Gestión de identidades, influencia en la seguridad

Maycol Paez, Oscar Yela, Brigitte Rodríguez, Juan Peña y Álvaro Cote

Mayo 10 2024

Resumen

La Identidad digital es un concepto que representa el modelo virtual de una persona en el vasto ecosistema en línea que es Internet. Esta Identidad Digital se ha convertido en un aspecto fundamental de la vida moderna, influyendo en la interacción entre la tecnología, la cultura y la sociedad.

La gestión de identidades y accesos se encarga de asegurar que únicamente las personas autorizadas puedan acceder a los recursos y datos críticos de una organización. Esta disciplina de seguridad informática garantiza una identidad digital para cada individuo en cualquier situación que requiera acceso de usuarios. Además, es un componente esencial en la seguridad empresarial y personal, ya que protege contra credenciales comprometidas y contraseñas vulnerables.

Dentro de las prácticas de ciberdefensa el uso de herramientas de ciberseguridad y las campañas de sensibilización y concientización son fundamentales en la prevención de posibles ataques cibernéticos. Aunque la ciberseguridad no solo implica tener tecnología de punta, protocolos seguros, software contra amenazas, seguridad perimetral; si no también se debe fomentar la cultura de ciberseguridad dentro de la organización y la sociedad en general protegiendo el activo más importante de las organizaciones, la información.

Palabras clave

Autenticación, credenciales, internet, identidad, gestión, administración, disponibilidad, integridad, confidencialidad, seguridad, sensibilización, concientización, software, ciberataques.

Abstract

Digital Identity is a concept that represents the virtual model of a person in the vast online ecosystem that is the Internet. This Digital Identity has become a fundamental aspect of modern life, influencing the interaction between technology, culture and society.

Identity and access management is responsible for ensuring that only authorized people can access an organization's critical resources and data. This cybersecurity discipline guarantees a digital identity for everyone in any situation that requires user access. Additionally, it is an essential component in business and personal security, protecting against compromised credentials and vulnerable passwords.

Within cyber defense practices, the use of cybersecurity tools and awareness-raising campaigns are essential in preventing possible cyber-attacks. Although cybersecurity not only implies having cutting-edge technology, secure protocols, anti-threat software, perimeter security; If not, a cybersecurity culture must also be promoted within the organization and society

in general, protecting the most important asset of organizations, information.

I. Introducción

La gestión de identidad juega un papel muy importante debido al aumento exponencial de las transacciones en línea. En un mundo donde la información personal y empresarial se expone constantemente, la gestión efectiva de la identidad se convierte en un escudo para la integridad y seguridad de los sistemas.

Una combinación de tecnología de punta y técnicas de seguridad sólidas mitigan riesgos como el robo de identidad y el fraude. Las soluciones de identidad modernas, respaldadas por tecnologías avanzadas como la biometría, el cifrado y la autenticación multifactorial, ofrecen una capa de protección robusta contra las amenazas digitales.

La mejor práctica en la administración de acceso hoy en día es el "privilegio mínimo". Esto implica asignar a cada entidad o aplicación solo los derechos de acceso necesarios para completar una tarea.

Los SaaS de gestión de identidad permiten a los usuarios acceder a sus identidades y recursos desde cualquier ubicación con conexión a internet, lo que facilita el trabajo remoto y la colaboración. ofrecen una combinación de accesibilidad, escalabilidad, seguridad y facilidad de uso que hacen que sean una opción atractiva para las organizaciones que buscan gestionar de manera efectiva las identidades de sus usuarios.

La autenticación de múltiples factores y la autenticación basada en riesgos son complementarias al inicio de sesión único. Mientras que el SSO proporciona comodidad y eficiencia, la MFA y la autenticación basada en riesgos mejoran la seguridad al agregar capas adicionales de protección contra amenazas cibernéticas.

En un entorno digital en constante cambio, es crucial reconocer que las amenazas cibernéticas evolucionan constantemente. Nuestra investigación resalta la necesidad de una adaptación continua de nuestras estrategias de gestión de identidades para hacer frente a nuevas y emergentes amenazas. La vigilancia proactiva, las actualizaciones regulares de software y la colaboración con la comunidad de ciberseguridad son componentes esenciales para mantenernos un paso adelante de los actores malintencionados.

Además de los desafíos técnicos, también enfrentamos consideraciones legales y regulatorias en relación con la gestión de identidades. Las leyes de privacidad de datos, como el GDPR y el CCPA, imponen requisitos estrictos sobre la recopilación, el almacenamiento y el uso de información personal. Nuestra implementación debe cumplir con estas regulaciones para evitar posibles sanciones y proteger la confianza de nuestros usuarios.

II. CONCEPTOS BASICOS

En el contexto dado el dato es el único medio posible de identificar a alguna persona, aunque no tiene ningún componente físico que se puede complementar, por lo que la información asociada a la persona sea proporcionada ya sea por la persona o por algun tercero se corresponde a la identidad de esa persona, esto también se puede encajar al para las empresas que tienen una gran cantidad de información almacenada en un entorno no privado de la empresa, haciendo que los datos tengan una relevancia fundamental en la gestión de identidades y la ciberseguridad en general.

La gestión de identidad en el ámbito de la seguridad de la información es un componente esencial para proteger los activos digitales de una organización. La correcta

administración de identidades y accesos garantiza que solo las personas autorizadas puedan acceder a la información pertinente, salvaguardando así la confidencialidad, integridad y disponibilidad de los datos sensibles.

Los roles de usuarios desempeñan un papel crucial en este proceso, ya que asignan permisos y responsabilidades dentro de los sistemas y aplicaciones. Establecer políticas claras de roles y privilegios ayuda a mitigar riesgos asociados con el acceso no autorizado o el uso inadecuado de la información.

La revisión periódica de los permisos y accesos asignados a los usuarios es una práctica fundamental en la gestión de identidad. La auditoría de los privilegios existentes permite detectar posibles brechas de seguridad y corregirlas de manera proactiva, garantizando así el cumplimiento normativo y la protección de los datos.

La protección de datos es otro aspecto crucial en la gestión de identidad. La implementación de medidas de cifrado, ofuscación y eliminación de identificación contribuye a preservar la privacidad y confidencialidad de la información, reduciendo el riesgo de exposición ante posibles amenazas.

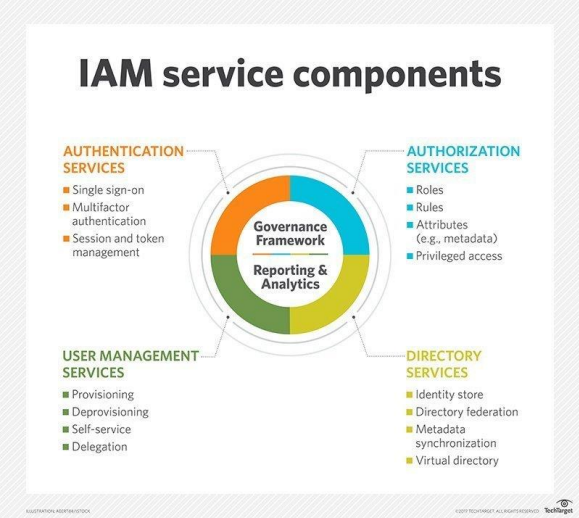
La prevención de ciberataques es una prioridad constante en el ámbito de la gestión de identidad. La adopción de medidas de seguridad robustas, como firewalls, sistemas de detección de intrusiones y análisis de comportamiento, ayuda a prevenir y mitigar potenciales ataques dirigidos a comprometer la integridad de las identidades y los datos.

Además, con un número cada vez mayor de empleados trabajando de forma remota, la gestión de identidades adquiere una relevancia más importante en el ámbito empresarial. Es importante implementar soluciones que permitan la autenticación segura de los usuarios fuera de la red corporativa, al tiempo que se garantiza la protección de los datos corporativos en dispositivos personales y redes no seguras.

En cuanto a los métodos de autenticación, la norma ISO 27001 proporciona un marco de referencia integral para el establecimiento y mantenimiento de un sistema de gestión de seguridad de la información. Esta norma incluye directrices específicas para la autenticación de usuarios, abordando aspectos como la verificación de credenciales, el uso de factores múltiples y la gestión de contraseñas.

En el ámbito de la ciberseguridad, el Marco de Ciberseguridad del NIST (NIST CSF) se presenta como un marco general y un modelo integral para la preparación en este ámbito dentro de una empresa. Este marco abarca varios módulos diseñados para evaluar la preparación de una organización en cuanto a ciberseguridad. Pero su utilidad no se limita solo a nivel organizacional, sino que también puede extenderse a nivel individual, especialmente mediante sus módulos de concientización y capacitación. Estos módulos están dirigidos a aumentar la conciencia entre las personas sobre los riesgos asociados a la ciberseguridad, así como a proporcionarles las habilidades necesarias para identificar y gestionar dichos riesgos cibernéticos (NIST, 2018a).

Además de las normas ISO 27001, el Marco de Ciberseguridad del NIST, también se debe considerar otros estándares y protocolos de seguridad, como OAuth, OpenID Connect y SAML. Estos estándares ampliamente ultilizados proporcionan un marco común para la autenticación y autorización, facilitando la interoperabilidad y la seguridad entre diferentes sistemas y aplicaciones.



III. EVOLUCIÓN DE LA IDENTIDAD DIGITAL

La evolución de la Identidad Digital ha sido un proceso complejo y multifacético que se ha desarrollado a lo largo de décadas, desde los primeros días de internet hasta la era digital contemporánea. En sus inicios, la Identidad Digital era principalmente estática y fragmentada, con la creación de identificadores digitales y perfiles básicos en plataformas en línea limitadas en su alcance y complejidad. Estos perfiles ofrecían una representación rudimentaria de la identidad personal en el primitivo mundo virtual.

Sin embargo, con la aparición de la web 2.0 a principios del siglo XXI, la Identidad Digital entró en una nueva fase de desarrollo. Las redes sociales emergentes, como Facebook, Twitter o LinkedIn, permitieron a los usuarios crear perfiles más dinámicos y participar en comunidades en línea en tiempo real. Esta interacción activa entre individuos en plataformas digitales dio lugar a una comprensión más compleja y multifacética de la identidad en línea. En este punto nace la identidad personal o interna que se refiere a la representación de aspectos individuales de la persona en línea, como el nombre, la edad, la ubicación, los intereses y las experiencias personales. Los perfiles en redes sociales, blogs o plataformas de citas son ejemplos de cómo las personas construyen y presentan su identidad personal en el mundo digital.

La "identidad interna se refiere a la autopercepción de un individuo en relación con sus experiencias y el mundo. Como es de naturaleza reflexiva, la autopercepción no puede manifestarse puramente internamente." (Boyd, 2001, p. 21), por lo que es necesario un complemento a esta dimensión, la identidad social se centra en cómo las personas se relacionan, conectan y se presentan en comunidades en línea y redes sociales. "La identidad social se percibe externamente, no confiando en la intención, sino en la expresión y percepción efectiva de la presentación de un individuo. Si bien la identidad social emerge de la identidad interna, su manifestación se lee a la luz del cuerpo que la transmite y de la situación en la que se transmite." (Boyd, 2001, p. 22), estas dimensiones no son independientes entre sí, sino que están interconectadas y se superponen, creando una representación compleja y multifacética de la persona. La web 2.0 también introdujo conceptos como la co-creción de contenido y la participación del usuario, lo que permitió a las personas no solo consumir información en línea, sino también contribuir activamente a su creación y difusión. Esto llevó a una mayor personalización y contextualización de la identidad digital, ya que los usuarios podían expresar sus intereses, opiniones y valores a través de contenido generado por el usuario, comentarios y participación en debates en línea.

"Fundamentalmente, la interacción social es una negociación entre individuos que actúan dentro de un contexto social particular para transmitir aspectos de su identidad. Esta negociación a menudo ocurre con poca reflexión consciente; Las personas interactúan

cómodamente entre sí, revelando lo que es apropiado mientras evalúan qué información se les está dando." (Boyd, 2001, p. 20).

Esta comprensión subyacente de la interacción social se ha trasladado al mundo digital con el surgimiento de la Identidad Digital. Al igual que en la interacción cara a cara, las personas negocian y transmiten aspectos de su identidad a través de plataformas en línea, desde perfiles de redes sociales hasta foros de discusión y aplicaciones de mensajería instantánea. Sin embargo, en el contexto digital, esta negociación de identidad puede ser más consciente y estratégica, ya que los usuarios pueden tener más control sobre qué información comparten y cómo se presentan en línea.

La evolución de la Identidad Digital ha ampliado las posibilidades de expresión y conexión en línea, pero también ha planteado nuevos desafíos en términos de autenticidad y privacidad. Según las personas navegan por un paisaje digital cada vez más complejo y diverso, la gestión de la identidad en línea es esencial. Los usuarios deben equilibrar la autenticidad con la privacidad y la seguridad, navegando hábilmente entre la revelación selectiva de información personal y la protección contra riesgos potenciales como el robo de identidad y el acoso en línea.
En este sentido, la Identidad Digital no solo refleja quiénes somos en línea, sino que también influye en cómo nos percibimos a nosotros mismos y cómo somos percibidos por los demás en el ecosistema digital. Esta interacción dinámica entre identidad personal y contexto social en línea es fundamental para comprender la evolución continua de la Identidad Digital y su impacto en la sociedad contemporánea.

La aparición de dispositivos móviles y la conectividad omnipresente han ampliado aún más el alcance y la influencia de la Identidad Digital en la sociedad contemporánea. La proliferación de aplicaciones y servicios en línea ha facilitado la expresión y la gestión de la identidad personal, profesional y social en una variedad de contextos y plataformas. La movilidad proporcionada por los dispositivos móviles ha permitido conectar a las personas en todo momento, lo que ha generado una mayor integración de la identidad digital en la vida cotidiana.

Además, la evolución de la Identidad Digital ha estado marcada por la creciente preocupación por la privacidad y la seguridad en línea. Los escándalos de violación de datos y la recopilación masiva de información personal han llevado a un mayor escrutinio sobre cómo se manejan y protegen los datos de identidad en el ciberespacio. Este enfoque renovado en la privacidad ha llevado a la adopción de regulaciones como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea y la creciente demanda de herramientas y prácticas que empoderen a los usuarios para controlar su identidad digital de manera más efectiva.

IV. INFLUENCIA DE LA IDENTIDAD DIGITAL EN LA SEGURIDAD

La gestión de identidad es una plataforma tecnológica que permite la identificación y verificación de personas o computadoras, así como el procesamiento de personas, de propiedad sobre físicas. u objetos virtuales y sobre todos los demás recursos imaginables.

La preocupación por los riesgos de privacidad en línea creó una necesidad sustancial de medir la privacidad con preguntas como ¿quién es usted?, ¿qué hace en Internet? Los riesgos de identidad pueden causarse por múltiples vías en línea, siendo las redes sociales un principal motivo de preocupación. otro motivo de preocupación son los ciberataques ya que estos pueden combinarse entre el ataque digital y el físico generando como consecuencias en muchas ocasiones la filtración de secretos,

como información de tarjetas, cuentas bancarias etc...

Debido a esto y puesto que la identidad digital se asocia directamente con los individuos un punto a favor es la gobernanza de servicios digitales de todo tipo, en donde encontramos la ciberseguridad la cual se clasifica en tres categorías:

- Categoría A1: Vigilancia y recopilación de inteligencia
- Categoría A2: Manipulación personalizada y disrupción
- Categoría A3: Explotación masiva o interrupción de servicios

Además de estas categorías existen ciertas leyes, regulaciones y marcos de privacidad creados con el fin de proteger lo digital, Con el surgimiento de estas reglas y regulaciones, la gente carece de la conciencia de lo que hacen estas reglas y contra qué tipo de riesgos ayudan a protegerlos (Sullivan,2018). El marco, NIST 800-63-3, en el que se explica la identidad digital y sus atributos fue creado para ser utilizado como guía para gestionar la identidad digital y los mecanismos de autenticación. Este marco define la identidad digital. así como sus atributos y estándares mínimos tecnológicos. (NIST, 2017)

A. DEFINCIONES

Autentificación: es el acto o proceso de confirmar que algo (o alguien) es quien dice ser. A la parte que se identifica se le llama probador. A la parte que verifica la identidad se la llama verificador.

Contraseña: o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña.

Gestión de identidad: utiliza un sistema integrado de políticas y procesos organizacionales para facilitar y controlar el acceso a sistemas de información y sus instalaciones.

Identidad: es asociada al individuo, identifica al individuo de manera única, esta puede ser física o digital. (University of south Florida, noviembre 2020)

Privacidad: la privacidad en identidad digital es entendida como la libertad de acceso no autorizado a los datos personales de la persona. (University of south Florida, noviembre 2020)

Seguridad: es la práctica o proceso de protección y recuperación de sistemas, redes, dispositivos y programas informáticos ante cualquier tipo de ciberataque.

V. TECNOLOGIA ACTUALIZADA Y RECURSOS

Producto de la unión de herramientas y sistemas para asegurar la veracidad de datos dentro de una organización lo que permite contar con soluciones como la autenticación multifactorial, la gestión de accesos privilegiados (PAM), el análisis de comportamiento del usuario (UBA) y la inteligencia artificial aplicada a la seguridad, entre otros. Estas herramientas permiten una protección robusta contra las amenazas cibernéticas en constante evolución y son fundamentales para mantener la integridad, disponibilidad y confidencialidad de los datos; los recursos hacen referencia a los elementos tangibles e intangibles necesarios para implementar y mantener las soluciones de

seguridad; estos recursos incluyen personal especializado en seguridad de la información, presupuesto para adquirir y mantenerlos, tiempo dedicado a la configuración y administración de sistemas, y políticas y procedimientos claros de seguridad de la información. Sin estos recursos, incluso la mejor tecnología actualizada puede no ser efectiva para proteger la identidad y los datos de una organización por ello van de la mano en este importante ítem formando un enfoque integral para proteger la identidad y los datos en el entorno digital actual.

VI. GESTIÓN DE ATAQUES CIBERNÉTICOS

Los ataques cibernéticos dirigidos a la gestión de identidades han experimentado un incremento alarmante. Según el informe “2023 Trends in Securing Digital Identities” de la Identity Defined Security Alliance (IDSA), se descubrió que el 90% de las organizaciones fueron víctimas de al menos una violación de seguridad vinculada a identidades digitales en el último año. Estos ataques se enfocan en comprometer las identidades digitales de individuos, organizaciones o entidades.

Los ataques de identidad se caracterizan por su objetivo de secuestro, suplantación y mal utilización de la información de identidad, como nombres de usuario, nombres de dominio, correos electrónicos, contraseñas, datos personales o certificados digitales. Los ciberdelincuentes explotan las vulnerabilidades para obtener acceso no autorizado a sistemas, datos o recursos.

Un caso ilustrativo de un ciberataque a la. gestión de identidad es el de IFX una empresa líder telecomunicación, infraestructura red y servidores, que sufrió un ataque cibernético de mayor envergadura de lo que se informó inicialmente. Los atacantes extrajeron datos de todos los usuarios abarcando sectores de la salud, universidades, empresas públicas, privadas; entre otras. Este incidente resalta la importancia de la seguridad en la gestión de identidades y la necesidad de implementar medidas de prevención y mitigación efectivas.

El desconocimiento de la gestión de ciberataques y del flujo de proceso que sigue un ataque para materializarse puede ser un factor de riesgo significativo. Según el concepto de Cyber Kill Chain, el ciclo de vida de un ciberataque consta de varias etapas, desde el reconocimiento hasta la ejecución del ataque. Si se interrumpe el ataque en cualquiera de estas etapas, se rompe la secuencia de este y este queda bloqueado. Sin embargo, si los usuarios o los responsables de la ciberseguridad desconocen este proceso, pueden no estar preparados para detectar y responder adecuadamente a los ataques.

La capacitación en ciberseguridad es esencial para fortalecer las defensas de una organización y protegerla de las amenazas cibernéticas. Los colaboradores bien informados y capacitados son mucho menos propensos a caer en trampas cibernéticas y cometer errores que puedan comprometer la seguridad de la empresa. La formación en concientización de ciberseguridad tiene como objetivo tener buenas prácticas y aviso de situaciones sospechosas en tiempo real.

La detección temprana de los ciberataques y una respuesta rápida son cruciales para minimizar el impacto y limitar la propagación del ataque y las consecuencias que tiene. La implementación de herramientas de monitoreo de seguridad, análisis de comportamiento y detección de amenazas en tiempo real permite identificar y responder proactivamente a las actividades sospechosas, reduciendo el tiempo de exposición y mitigando el daño potencial.

Ante la creciente sofisticación de los ciberataques al ser ya no tanto por atacantes individuales si no por organizaciones bien

organizadas y financiadas, la colaboración entre las organizaciones en la comunidad de ciberseguridad se vuelve cada vez más importante. Compartir información sobre amenazas (que ya las empresas encargadas de los antivirus en menor medida), tácticas de ataque y mejores prácticas de seguridad permiten a las organizaciones fortalecer sus defensas colectivas y estar mejor preparadas para enfrentar las amenazas cibernéticas en evolución.

VII. Conclusiones

La gestión de identidad es crucial en el mundo digital actual debido al aumento de las transacciones en línea y la exposición constante de información personal y empresarial. La implementación de soluciones modernas respaldadas por tecnologías avanzadas como la biometría y la autenticación multifactorial es fundamental para proteger la integridad y seguridad de los sistemas. Además, es importante adaptar continuamente las estrategias de gestión de identidades para hacer frente a las nuevas amenazas cibernéticas y cumplir con las regulaciones de privacidad de datos.

Referencias

Ciberataques. Guía para la gestión y notificación de ataques informáticos. (2021, April 7). Ciberseguridad. https://ciberseguridad.com/ciberataques/

Flores, C. (2023, November 29). Ciberataques y el Modelo de la Cyber Kill Chain: Comprendiendo las Fases del Ataque Cibernético. Asperis Security. https://www.asperis.es/blog/cyber-kill-chain-ciberataque/

identity management (ID management). (2024, April 11). Security; TechTarget. https://www.techtarget.com/searchsecurity/definition/identity-management-ID-management

Inicio de sesión único - IBM® Security Verify. (n.d.). Ibm.com. Retrieved May 9, 2024, from https://www.ibm.com/es-es/products/verify-saas/single-sign-on

ISO 27002 punto por punto A9 Control de acceso - Caso Práctico. (2019, February 9). Norma ISO 27001. https://normaiso27001.es/a9-control-de-acceso/

jaiderospina. (n.d.). Articulo/ArticulosConsulta at main · jaiderospina/DEVSECOPS2024.

¿Qué es la capacitación de concientización sobre seguridad y por qué es importante? (2024, March 27). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-security-awareness-training

¿Qué es la gestión de identidades y accesos? Definiciones IAM, SSO, MFA e IDaaS. (2023, May 10). Ibm.com. https://www.ibm.com/es-es/topics/identity-access-management

¿Qué es la tríada CIA y por qué es importante? (n.d.). Fortinet. Retrieved May 9, 2024, from https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

(N.d.). Arcgis.com. Retrieved May 9, 2024, from https://enterprise.arcgis.com/es/portal/latest/administer/windows/roles.html

VIII. CONCLUSION

La Identidad Digital es el modelo virtual de una persona en Internet, esencial en la vida moderna, y su gestión garantiza que solo personas autorizadas accedan a recursos críticos. Las herramientas de ciberseguridad y campañas de concientización son fundamentales para prevenir ciberataques y proteger la información. La evolución de la Identidad Digital ha pasado de ser estática a dinámica, con redes sociales y participación activa. Esto ha creado desafíos en autenticidad y privacidad. La gestión de identidad abarca políticas, roles de usuario, revisiones y protección de datos para prevenir ataques cibernéticos. La ISO 27001 y el Marco de Ciberseguridad del NIST son fundamentales. La seguridad se refuerza con autenticación multifactorial, PAM, análisis de comportamiento y colaboración en la comunidad de ciberseguridad. Los ciberataques aumentan, pero la capacitación y la detección temprana son clave para enfrentarlos.