ARTICULO IDENTIDADES DIGITALES
ARTICLE DIGITAL IDENTITIES

Duver Salgado Rojas
dsalgadoroj@uniminuto.edu.co
Johan Salinas Acosta
jsalinasac1@uniminuto.edu.co
Harold Cerquera Saez
hcerquerasa@uniminuto.edu.co
Jhoan Montealegre Romero
jhoan.montealegre-r@uniminuto.edu.co
Pedro Julio Orozco Obregoso
porozcoo@uniminuto.edu.co

Universidad Minuto De Dios
Bogotá D.C.
Colombia

***Resumen*—**El grupo realizó un análisis exhaustivo sobre la temática central de la Identidad Digital, centrándose en un enfoque discursivo. Adicionalmente subrayó la importancia del uso cuidadoso y meditado de los datos personales en línea, teniendo en cuenta aspectos como la privacidad, la seguridad y la autenticidad. Es importante resaltar la necesidad de que los usuarios sean conscientes de cómo establecer y proteger su identidad digital en un entorno cada vez más conectado y arriesgado. El documento IEE abordara diferentes temáticas y cuestiones clave, ofreciendo una visión general del estado actual de la identidad digital y sus implicaciones futuras.

***Palabras clave*—** Identidad, anonimato, seudonimato, identidad digital, autenticación, custodia de identidad, información biométrica, transacción, conjunto de anonimato, anonimato del remitente, anonimato del destinatario, transacción no vinculable, credencial, sistema de credenciales seudónimas, infraestructura de clave pública (PKI), certificado de clave pública, certificado de atributos, sistema de firma colectiva, gestión de identidad, tarjeta de identidad electrónica, privacidad, privacidad informativa, legislación sobre protección de datos y Directiva de la UE sobre protección de datos

***Abstract*—**The group conducted an exhaustive analysis on the central theme of Digital Identity, focusing on a discursive approach. It also stressed the importance of careful and thoughtful use of personal data online, taking into account aspects such as privacy, security and authenticity. It is important to highlight the need for users to be aware of how to establish and protect their digital identity in an increasingly connected and risky environment. The IEE paper will address different themes and key issues, providing an overview of the current state of digital identity and its future implications.

***Keywords*—**Identity, anonymity, pseudonymity, digital identity, authentication, identity escrow, biometric information, transaction, anonymity set, sender anonymity, recipient anonymity, non-bindable transaction, credential, pseudonymous credential system, public key infrastructure (PKI), public key certificate, attribute certificate, collective signature system, identity management, electronic identity card, privacy, informational privacy, data protection legislation, EU Data Protection Directive

I. INTRODUCCIÓN

En la era digital, la Identidad Digital se ha convertido en un tema central que abarca múltiples facetas de la vida moderna. Desde la forma en que nos presentamos en las redes sociales hasta cómo protegemos nuestra información personal en línea, la identidad digital juega un papel fundamental en la forma en que interactuamos y nos relacionamos en el ciberespacio. Este concepto abarca no solo la información que compartimos en línea, sino también cómo nos percibimos a nosotros mismos y cómo los demás nos perciben a través de nuestras actividades en la web.

Explorar la identidad digital implica adentrarse en un universo complejo donde la privacidad, la autenticidad y la reputación se entrelazan de manera intrincada. ¿Cómo construimos y gestionamos nuestra identidad en un entorno digital en constante evolución? ¿Qué impacto tiene nuestra presencia en línea en nuestras relaciones personales, profesionales y en nuestra propia percepción de nosotros mismos? Estas son preguntas que invitan a la reflexión y a la exploración de los diversos aspectos de la identidad digital.

Desde la creación de perfiles en redes sociales hasta la gestión de nuestra huella digital, la identidad digital no solo

refleja quiénes somos, sino también nuestras aspiraciones, miedos y valores en el mundo en línea. Adicionalmente es importante mencionar que en la era de la sociedad de la información, el gobierno electrónico también va a emerger como una transformación crucial en la administración pública, esta evolución implica procesos más dinámicos y centrados en el ciudadano, marcando un cambio hacia el Internet como plataforma principal de servicios. Otro tema es la emisión de tarjetas de identidad electrónica en varios países europeos que promete eficiencia en la prestación de servicios, aunque sus implicaciones en la privacidad generan interrogantes, por tal motivo es necsario abordar las inquietudes que van a impulsar el desarrollo de una identidad digital.

Por último, en este artículo nos embarcaremos en un viaje de reflexión sobre la Identidad Digital, explorando sus múltiples facetas, su impacto en la sociedad y las implicaciones éticas que conlleva. Es decir, abordaremos múltiples temas de la **gestión de identidad digital,** explorando el propósito principal y su impacto en la sociedad contemporánea.

II. IDENTIDAD ANONIMA

En el desarrollo del articulo exploraremos primero los conceptos de identidad digital, anonimato y seudonimato. Destacando la importancia de comprender estos términos para navegar por el mundo online.

A. Identidad

Nos referimos a las características que definen a un individuo. Puede desglosarse en aspectos internos (autopercepción) y externos (cómo te perciben los demás). La identidad es dinámica y evoluciona con el tiempo.

B. Identificación

Este proceso establece la identidad de una persona utilizando características únicas. Los métodos tradicionales incluyen la apariencia física, la fecha de nacimiento y los números de la seguridad social. Cada vez se utilizan más los datos biométricos, como las huellas dactilares y el ADN.

C. Anonimato

Se refiere al estado de no ser identificado. En el mundo digital, el anonimato puede aplicarse a los usuarios, la comunicación o las transacciones. Los conjuntos de anonimato se refieren al grupo de usuarios potenciales a los que podría atribuirse una acción. Un anonimato más fuerte viene con conjuntos de anonimato más grandes.

D. Seudonimato

Su utilización de un nombre falso como identificador. Los seudónimos permiten a los usuarios crearse una reputación en Internet sin revelar su identidad real. Las subastas en línea son un ejemplo común en el que los usuarios interactúan bajo seudónimos.

Es importante destacar que el presente artículo quiere dar a distinguir entre anonimato y seudonimato. El anonimato no permite vincular las transacciones a un único usuario. Los seudónimos, en cambio, permiten a los proveedores de servicios conectar transacciones en las que interviene el mismo seudónimo, lo que posibilita la creación de reputación.

Finalmente, se explora el concepto de anonimato revocable como una solución para situaciones en las que se requiere responsabilidad, incluso en entornos de anonimato. Se destaca cómo este enfoque equilibra la privacidad con la rendición de cuentas en el mundo digital en constante evolución.

III. IDENTIDAD DIGITAL

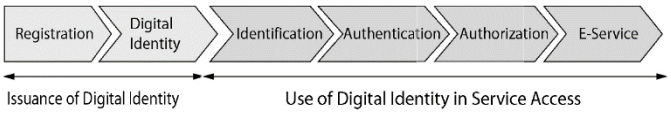
En el mundo digital, definir la identidad se torna tan complejo como definir la identidad humana misma. A grandes rasgos, la identidad digital se concibe como una representación de la identidad humana legible por máquinas, utilizada en sistemas electrónicos para interactuar con máquinas o personas locales o remotas. Su función principal es habilitar el control de acceso y vincular una transacción o conjunto de datos en un sistema de información con un individuo identificable. La identidad digital permite identificar, autenticar y autorizar a los usuarios para acceder a recursos o servicios específicos. La seguridad de un sistema de información depende en gran medida de la capacidad para identificar y autenticar a los usuarios.

Las identidades digitales también pueden ser anónimas, seudónimas, identificativas o de grupo. Una identidad anónima no puede vincularse en absoluto a un identificador, mientras que una transacción seudónima puede ser vinculada por un proveedor de servicios a un seudónimo, pero no a un individuo identificable. Por último, las identidades digitales son necesarias para identificar a los usuarios y autorizarles a acceder a los recursos (o servicios) de un sistema. Antes de conceder a un usuario con identidad digital el acceso a un servicio, deben realizarse varias etapas de procesamiento, como el registro, la identificación, la autenticación y la autorización.

Otro tema fundamental es el contexto del acceso a servicios electrónicos, la importancia de las identidades digitales radica en su capacidad para identificar a los usuarios y concederles acceso a los recursos o servicios dentro del sistema correspondiente. Este proceso típicamente implica la adquisición de una identidad digital, la verificación de la identidad del usuario y la autorización para acceder al servicio específico. Los sistemas de control de acceso pueden presentar una estructura centralizada o descentralizada, y la forma de autenticación puede variar, ya sea a través de dispositivos físicos o mediante información privada conocida únicamente por el usuario.

En síntesis, se puede afirmar que la identidad digital emerge como un componente fundamental en el contexto actual de la era digital, presentando implicaciones de gran relevancia en

términos de seguridad, privacidad y la vivencia del usuario en el entorno en línea. La comprensión y el manejo eficiente de esta dimensión son esenciales para asegurar operaciones seguras y resguardar la confidencialidad de las personas en el ámbito digital.



IV. IDENTIDAD DIGITAL EXTENDIDA

En la era actual, diversos países europeos están inmersos en iniciativas dirigidas a la implementación de tarjetas de ciudadanía digital. Estos dispositivos, que principalmente almacenan información relacionada con la identidad del titular mediante certificados X.509, tienen como principal objetivo proporcionar una identificación sólida del ciudadano. No obstante, se señala que el enfoque actual de estas tarjetas es estático, lo que impide la posibilidad de añadir o gestionar información adicional para reflejar de manera dinámica la identidad del individuo.

Adicionalmente, se plantea la preocupación de que este enfoque pueda comprometer la privacidad del ciudadano, especialmente dado que muchas de estas tarjetas son utilizadas en una amplia variedad de aplicaciones, tanto en el ámbito público como privado. Esto facilita la vinculación de transacciones y la identificación del titular de la tarjeta, lo que podría representar una amenaza para la privacidad del individuo.

A. Puntos Primordiales

- El enfoque actual de las tarjetas de ciudadano digital es estático, ofrece una funcionalidad limitada y tiene el potencial de invadir la privacidad del usuario.
- El concepto propuesto introduce nuevos elementos en la identidad digital, incluidas las credenciales seudónimas, para permitir a los usuarios acceder a los servicios de forma anónima.
- El concepto propuesto también introduce nuevas funcionalidades en las tarjetas de ciudadano para gestionar estos elementos, como la gestión de credenciales y la gestión de información de identidad.
- El objetivo general del concepto propuesto es proporcionar una identidad digital más completa y protectora de la privacidad para las aplicaciones de gobierno electrónico.

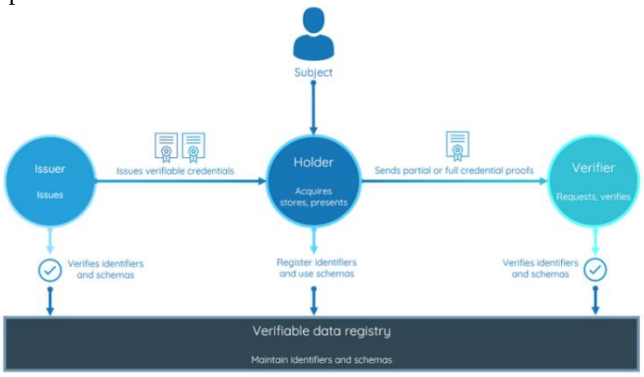
V. INFRAESTRUCTURA EMISOR DE CREDENCIALES

En el ámbito de la infraestructura de emisión de credenciales, las organizaciones desempeñan un papel vital al establecer identidades alternativas para los individuos y proporcionarles credenciales. Estas credenciales validan afirmaciones sobre un individuo, generalmente relacionadas con las operaciones comerciales de una organización. Por ejemplo, el departamento de registro de población podría actuar como emisor de una credencial anónima que verifica la edad de un ciudadano. Sin embargo, para funcionar como emisor de credenciales, una organización necesita integrar componentes adicionales en sus sistemas de información existentes.

Estos componentes son fundamentales para emitir credenciales y difundir información relevante tanto para los usuarios como para las partes confiables. La infraestructura de un emisor de credenciales incluye un administrador de registro y certificación de credenciales, un administrador de revocación de anonimato y una base de información de credenciales. Esta última publica información significativa para las partes confiables y los individuos, que abarca políticas y prácticas de credenciales, listas de revocación y claves públicas del emisor.

El administrador de registro y certificación de credenciales tiene la responsabilidad de registrar a los ciudadanos y otorgarles credenciales. Durante el proceso de registro, se asigna un seudónimo a cada individuo y se verifican las condiciones necesarias para emitir una credencial específica. La organización mantiene una base de datos que detalla los seudónimos y credenciales asignados a cada ciudadano, junto con los protocolos de emisión correspondientes. Esta entidad desempeña un papel similar al de una autoridad de certificación en una infraestructura de clave pública.

Por otro lado, la base de información de credenciales ofrece detalles sobre la emisión, gestión y revocación de credenciales, dirigidos tanto a los usuarios finales como a las partes confiables. Además de describir las credenciales y sus políticas, esta base incluye guías dirigidas a los ciudadanos para comprender el proceso de manejo de credenciales y sus implicaciones.



VI. ESQUEMAS DE GESTIÓN DE ACCESO E IDENTIDAD UTILIZABLES PARA CIUDADES INTELIGENTES

Se destaca la relevancia de los esquemas de gestión de identidad y acceso (IAM) utilizables para supervisar y controlar las identidades y los privilegios de acceso de los usuarios en el contexto de una ciudad inteligente segura.

Se subraya que cualquier vulnerabilidad en infraestructuras críticas, como soluciones financieras inteligentes, transporte inteligente y edificios inteligentes, podría interrumpir la vida cotidiana de los residentes.

A. Debilidades de los esquemas de verificación tradicionales

- Se señala que los esquemas de verificación basados en el conocimiento y los tokens son susceptibles a diversos tipos de ataques, como la ingeniería social, la fuerza bruta, la observación y la suplantación
- Se enfatiza que las contraseñas débiles continúan siendo la causa principal de ataques de botnets y denegación de servicio.
- Se indica que estos mecanismos tradicionales no cumplen con los requisitos de usabilidad de los usuarios finales.

B. Ventajas de los esquemas biométricos

- Se resalta que los esquemas biométricos pueden superar las limitaciones de seguridad y usabilidad de los esquemas tradicionales
- Se describe cómo la autenticación basada en características biológicas y de comportamiento únicas de un individuo ofrece una mayor seguridad al evitar vulnerabilidades como el compartir, robar o adivinar información de identificación.

C. Esquemas IAM propuestos

- Se presentan diferentes esquemas IAM diseñados para distintos contextos: Hold & Tap para soluciones financieras inteligentes, DriverAuth para transporte inteligente y Step & Turn para edificios inteligentes.
- Se detalla cómo estos esquemas utilizan métodos de autenticación basados en características biométricas y de comportamiento para mejorar la seguridad y la usabilidad.

D. Seudonimato

- Se menciona la necesidad de realizar un análisis exhaustivo de seguridad contra diversos ataques.
- Se discuten los factores que pueden afectar la efectividad de los rasgos biométricos.
- Se destaca la importancia de contar con conjuntos de datos demográficos amplios y un control de calidad adecuado de las plantillas biométricas.

Ya para concluir en la actualidad de las ciudades inteligentes, se considera fundamental garantizar la seguridad de los sistemas, se han diseñado esquemas de autenticación basados en biometría, como Hold & Tap, DriverAuth y Step & Turn, para aplicaciones financieras, transporte y edificios inteligentes respectivamente.

Hold & Tap ofrece la posibilidad de ingresar texto alfanumérico aleatorio para acceder a aplicaciones seguras, utilizando los tiempos de toque y los movimientos de mano como medida de seguridad. Por su parte, DriverAuth verifica la identidad de los conductores antes de asignarles nuevos viajes, garantizando la seguridad en el transporte. Mientras tanto, Step & Turn simplifica el acceso a edificios inteligentes al analizar los comportamientos únicos al caminar y girar.

Estos avances en seguridad son cruciales para salvaguardar la privacidad y la integridad de los datos en entornos urbanos digitales. Al integrarse con plataformas en la nube y sistemas de gestión de identidad en línea, estas soluciones refuerzan la seguridad en las ciudades inteligentes, proporcionando una experiencia de usuario segura y sin complicaciones.

VII. Integración de Perspectivas de Investigación Adicionales

A. "Digital identity for development: The quest for justice and a research agenda"

El artículo "Digital identity for development: The quest for justice and a research agenda" aborda la identidad digital desde la perspectiva del desarrollo y la justicia social. En este contexto, se destaca la importancia de considerar cómo las identidades digitales pueden influir en la inclusión social y económica de comunidades marginadas. Además, el artículo propone una agenda de investigación que enfatiza la necesidad de investigar más a fondo temas como la privacidad, la seguridad y la equidad en el ámbito de la identidad digital.

Esta perspectiva amplía nuestra comprensión de la identidad digital al resaltar su impacto en el desarrollo humano y la igualdad de oportunidades. Por ejemplo, investigaciones adicionales podrían explorar cómo las identidades digitales pueden facilitar el acceso a servicios básicos como la educación y la salud en regiones desfavorecidas. Además, se podría examinar cómo las políticas de identidad digital pueden diseñarse de manera que protejan los derechos y la dignidad de los individuos, especialmente en contextos donde la falta de identificación puede excluir a las personas de los beneficios sociales y económicos.

B. "Identity Management as a target in cyberwar"

El artículo "Identity Management as a target in cyberwar" arroja luz sobre los desafíos de seguridad asociados con la gestión de identidad en entornos digitales. En particular, destaca cómo la gestión de identidad puede convertirse en un objetivo en conflictos cibernéticos, lo que subraya la importancia de proteger las infraestructuras de identidad digital contra posibles ataques. Este enfoque resalta la intersección entre la seguridad cibernética y la gestión de identidad, y enfatiza la necesidad de diseñar sistemas de identidad digital que sean resistentes a las amenazas cibernéticas.
La perspectiva presentada en este artículo complementa nuestra comprensión de la identidad digital al destacar los riesgos de

seguridad asociados con su implementación. Por ejemplo, las ciudades inteligentes, que dependen en gran medida de sistemas de identidad digital para ofrecer servicios eficientes, podrían ser vulnerables a ataques cibernéticos dirigidos a comprometer estas infraestructuras. Por lo tanto, es crucial que los diseñadores de sistemas de identidad digital consideren cuidadosamente las implicaciones de seguridad y adopten medidas proactivas para proteger estos sistemas contra posibles amenazas.

VIII. APROVECHANDO LOS JUEGOS SERIOS PARA MEJORAR LA CONCIENCIACIÓN SOBRE LA SEGURIDAD DEL SOFTWARE

En La seguridad del software es una preocupación creciente en el mundo tecnológico actual. Con la creciente complejidad de los sistemas informáticos y la constante evolución de las amenazas cibernéticas, es crucial que los desarrolladores de software y los profesionales de TI estén bien informados y preparados para abordar los desafíos de seguridad.

Un enfoque innovador para mejorar la conciencia de seguridad del software es el uso de juegos serios. Estos juegos no solo son educativos, sino que también son divertidos y atractivos, lo que los convierte en una herramienta efectiva para enseñar conceptos complejos de seguridad de manera accesible y práctica.

En un estudio reciente publicado en ResearchGate, titulado "Mejorando la Conciencia de Seguridad de Software Utilizando un Juego Serio", los investigadores exploran cómo un juego serio puede ser utilizado para mejorar la conciencia y comprensión de la seguridad del software entre los profesionales de TI y los desarrolladores de software.

El juego serio presenta situaciones realistas de seguridad del software y desafíos a los jugadores a tomar decisiones que afecten la seguridad de un sistema. Al interactuar con el juego, los jugadores desarrollan un mejor entendimiento de las vulnerabilidades comunes del software, las mejores prácticas de seguridad y las técnicas de mitigación.

Los resultados del estudio sugieren que el uso de juegos serios puede tener un impacto positivo en la conciencia de seguridad del software. Los participantes que jugaron el juego mostraron un aumento significativo en su conocimiento de seguridad del software y una mayor disposición para aplicar prácticas de seguridad en su trabajo diario.

Este estudio destaca el potencial de los juegos serios como una herramienta efectiva para mejorar la conciencia de seguridad del software y abordar las brechas de conocimiento en este campo. Como la seguridad del software sigue siendo una prioridad en la era digital, es importante explorar y aprovechar nuevas y creativas estrategias educativas como los juegos serios.

IX. EXPLORANDO LA INTERSECCIÓN DE LA INTELIGENCIA ARTIFICIAL Y LA ÉTICA EN LA TOMA DE DECISIONES EMPRESARIALES

En un mundo cada vez más digitalizado, la integración de la inteligencia artificial (IA) en los procesos empresariales está en aumento. Sin embargo, a medida que las organizaciones adoptan tecnologías de IA para optimizar la eficiencia y mejorar la toma de decisiones, surgen importantes cuestionamientos éticos que deben abordarse.

Un estudio reciente publicado en Springer, titulado "Explorando la Intersección de la Inteligencia Artificial y la Ética en la Toma de Decisiones Empresariales", arroja luz sobre esta compleja interacción. Los investigadores examinan cómo las decisiones empresariales impulsadas por la IA pueden influir en consideraciones éticas clave, como la equidad, la transparencia y la responsabilidad.

La investigación destaca que si bien la IA tiene el potencial de mejorar significativamente la precisión y la velocidad de las decisiones empresariales, también plantea desafíos éticos importantes. Por ejemplo, los algoritmos de IA pueden estar sesgados, reflejando y amplificando prejuicios humanos subyacentes, lo que lleva a decisiones discriminatorias o injustas.

El estudio aborda la necesidad de desarrollar marcos éticos sólidos para guiar el desarrollo y la implementación de sistemas de IA en entornos empresariales. Esto incluye la promoción de la equidad algorítmica, la transparencia en los procesos de toma de decisiones y la rendición de cuentas por los resultados generados por la IA.

Además, se destaca la importancia de la colaboración multidisciplinaria entre expertos en IA, ética, derecho y ciencias sociales para abordar de manera efectiva los desafíos éticos emergentes en este campo. Solo a través de un enfoque holístico y colaborativo, las organizaciones pueden garantizar que la IA se utilice de manera ética y responsable en el ámbito empresarial.

Este estudio ofrece una visión perspicaz sobre la compleja intersección entre la inteligencia artificial y la ética en la toma de decisiones empresariales. En un mundo donde la tecnología avanza rápidamente, es fundamental abordar estos problemas éticos para garantizar un uso ético y equitativo de la IA en el entorno empresarial.

X. OPTIMIZACIÓN DE LA EFICIENCIA ENERGÉTICA EN EDIFICIOS RESIDENCIALES UTILIZANDO BLOCKCHAIN

En el artículo "¿Blockchain para la gestión de la identidad? Una perspectiva filosófica, legal y técnica", se analiza la gestión de la identidad como un recurso en el contexto de la identidad digital y el blockchain. El artículo explora diversos temas, incluyendo:

- Perspectivas filosóficas sobre la identidad:

Se examinan las diferentes concepciones de la identidad a lo largo de la historia, desde las perspectivas individualistas hasta las colectivistas.

- Aspectos legales de la identidad:

Se analizan los marcos legales existentes para la gestión de la identidad, destacando los desafíos y las oportunidades que presenta la era digital.

- Casos de identidad digital:

Se presentan ejemplos concretos de cómo se utiliza la identidad digital en diversos sectores, como la banca, la atención médica y el gobierno.

- Tecnologías emergentes:

Se discuten las tecnologías emergentes como "Distributed Ledger Technology" (DLT) y "Zero Knowledge Proof" (ZKP) y su potencial para transformar la gestión de la identidad.

- Hacia una identidad auto-soberana

Adicionalmente, la gestión de la identidad digital se está transformando en un servicio básico, y que las tecnologías blockchain podrían desempeñar un papel crucial en este proceso. Se introduce el concepto de "identidad auto-soberana", en la que los individuos tienen un mayor control sobre sus datos personales.

En última instancia, el artículo se describe un futuro en el que las personas podrían tener un mayor control sobre su identidad digital gracias a las nuevas tecnologías, como el blockchain. Esto podría conducir a una sociedad más justa y equitativa, donde los individuos tengan más autonomía sobre sus datos y su privacidad.

XI. ANÁLISIS COMPARATIVO DE TÉCNICOS Y JURÍDICOS MARCOS DE VARIOS DIGITAL NACIONALES SOLUCIONES DE IDENTIDAD

En Un sistema nacional de identidad digital se ha convertido en un requisito clave para un fácil acceso a los servicios públicos en línea, especialmente durante la pandemia de Covid-19. Aunque muchos países han adoptado sistemas nacionales de identificación digital, muchos todavía están en el proceso de establecerlos. A través de un análisis comparativo de los aspectos técnicos y legales de varias soluciones nacionales de identificación digital seleccionadas actualmente en uso en diferentes países, exploraremos la diversidad de tecnologías y arquitecturas, así como la importancia del marco legal de soluciones de identificación digital específicas. el rol de También muestra algunas cuestiones importantes relacionadas con la implementación de estas soluciones, cómo garantizar la soberanía nacional sobre las soluciones y cómo encontrar el equilibrio adecuado entre las necesidades de los sectores público y privado.

A. Antecedentes

La gestión de la identidad en línea ha evolucionado con el tiempo, desde simplemente usar nombres de usuario y correos electrónicos con contraseñas, hasta perfiles completos que incluyen presencia en línea, actividades y contenido que ayudan a definir la identidad. Esto ha llevado a la recopilación y procesamiento de más datos personales, lo que plantea desafíos en cuanto a cómo se utilizan, procesan y almacenan estos datos. Aunque la Internet inicialmente carecía de estándares para identificar a los usuarios, la anonimidad ha sido una característica importante que ha permitido el éxito de las comunidades en línea. Sin embargo, la libertad en Internet se ha convertido en una preocupación importante para los usuarios, y la legislación en todo el mundo refleja estas preocupaciones al proporcionar un marco legal para el procesamiento, intercambio y almacenamiento de datos personales por parte de los proveedores de servicios.

Un marco legal para la identidad en línea debe proteger la privacidad y al mismo tiempo brindar alguna forma de responsabilidad para prevenir delitos cibernéticos como el fraude, el discurso de odio y el terrorismo cibernético. Las decisiones tecnológicas para construir soluciones de identidad en línea deben equilibrarse con el marco legal. Esta lógica también se aplica a las soluciones nacionales de identidad digital. Proporciona a los usuarios un atributo de identidad digital confiable que se puede utilizar para realizar transacciones en línea de forma segura y privada, lo que permite el control del usuario, el seudónimo e incluso el anonimato en ciertos casos de uso médico.

B. Datos de gestión de identidad

Los datos de gestión de identidad para una persona natural abarcan una amplia gama de información, desde datos básicos hasta perfiles en redes sociales y comunidades en línea, datos biométricos y datos generados por actividades en internet. Estos datos se utilizan para identificar, autenticar y autorizar a la persona en cuestión, e incluyen elementos como identificadores, atributos y credenciales, así como factores de autenticación como contraseñas, claves privadas y características biométricas como huellas dactilares y reconocimiento facial.

C. Datos Personales

Se describe que los datos personales comprenden toda información relacionada con una persona identificada o identificable, incluyendo identificadores como nombre, números y datos biométricos, entre otros. Se menciona que en otras legislaciones se denominan Información Personal o Información Personalmente Identificable (PII). Además, la regulación eIDAS define los Datos de Identificación Personal (PID) como aquellos que posibilitan la identificación de una persona natural o jurídica. En resumen, tanto los PID como

cualquier otra información que permita identificar a una persona, directa o indirectamente, son considerados datos personales, incluyendo los datos de gestión de identidad.

D. Servicios electrónicos de confianza

Se define a los servicios electrónicos que se ocupan de verificar, crear y conservar firmas electrónicas, sellos, certificaciones de sitios web, marcas de tiempo electrónicas y servicios similares. Estos servicios fueron definidos inicialmente por el Parlamento Europeo y el Consejo Europeo en la Directiva sobre Firma Electrónica del 1999 y luego en el Reglamento eIDAS. Según este último, el proveedor de estos servicios se llama Proveedor de Servicios de Confianza (TSP). Si estos servicios cumplen con requisitos adicionales establecidos en el reglamento eIDAS, se consideran Servicios de Confianza Cualificados, y el proveedor se identifica como un Proveedor de Servicios de Confianza Cualificado (QTSP).

E. Nivel de garantía

El Nivel de Aseguramiento (LoA, por sus siglas en inglés) es el grado de confianza en una identidad digital reclamada o la certeza con la que se puede confiar en una afirmación sobre una identidad específica durante la autenticación. La regulación eIDAS define 3 niveles de aseguramiento para la identificación electrónica: bajo, sustancial y alto. LoA también es conocido como IAL (Nivel de Aseguramiento de Identidad) en otros marcos de referencia. Por ejemplo, el Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST) define diferentes IAL para la verificación de identidad, autenticación y federación. Se requieren diferentes niveles de LoA según la variedad de casos de uso.

XII. La necesidad de un sistema nacional Identidad digital Infraestructura.

La seguridad cibernética de los datos de atención médica es más crucial y compleja hoy en día que nunca. En los países del G20, más del 50% de los ingresos gubernamentales se destinan al gasto en atención médica, una cifra en aumento. Sin embargo, la accesibilidad en línea a los servicios de salud se ve restringida debido a la naturaleza delicada de los datos y nuestra falta de capacidad para proteger eficazmente la entrega de servicios en línea. Como resultado, muchas acciones que podrían realizarse en línea de manera más eficiente, como acceder a registros médicos o abrir una cuenta bancaria, se llevan a cabo en persona, a un costo mayor. Actualmente, solo los servicios más básicos y de bajo riesgo están disponibles en línea, y, aun así, enfrentan altos costos debido a violaciones de datos y restablecimiento de contraseñas. Este es un desafío global que afecta a comunidades en todo el mundo.

El sector de la salud es uno de los sectores más fragmentados de la economía, careciendo de una fuerza unificadora entre el gobierno, hospitales, médicos, laboratorios, investigadores, pacientes, fabricantes de dispositivos médicos y organizaciones de salud (como Servicios de Sangre de Canadá y la Sociedad Canadiense del Cáncer). De hecho, el enfoque de este problema como uno de topología en lugar de seguridad podría brindar valiosas ideas sobre la dirección a seguir.

XIII. IDENTIDAD DIGITAL UN RIESGO CENTRADO EN EL SER HUMANO.

La creciente preocupación por la seguridad cibernética en un mundo cada vez más digitalizado. Se señala que, en las últimas dos décadas, el comercio electrónico se ha convertido en una fuerza disruptiva en prácticamente todos los mercados. Se destaca el aumento del interés de los clientes por las compras en línea y cómo esto ha obligado a las empresas a adaptarse completamente a esta tendencia, con un aumento significativo en las ventas minoristas globales a través del comercio electrónico, alcanzando aproximadamente el 18% en 2020. Sin embargo, se reconoce que esta transición también ha traído consigo un aumento en los intentos de fraude, ya que los delincuentes pueden esconderse fácilmente detrás del anonimato en línea.

En respuesta a esto, se describe una iniciativa de la Unión Europea para reducir la desconfianza en el comercio electrónico mediante la creación de un sistema que vincule las identidades digitales de compradores y vendedores con sus identidades físicas, lo que ayudaría a prevenir el fraude y fortalecer la responsabilidad. Aunque esta iniciativa aún está en sus etapas iniciales, se reconoce la importancia de abordar los desafíos y desarrollar la resiliencia cibernética necesaria para protegerla de posibles ataques de actores maliciosos, como sindicatos criminales y hackers patrocinados por estados extranjeros.
Se realizo un estudio sobre el impacto personal del robo de identidad, destacando las experiencias y luchas de una víctima de robo de identidad. Este relato subraya la complejidad y el dolor involucrados en el proceso de recuperación después de que la identidad de una persona ha sido comprometida. Se enfatiza cómo las compañías y las instituciones gubernamentales a menudo ponen una carga adicional sobre las víctimas al exigirles que demuestren su identidad de manera exhaustiva, lo que contrasta con la facilidad con la que los delincuentes pueden obtener acceso a información privada.

Se concluye con una declaración de propósito, donde se establece que el objetivo principal del estudio es explorar la conciencia de las personas sobre los riesgos asociados con su identidad digital y desarrollar un entendimiento más profundo de cómo gestionar estos riesgos de manera efectiva. Se reconoce la importancia de escuchar la voz de las personas afectadas por la seguridad cibernética y se subraya la necesidad de combinar la rigurosidad académica con la relevancia práctica para abordar eficazmente estos desafíos en la era digital.

I. Referencias

A, A. (2017). Self-sovereign identity. Styria EGIZ GV AT. Obtenido de https://technology.a-sit.at/en/whitepaper-self-sovereign-identity/

Android: Motion sensors. (20 de 02 de 2022). Obtenido de https://developer.android.com/guide/topics/sensors

Ciobotaru, I. (16 de December de 2020). Medium. Obtenido de https://weeb0.medium.com/anonymous-and-authenticated-digital-identity-on-the-open-internet-1863fc4dc5db

Collins, R. C. (1998). ditor. Collins English Dictionary. Glasgow.

Data Breach Investigations Report (DBIR). (20 de February de 2022). Obtenido de https://enterprise.verizon.com/content

Francesco Buccafurri, G. L. (12 de January de 2023). Allowing privacy-preserving fog computing with digital identity assurance in remote clinical services. pág. https://www.inderscienceonline.com/doi/abs/10.1504/EG.2023.129413.

Glöckler, J. S. (2023). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. Business & Information Systems Engineering. Obtenido de https://doi.org/10.1007/s12599-023-00830-x

Goel, y. (29 de Jun de 2014). The New York Times. Obtenido de https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html

I. Pires, N. G.-R. (2016). From Data Acquisition to Data Fusion: A Comprehensive Review and a Roadmap for the Identification of Activities of Daily Living Using Mobile Devices.

Inc., R. D. (1997.). PKCS #11 - Cryptographic Token Interface. Obtenido de http://www.rsasecurity.com/rsalabs/pkcs/

Kwangjo, K. (2001). Berlin: editor, Public Key Cryptography. Proceedings of 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001, volume 1992 of Lecture Notes in Computer Science, pages 190–206. Springer, Berlin, 2001.

Kwangjo, K. (2003). Better Business Bureau. BBB On Line Privacy Seal. Obtenido de http://www.bbbonline.org/privacy/

Liang, X. a. (2021). A Survey on Security Attacks and Solutions in the IoT Network. En I. (. Engineers). Proceedings of the 11th Annual Computing and Communication Workshop and Conference (CCWC).

Lysyanskaya, J. C. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. Berlin: In Birgit Pfitzmann, editor, Advances in Cryptology - EUROCRYPT 2001, volume 2045 of Lecture Notes in Computer Science, pages 93–118. Springer, Berlin, 2001.

Oorschot, P. V. (s.f.). User authentication—passwords, biometrics and alternatives. En P. V. Oorschot, Proceedings of the Computer Security and the Internet (págs. 55-90). Cham: 2021.

Schwabe Gerhard, R. L. (12 de Aug de 2004). Anonymous digital identity in e-government. Obtenido de https://www.zora.uzh.ch/id/eprint/60504/

Suáre, M. F. (s.f.). Vista de Desarrollo de un Juego Formativo para Aportar a la Concienciación en Ciberseguridad al Personal de la Escuela Militar de Aviación (Emavi) "Marco Fidel Suárez" de la Fuerza Aérea Colombiana en la ciudad de Cali. Obtenido de Ciencia y Poder Aéreo. (s.f.).: https://publicacionesfac.com/index.php/cienciaypoderaereo/article/ view/577/751

William Yeoh, M. G. (2023). Improving National Digital Identity Systems Usage: Human-Centric Cybersecurity Survey. Journal of Computer Information Systems , https://www.tandfonline.com/doi/full/10.1080/08874417.2023.2251452.

Yasin, A. L. (2019). Improving software security awareness using a serious game. IET Software, 13(2), 159-169. . Obtenido de https://doi.org/10.1049/iet-sen.2018.5095

Young, C. G. (2002). Web-based Survey on Electronic Public Services. Obtenido de http://verdi.unisg.ch/org/idt/ceegov.nsf

Zwitter, A. G. (2020). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. Frontiers In Blockchain, 3. Obtenido de https://doi.org/10.3389/fbloc.2020.00026