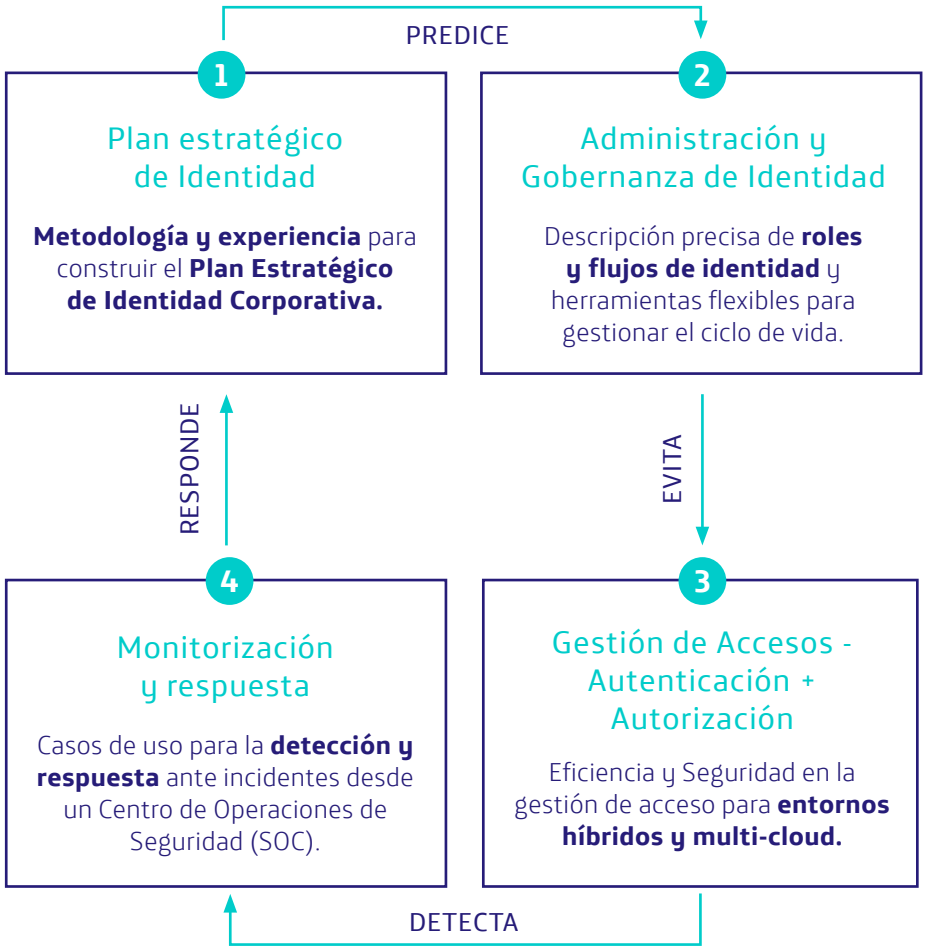
03. Riesgos Regulatorios

- La **certificación de accesos a recursos corporativos** resulta una tarea muy laboriosa o directamente imposible de realizar.
- Cumplir con las **normativas regulatorias de privacidad y protección de datos**, como GDPR y LGDP, durante el acceso y custodia de la información de carácter personal de empleados, colaboradores y usuarios finales.
- Imposibilidad de **evitar y detectar filtraciones de información** de usuarios finales.

02 Modelo CARTA para la gestión de la identidad

Telefónica propone un modelo de gestión de la identidad basado en los principios de CARTA (Continuous Adaptive Risk and Trust Assessment)*.

La gestión de la identidad es una tarea dinámica que debe ser lo suficientemente líquida como para extenderse a un perímetro de seguridad difuso, e incluso inexistente. En este modelo, la seguridad se fundamenta en el principio de confianza cero (Zero-trust), por tanto, el acceso a recursos está sujeto a parámetros contextuales –como el lugar, el mecanismo de conexión, el dispositivo y el comportamiento del usuario– y en base a procesos adaptativos de autenticación continua vinculados a motores de riesgo. Por último, este modelo CARTA demanda una monitorización permanentemente de anomalías para detectar posibles infiltraciones.



* En 2017, Gartner introdujo un nuevo enfoque estratégico para la seguridad de la información: evaluación continua de riesgo y confianza adaptativa (CARTA). Este nuevo principio abarca la realidad de asegurar un mundo donde las capacidades digitales de los negocios son accesibles desde cualquier lugar, por cualquier dispositivo y donde los atacantes evolucionan tan rápido como las estrategias de protección.

03 Los pilares tecnológicos de la Identidad y gestión de accesos

Una solución completa de gestión de la identidad y los accesos requiere dar respuesta a cuatro categorías de casos de uso mediante un ecosistema de tecnologías punteras, que permiten despliegues ágiles y amplias posibilidad de integración.

Administración y Gobernanza de la Identidad

Gestión del Acceso

Customer Identity and Access Management

Gestión de Cuentas Privilegiadas

Se requiere un despliegue paulatino de tecnologías, de acuerdo al Plan Estratégico de Identidad, y preferiblemente en modalidad SaaS completa o parcial siempre y cuando los requisitos organizativos lo permitan.

Será fundamental a la hora de elegir estas tecnologías tres factores:

- **Las capacidades avanzadas** de autenticación biométrica, analítica de identidad y detección de comportamientos anómalos.
- **La flexibilidad** para realizar configuraciones de manera rápida, intuitiva y replicable.
- **La disponibilidad de conectores** con servicios o aplicaciones SaaS, nubes públicas y aplicaciones legadas para implantar fácilmente casos de uso complejos.

Casos de uso de Identidad

Existe un consenso en el mercado en agrupar los casos de uso de identidad y gestión de accesos en las siguientes cuatro categorías tecnológicas.

Administración y Gobernanza de la Identidad (IGA)

- **Consolidación de Identidades** (sincronización/ federación).
- **Repositorio de identidades** centralizado.
- **Provisión de identidades** automatizada.
- **Revisiones Periódicas.**
- **Certificación de Accesos.**
- **Gestión de bajas** de empleados.
- Control de **Acceso Basado en Roles** (RBAC).
- Descubrimiento de **cuentas huérfanas.**
- Gestión de **usuarios colaboradores.**
- Flujos de **aprobación automatizados.**

Gestión del acceso

- **Multi-factor Authentication.**
- **Autenticación** Centralizada.
- **Portal de acceso** unificado.
- **Single-Sign on** (cloud, on-premise, devops).
- Autenticación continua **passwordless**.
- Políticas de **gestión de Accesos.**
- **Zero-Trust Network Access.**

Gestión de la Identidad y Accesos de Clientes (CIAM)

- Funciones de **Autoservicio**.
- **Single-Sign on** para clientes.
- **Identidad Social** (BYOI).
- Gestión del **consentimiento y la privacidad.**
- **Onboarding digital.**
- **Analíticas** e informes.
- **Registro de perfil** progresivo.
- **Integración con CRM.**

Gestión de cuentas privilegiadas (PAM)

- **Password Vault.**
- Autogeneración de **contraseñas.**
- Detección de **usos anómalos** de cuentas.
- **Monitorización** de sesiones.
- **Bloqueo** de sesiones.
- **Auditoría** de Cuentas Privilegiadas.
- Descubrimiento de **cuentas privilegiadas.**

04 Claves para implantar tu plan estratégico

01. Análisis y Diseño

02. Despliegue y configuración

03. Administración y Monitorización

01. Análisis y Diseño

La Consultoría Experta ayuda a las corporaciones a construir su Plan Estratégico de Identidad.

- Utiliza una metodología exitosa para la construcción del **modelo de gestión y gobierno de la identidad.**
- Colaboración entre diferentes departamentos para realizar las **tareas de coordinación** entre equipos.
- **Levantamiento de información** mediante entrevistas a actores relevantes.
- Alineamiento con las **políticas de seguridad** corporativas.
- Evaluación de **riesgos y prioridades.**
- **Definición y seguimiento de Indicadores** (KPIs) para garantizar la implantación exitosa.
- Diseño de **procesos y roles** de la organización.
- Coordinación con los equipos de negocio para la **gestión de las identidades de usuarios finales.**
- **Diseño de la arquitectura** y selección tecnológica.

02. Despliegue y configuración

Mediante equipos de tecnólogos certificados afronta la implantación de las tecnologías seleccionadas en tu plan estratégico.

- Despliega la tecnología en el ecosistema más adecuado para tu organización, **cloud pública, cloud privada u on-premise.**
- Configura o desarrolla los **conectores** con tus servicios y aplicaciones.
- Implanta el modelo de **procesos y roles.**
- **Gestiona el proyecto mediante metodologías agiles** de iteraciones cortas y con objetivos realistas.
- Diseña un **plan de formación y certificación** a medida para cada departamento.
- Asegura el **conocimiento transversal.**

03. Administración y monitorización

Integra dentro de tu modelo de gestión de seguridad corporativo la gestión de la Identidad y los accesos y adminístralo desde tu SOC de referencia.

01. Administra

- Soporte 7x24 de resolución de incidencias y dudas.
- Control de versiones y gestión de release.
- Registro de casos y priorización de tickets.

02. Monitoriza

- Monitorización proactiva de los sistemas IAM.
- Alertas en tiempo real de caídas del sistema.
- Identificación de situaciones anómalas.

03. Evalúa

- Seguimiento continuo de KPIs.
- Generación de Informes a medida.
- Seguimiento estricto de SLAs.

04. Evoluciona

- Consultoría anual para optimizar la gestión.
- Mejora continua de los procesos de gestión del ciclo de vida y políticas.
- Implementación de nuevos conectores.

MONITORIZACIÓN AVANZADA

Priorizar alertas y organizar acciones de remediación automatizadas basado en flujos de trabajo y políticas predefinidas.

Consultar la actividad de riesgo de los usuarios, como inicios de sesión fallidos o incorporación de nuevos factores de autenticación para detectar amenazas antes de que sucedan.

Enriquecimiento automático de las alertas de seguridad con información del contexto de identidad.

Identificar anomalías en base a la construcción de patrones de comportamiento de entidades:

- Patrones de inicio de sesión inusuales.
- Actividad repentina, inusual o rara con archivos, sistemas o procesos.
- Suplantación de usuario para acceso a archivos y unidades.
- Acceso a fuerza bruta.
- Reconocimiento interno.
- Baja y lenta filtración de datos del usuario a almacenamiento externo o conectado.
- Actividad de bot.
- Problemas de rendimiento de la máquina.
- Cuentas de servicio mal configuradas.

La gestión de la identidad y los accesos es un reto mayúsculo que requiere de una base tecnológica, así como un conocimiento experto y también un liderazgo estratégico a la vez que realista.

En ElevenPaths conocemos la problemática y hemos adaptado nuestras soluciones a este escenario complejo de ecosistemas difusos. Nuestras soluciones combinan la tecnología más vanguardista con unos servicios profesionales certificados y con una gran experiencia.

Permítenos ayudarte en afrontar este desafío y construir contigo la solución adaptada a tu organización que convierte la gestión de la identidad en tu ventaja competitiva.

Sobre ElevenPaths

En ElevenPaths, la compañía de ciberseguridad del Grupo Telefónica, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su transformación digital, creando innovación disruptiva, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria.

Combinamos la frescura y energía de una start-up con la potencia, conocimiento y robustez de Telefónica, contribuyendo con soluciones que posibilitan la prevención, detección y respuesta ante amenazas diarias en nuestro mundo digital.

Generamos alianzas estratégicas que permiten ampliar la seguridad de nuestros clientes y además, colaboramos con organismos y entidades como la Comisión Europea, CyberThreat Alliance, ECSO, EuroPol, Incibe, y la la Organización de los Estados Americanos (OEA).

Más información:
elevenpaths.com | @ElevenPaths | blog.elevenpaths