La exposición favorita de los ciberdelincuentes: errores más comunes en la gestión de identidad y accesos

La gestión de identidades y accesos se ha convertido en un pilar crítico de la ciberseguridad: solo en el primer semestre de 2025 se sustrajeron más de

1,8 mil millones

de credenciales (*) en organizaciones de todo el mundo.

Por otra parte, la adopción de la IA trae consigo tantas oportunidades de mejora como riesgos: ya existen

83 identidades

de máquina por cada identidad humana.

(*) Flashpoint, Global Threat Intelligence Index: 2025 Midyear Edition

IndraMind

EL GRITO (DE CONTRASEÑAS)

Difundir credenciales, almacenarlas en espacios no seguros, crear passwords poco robustas o usar las mismas para varios sitios

Compartir, reutilizar o guardar contraseñas en lugares no seguros pueden convertir un simple error humano en una brecha de seguridad fácilmente evitable. Cuando un usuario “grita” sus credenciales —anotadas en documentos físicos, chats no cifrados o archivos compartidos— expone información sensible que puede comprometer a toda la organización.

El riesgo de este fallo podría implicar accesos no autorizados, robo o exposición de datos, movimientos laterales dentro de la red o malware, pues unas credenciales mal gestionadas suelen ser el punto de entrada para ciberataques, como ransomware.

Más del 80% de las brechas de seguridad están vinculadas al uso de credenciales comprometidas, débiles o reutilizadas.

Fuente: Verizon Data Breach Investigations Report 2024

¿Qué puedes hacer como organización?

- Apuesta por el enfoque passwordless, eliminando progresivamente las contraseñas cuando no sean necesarias y utilizando, en su lugar, métodos más seguros de verificación de identidad (OTP, MFA, biometría...). Mientras existan contraseñas, establece y aplica una política sólida: longitud mínima, complejidad, renovación, etc.

- Invierte en formación y concienciación en buenas prácticas para la gestión segura de credenciales.

- Revisa periódicamente los accesos y realiza auditorías de uso de credenciales.

LA LIBERTAD GUIANDO A (LOS TERCEROS)

Acceso no gobernado de personal externo a la organización

Como en La Libertad guiando al pueblo, en una organización todo el equipo debería avanzar en la misma dirección. Pero ¿sabemos realmente quién forma parte del grupo en cada momento?

Cuando los accesos de terceros no se gestionan adecuadamente, la seguridad de toda la organización puede verse comprometida.

Un solo acceso mal controlado puede abrir la puerta a entradas no autorizadas, exposición de datos críticos, filtración de información confidencial, instalación de malware, incumplimientos normativos o, incluso, suplantaciones de identidad.

1 de cada 3 incidentes de seguridad en 2024 tuvo su origen en accesos de terceros no gobernados.

Fuente: SecurityScorecard 2025 Global Third-Party Breach Report

¿Qué puedes hacer como organización?

- Revisa y revoca accesos de terceros de manera regular, especialmente cuando un proyecto o servicio finaliza.
- Establece políticas claras de acceso para terceros, alineadas con estándares como ISO 27001 o GDPR, y realiza auditorías periódicas para verificar cumplimiento.
- Adopta soluciones avanzadas e inteligentes de gestión y verificación de identidades. PAM, para controlar cuentas críticas o con privilegios, y CIAM, para la correcta gestión y trazabilidad de los usuarios externos.

EL JARDÍN DE LAS (ALERTAS)

No monitorizar, detectar y analizar alertas de seguridad con regularidad

Como en El Jardín de las Delicias, los pequeños detalles pueden pasar desapercibidos... hasta que ya es demasiado tarde. La digitalización de sistemas y procesos, la convergencia IT-OT y la adopción de la IA, entre otros avances, abren nuevos vectores de riesgo que solo se detectan con una supervisión activa y continua.

Tener visibilidad completa del entorno conectado y delimitar quién puede acceder y a qué permite detectar comportamientos anómalos y prevenir incidentes como el compromiso de cuentas o las brechas de seguridad.

9 de cada 10 organizaciones han sufrido al menos dos brechas de seguridad relacionadas con la identidad digital en el último año.

Fuente: CyberArk Identity Security Threat Landscape Report 2024

¿Qué puedes hacer como organización?

- Evoluciona hacia un SOC inteligente y automatizado que incorpore capacidades de detección y respuesta ante amenazas de identidad digital. Tecnologías como ITDR permiten monitorizar el comportamiento de los usuarios, detectar comportamientos anómalos, y responder con rapidez a ataques basados en el abuso de credenciales.

(VERIFICA QUE ERES TÚ CON UN) AUTORRETRATO

No contar con la IA como aliada para la verificación de identidades

En el autorretrato cubista de Picasso, el rostro del artista parece reconocible, pero no del todo. Con la identidad digital, puede suceder lo mismo, sobre todo, con el avance de la IA. Cada vez, resulta más complicado distinguir la realidad de la ficción, y las herramientas para crear voces, imágenes y vídeos sintéticos están al alcance de cualquier usuario.

Si una identidad creada o manipulada por IA logra comprometer un control de acceso puede moverse lateralmente por diversos sistemas, escalar privilegios, difundir información confidencial e, incluso, poner en riesgo la continuidad del negocio.

1 de cada 2 empresas ha sido víctima de deepfakes de rostro o voz, y más del 40% considera que el mayor riesgo asociado es el robo de identidades.

Fuente: Regula Deepfake Trends 2024

¿Qué puedes hacer como organización?

- Avanzar hacia modelos de autenticación passwordless, como el uso de biometría soberana de primer nivel basada en IA. Esta tecnología permite detectar fraudes avanzados, como ataques de presentación (PAD), de inyección, deepfakes o ataques a la base de datos biométrica, y verificar identidades de forma más fiable, elevando el nivel de seguridad sin fricción para el usuario.r en la experiencia del usuario.

INDRAMIND CYBERSECURITY

Te acompañamos en el buen gobierno de la seguridad mediante una adecuada gestión de la identidad digital y del control de acceso con soluciones avanzadas e inteligentes, y biometría propia soberana de primer nivel mundial.

+25 años de experiencia en el ámbito de Identidad Digital y +35 en ciberseguridad.

+2.000 profesionales en todo el mundo y más de 400 especialistas en gestión de identidad.

Nuestro conocimiento, especialización sectorial y cobertura internacional nos permite dar respuestas adaptadas a cada organización.

4 millones de identidades verificadas al año y cero fraude.

Contamos con biometría propia de primer nivel.

Somos una compañía homologada como Prestador Cualificado de Servicios de Confianza (eIDAS) a nivel europeo.

IndraMind