RELACIÓN ENTRE IDENTIDAD DIGITAL, SOCIAEDAD Y TECNOLOGÍA

Edward Hernando Castro Idárraga
Daniel Steven López Pérez
Sebastián Sarmiento Prieto
Fabian Albeiro Silva López
Sebastián Camilo Romero León

Universidad Minuto De Dios
Bogotá D.C.
Colombia
Mayo 11 del 2024

Resumen

En este artículo se aborda la transformación de la identidad en la era digital, destacando su compleja interacción con el entorno digital. Se exploran aspectos como formación, expresión y gestión de la identidad en línea, junto con los factores que influyen en su construcción, como la representación en redes sociales y la privacidad. También se examinan desafíos éticos y sociales, como la veracidad de la información y la discriminación algorítmica. El estudio busca enriquecer el conocimiento sobre la identidad digital y proponer vías para abordar sus problemáticas de manera efectiva, promoviendo un uso más ético y seguro de la tecnología digital.

Abstract

The digital era has redefined the notion of identity, giving rise to what is known as digital identity. This phenomenon, which encompasses the representations and interactions of individuals online, raises multidisciplinary challenges regarding online privacy, authenticity, and security. This study explores the complex relationship between human identity and the digital world, analyzing its formation, expression and management, as well as the factors that influence it, such as representation on social networks and the perception of privacy. In addition, it addresses ethical and social challenges, such as the veracity of information and algorithmic discrimination, with the aim of promoting more ethical and secure use of digital technology.

I. INTRODUCCIÓN

En la era actual dominada por la tecnología digital, el concepto de identidad ha experimentado una transformación radical. La proliferación de plataformas en línea, la conectividad global y la ubicuidad de la Tecnología han dado lugar a lo que ahora se conoce como identidad digital. Este fenómeno abarca las representaciones y las interacciones de un individuo en el mundo digital, planteando una serie de desafíos que abarcan múltiples disciplinas y generando interrogantes cruciales sobre la privacidad, la autenticidad y la seguridad en línea.

Este estudio tiene como objetivo indagar en la compleja interacción entre la identidad humana y el entorno digital. Desde una perspectiva interdisciplinaria, se explorarán diversos aspectos de la identidad digital, incluyendo su formación, expresión y gestión. Asimismo, se analizarán los factores que influyen en la construcción de la identidad en línea, como la representación personal en las redes sociales, el impacto de los algoritmos y la percepción de la privacidad en un mundo cada vez más conectado.

Además, se abordarán los desafíos éticos y sociales asociados con la identidad digital, como la veracidad de la información, la

manipulación de la opinión pública y la discriminación algorítmica. A través de un análisis crítico, se pretende iluminar estas problemáticas y explorar posibles vías para su abordaje efectivo en el contexto actual.

En última instancia, este estudio aspira a enriquecer el conocimiento académico y práctico sobre la identidad digital, ofreciendo una visión integral de sus implicaciones en la sociedad contemporánea y delineando áreas de investigación futura que fomenten un uso más ético, inclusivo y seguro de la tecnología digital.

II. DESARROLLO DEL ARTÍCULO

El autor Andre Boysen (2019), basa su estudio en la vulnerabilidad y ciberseguridad de datos médicos los cuales han venido teniendo una mejora en los datos a nivel de seguridad el cual ha hecho que las aplicaciones o servicios que se tramitan atreves de internet se vuelvan lentos y complejos por la cantidad de información que se puede manejar en un solo usuario o persona ya que la identidad digital ha favorecido este tema por el 2FA que es el doble factor de autentificación en procesos o procedimientos que se requiera de una ejecución para obtener alguna determinada información, también habla sobre la frecuencia con que los delincuentes han venido interceptando este tipo de información sea digital o biométrica que han venido evolucionando en plantillas para suplantar datos biométricos.

El autor Andre Boysen también nos comparte que, "la identidad digital tiene el potencial cambiar el panorama de la atención sanitaria y la forma en que se comparten los datos médicos en Canadá."" (2019, p. 37). También es Reconocido como un líder en este campo a nivel mundial sobre la identidad digital, privacidad, digital transformación y cadena de bloques sobre la cual contribuye en la sociedad actual en la mejora a nivel del sector salud en Canadá y da los principios para trabajarlos en cualquier país. Este, concluye que, “La identidad es algo que puedes mantener en tus manos, fáciles de usar y aceptados en todas partes, muy parecido a una tarjeta de crédito o un teléfono móvil. Es confiable y rentable para las empresas y brindará a los canadienses más elección, control y conveniencia. A través del modelo canadiense emergente, los consumidores podrán combinar sus finanzas cuenta de la institución con su teléfono móvil y una identificación emitida por el gobierno para crear una tarjeta digital identidad que sigue siendo física (con la SIM tarjeta en su dispositivo móvil) y fácil de usar y se puede utilizar en todas partes. “” (2019, p. 40).

Lo que podemos concluir sobre este tema es que la identidad digital está en todas partes, es cualquier proceso tecnológico que realiza una persona, que nos identifica ante un sistema, en el cual podemos tener confianza que nos brindan las empresas sea en cualquier ambiente financiero, social, religioso, político etc. en el cual nos veamos involucrados y se genera una identidad digital sobre nosotros.

Complementando al autor anterior la autora Elena Torroglosa (2017), nos informa que, “La identidad digital comprende, en general, información personal y laboral, contactos, gustos y preferencias. Todos estos datos pueden ser solicitados por los proveedores de servicios como requisitos para prestar o personalizar el servicio ofrecido. La realidad es que cualquier internauta tiene que compartir parte de su información privada para poder utilizar los servicios de Internet, por lo que los usuarios necesitan herramientas específicas para gestionar y proteger sus credenciales e información compartida. Los sistemas de gestión de identidad ofrecen a los usuarios herramientas y mecanismos para ayudarles en la tarea de controlar las credenciales y la información personal. Estos mecanismos van desde la gestión de credenciales y garantía de privacidad para inicio de sesión único, entre otros. Desde el Desde el punto de vista de los proveedores de servicios, los sistemas de gestión de identidades permiten la simplificación de gestión de usuarios, ya que asumen la delegación del proceso de autenticación y almacenamiento de

credenciales.” (2017, p 13).

Con esta información dada se da a conocer, que la identidad digital es un proceso bastante complejo donde siempre se va a requerir información sensible de quien use un servicio.

En la era digital, nuestra identidad se ha vuelto una entidad compleja que trasciende las fronteras físicas, Auerbach, N. (2004, p.14), se refiere a la identidad digital como “una representación de una identidad humana leíble por una máquina que es usada en sistemas electrónicos para interacciones con máquinas remotas o locales o personas”. Auerbach, construye esta descripción mediante una investigación sobre la identidad de una persona bajo diferentes disciplinas, esto incluye la psicológica, la lingüística, anatómica etc.

Se podría argumentar que la identidad digital puede asociarse con una única manera de establecer la singularidad de un individuo, teniendo en cuenta que la identidad digital tiene como uno de sus propósitos la identificación de una persona en un sistema informático, nada más lejos de la realidad, pues a lo largo del tiempo cada sistema informático ha desarrollado sistemas de identificación propios, por lo que a lo largo del ciberespacio tenemos múltiples sistemas de identificación para una misma persona, en este sentido, la identidad digital tiene como uno de sus objetivos la identificación de un individuo dentro de un sistema informático. El propósito de identificar a un individuo en un sistema informático no solo se centra en el acto en sí mismo, sino que esto nos permite, según sea identificado, gestionar permisos del individuo sobre el sistema informático en cuestión (u otro, pero esto lo veremos más adelante), Auerbach, N. nos dice que, “ El propósito de la identidad digital es habilitar la funcionalidad de control de acceso y enlazarlo también nos compartir con una transacción particular o un conjunto de datos en un sistema de información a un identificador individual”. (2004, p. 14).

Al participar en sistemas de información y aceptar los términos y condiciones asociados, estamos involucrándonos en lo que podríamos llamar una especie de "contrato digital". Esta acción refleja una necesidad intrínseca en los seres humanos de interactuar y colaborar dentro de estructuras sociales, incluso cuando esas estructuras son digitales y pueden no ser tan evidentes como las interacciones cara a cara.

Históricamente, los humanos han formado comunidades y sociedades basadas en reglas compartidas y normas sociales. Estas reglas pueden variar desde acuerdos tácitos sobre comportamientos aceptables hasta leyes y regulaciones explícitas. “La mayoría de las veces, los comportamientos y acciones de las personas se llevan a cabo y solo pueden llevarse a cabo cuando están físicamente involucradas, ya sea por sí mismas o mediante otra persona que las represente.” Chango (2022, p. 6).

En el mundo digital, esta dinámica social se traslada a plataformas y sistemas en línea, donde aceptamos las reglas del juego al participar en ellos.

La necesidad de aceptar estos "contratos digitales" surge de nuestra naturaleza social y nuestra dependencia de la colaboración y la interacción con otros para alcanzar objetivos comunes. Al igual que en el mundo físico, donde respetamos las leyes y normas para mantener el orden social y la cooperación, en el mundo digital aceptamos términos y condiciones para garantizar un funcionamiento fluido de los sistemas y plataformas en línea.

En nuestra vida cotidiana, nos encontramos con numerosos ejemplos de este tipo de interacciones digitales. Desde registrarnos en redes sociales hasta comprar productos en línea, cada acción implica aceptar ciertas reglas y condiciones establecidas por los proveedores de servicios. Aunque puede parecer rutinario o incluso automático, este proceso refleja nuestra necesidad innata de pertenecer a comunidades y participar en sistemas sociales, incluso cuando esos sistemas existen en un entorno digital. En última instancia, aceptar estos

"contratos digitales" nos permite aprovechar las numerosas oportunidades y beneficios que ofrecen las tecnologías modernas mientras mantenemos un equilibrio entre nuestra libertad individual y nuestras responsabilidades sociales.

Antes pudimos identificar que la identidad digital pretende identificar a un individuo dentro de un sistema informático para concederle permisos según el negocio, pero que cada sistema tenga su forma de autenticarlo puede generar inconvenientes al integrar diferentes sistemas de información, desde problemas técnicos como la replicación excesiva de los datos, o el manejo visualización o interpretación de estos, hasta generar molestias a un usuario final por tener múltiples registros en un mismo ecosistema. Esto no solo está limitado a los sistemas anteriormente mencionados, podríamos agregar por ejemplo el servicio de Xbox Game pass, Office 365, etc., y no tendríamos porqué limitarnos a un número especifico, podría seguir creciendo según nuestras necesidades. Notamos que un usuario puede ser identificado tanto por un sistema de información para que este lo autorice dentro de sí mismo, pero no solo eso, sino que un único sistema de identificación puede ser usado para múltiples servicios.

Tener un sistema centralizado de identificación, de manera resumida, nos menciona Niklas Auerbach, tiene como “beneficio para los usuarios que ellos solo tienen que iniciar sesión una vez que su sistema proveedor de identidad federada y no repetirlo cada vez que ellos lo usen. Algunas identidades federadas no solo comprimen la funcionalidad de autenticación, sino que también abarcan un asociado conjunto de datos personales que puede ser usada para transacciones basades en la web”. (2004, p. 14), cabe destacar que esto que nos menciona Niklas no solo es aplicable a una organización federada, sino también a diferentes organizaciones que se comunican entre sí. Teniendo esto en cuenta, podemos afirmar que la identidad digital no solo pretende identificar a una persona para otorgarle una autorización, sino que también refiere a los datos que están atados a esta persona. Según James E. Marcia (2015, citado en Auerbach, N. 2020), la identidad "es percibida como 'una organización dinámica de impulsos, habilidades, creencias e historia individual' (, p. 67)., teniendo en cuenta esta definición de identidad desde la psicología, podemos notar que la identidad también está profundamente relacionada con datos nuestros, un historial, etc., Tener esta data facilita a los sistemas de información modernos a conocerte mejor, por eso hablamos de identidad más allá de una autorización a un individuo, sistemas que en base al conocimiento de sus usuarios les ofrecen productos y servicios de acuerdo a sus gustos, información sugerida en con base en nuestras preferencias, etc., esto no solo es para ofrecernos las utilidades de otros.

“Esta construcción de identidad a partir de flujos de datos masivos está arraigada en el modelo de negocio de la cultura consumista y, de hecho, es altamente lucrativa financieramente (Mayer-Schönberger y Cukier 2013). Así, las capacidades de retorno de inversión de la captura de datos son prodigiosas, y a medida que más información esté disponible en línea, se pueden lograr más ganancias a partir de niveles crecientes de formación de identidad.” Gellar, S. I. (2019, p. 5).

También sirve para que seamos nosotros los que nos mostremos al mundo, nuestras habilidades, conocimientos.
Por esto mismo Auerbach, N. propone una definición más acotada de identificación digital, “la definición más simple del término identidad digital, es un patrón por el cual el usuario es conocido por el sistema. (2004, p. 14). En última instancia, esto subraya la naturaleza dinámica y en constante evolución de la identidad digital, que continúa siendo un campo de estudio y desarrollo fascinante en la era digital.

En un mundo cada vez más digitalizado, nuestras interacciones, comunicaciones y transacciones se realizan en gran medida a través de plataformas en línea, lo que genera una huella digital única para cada individuo. Esta huella digital, compuesta por datos, información y actividades en la web, todo esto

conforma lo que conocemos como identidad digital.

Una de las características más prominentes de la identidad digital es su naturaleza multifacética y en constante evolución. No se limita únicamente a perfiles en redes sociales o cuentas de correo electrónico, sino que abarca una amplia gama de aspectos, desde registros de búsqueda en línea hasta participación en comunidades virtuales y compras en internet. Esta diversidad de elementos contribuye a la complejidad de la identidad digital y a su capacidad para reflejar la personalidad, intereses y comportamientos de un individuo en el mundo virtual.

Es tanto lo que hacemos lo que dice de nosotros que inclusive, es posible identificar a un individuo no solo por sus credenciales, un numero único de identificación, un token de acceso, un apodo o una contraseña, sino que mediante el historial de todas las interacciones que este deja a través del ciberespacio es posible identificarlo. "Se define datos personales como cualquier información relacionada a una identidad o una persona identificable. Esto también incluye cualquier dato que pueda ser usado para identificar a la persona detrás incluso indirectamente", Naghmouchi, Laurent, Levallois-Barth y Kaaniche (2023, p. 3).

Por lo anterior también se tienen implicaciones que ha venido aumentando la ciberdelincuencia como lo menciona S.O. De Boer (2021) en su tesis, “en 2020, los casos de ciberdelincuencia reportados en comercio electrónico aumentó por cerca de 50%. Este podría ser un temprano indicación eso comercio electrónico tiene convertirse un atractivo objetivo para ciberdelincuentes. (2021, p. 3) donde podemos apreciar que a medida que aumenta el valor de información personal somos más susceptibles a ataque informáticos para captar esta información sensible que posee cada usuario.

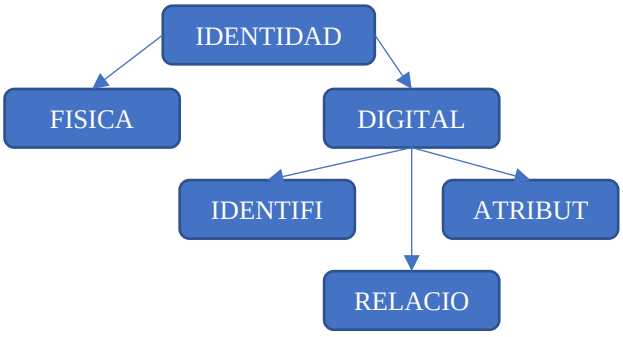
La visión de Simón Ian Gellar sobre la identidad digital establece una base sólida para comprender cómo los elementos cualitativos y cuantitativos se entrelazan para definir a un individuo en el mundo en línea. Este enfoque, según Gellar, comienza con la interacción entre individuos, lo que proporciona una comprensión inicial del "yo" en el contexto digital. En este proceso, las herramientas tecnológicas, como computadoras y aplicaciones interactivas, desempeñan un papel crucial al recopilar datos sobre las actividades en línea de una persona. Estos datos alimentan algoritmos sofisticados que construyen perfiles digitales, a menudo sin el conocimiento consciente del individuo, influyendo así en cómo es percibido y se relaciona en la web social.

Este concepto se conecta con la Teoría del Yo espejo de Cooley, que postula que la identidad de una persona se forma a través de la percepción social. Según esta teoría, la sociedad actúa como un espejo que refleja la imagen que una persona proyecta al mundo. Esto se complementa con la idea de Emerson de que el ser humano es tanto su ser interno como la expresión que muestra al mundo. En el contexto actual, la tecnología amplifica esta expresión al facilitar la creación de una identidad única a través de redes sociales y otras plataformas en línea. Estos medios tecnológicos permiten que las personas consoliden y proyecten su identidad de manera más accesible y efectiva, creando así una interacción más profunda entre el individuo y el mundo digital que, a su vez, aprende y se adapta al comportamiento humano. En este sentido, la gestión ética y responsable de la identidad en línea se vuelve crucial, ya que el fenómeno no solo afecta la privacidad individual, sino también la percepción y la interacción sociales en un contexto digitalmente interconectado.

En última instancia, la convergencia entre la visión de Simón Ian Gellar sobre la identidad digital y las teorías sociológicas como la del Yo espejo de Cooley y los postulados de Emerson subraya la complejidad y la interdependencia entre el individuo y la sociedad en el mundo contemporáneo. El avance tecnológico ha ampliado las oportunidades para la expresión y la proyección de la identidad, pero también ha

planteado desafíos éticos y prácticos que requieren una reflexión cuidadosa. A medida que continuamos navegando por el vasto y cambiante paisaje de la identidad digital, es esencial considerar no solo cómo nos representamos a nosotros mismos en línea, sino también cómo esa representación afecta nuestra percepción individual y colectiva del mundo. En última instancia, la gestión consciente y responsable de nuestra identidad digital se vuelve fundamental para cultivar un entorno en línea que fomente la autenticidad, el respeto y la conexión genuina entre los seres humanos.

Desde su perspectiva, el autor Toufic N. Chebib, en su tesis "Digital Identity: A Human-Centered Risk Awareness Study" (2020), expone la identidad como un tema controvertido y difícil de definir. Los diccionarios ofrecen diversas definiciones, pero el punto común se encuentra en asociar el comportamiento humano a personas o personalidades que están singularmente asociadas con individuos. Identificar y asociar conductas, acciones e interacciones puede relacionarse con un individuo y es parte de su identidad. De esta manera, la identidad puede dividirse en dos categorías: identidades físicas y digitales (Alashoor, Baskerville y Zhu, 2016). Asociar lo físico con lo digital es crucial para aumentar la confianza y la autenticidad de las interacciones digitales (Camp, 2004).



Es fundamental considerar también la identidad digital desde una perspectiva legal. El derecho de una persona a la tranquilidad, solicitándola si así lo desea, es primordial. Para comprender cómo se vincula la privacidad con el individuo, es vital reconocer la importancia de mantener los datos personales en privado, lo que implica que no deben ser accedidos sin autorización.

La protección de la privacidad de los datos personales se relaciona directamente con prevenir el acceso no autorizado a esta información. Esto incluye desde grandes violaciones de datos en empresas hasta intrusiones más sutiles a través de tecnologías como los asistentes virtuales y las redes sociales en línea. Esto subraya la necesidad de entender los riesgos asociados con la privacidad de los datos.

Empresas como Facebook, Target, Experian, Marriott y Amazon han experimentado ciberataques o han compartido datos personales con terceros, ya sea intencional o accidentalmente. Estos incidentes han expuesto información personal identificable (PII) a entidades no autorizadas, algunas líderes mundiales en sus respectivos campos. La violación de datos de Marriott en 2018 atrajo una considerable atención mediática, principalmente debido a su gravedad y el impacto que tuvo en millones de personas en todo el mundo.

Por otro lado, Ernesto Liceda, en su artículo La identidad digital (2011) afirma que el Estado es el único que puede afectar la identidad de una persona. Para que se pueda atacar la identidad de una persona se debe dar la situación en que este le permita conocer datos de la persona y pueda cambiarlo con un instrumento público.

Régimen legal aplicable a la protección de datos personales.

Liceda también menciona que, al hablar de protección de datos personales, surge la necesidad de clasificarlos en tres categorías excluyentes según el tipo de dato del que se trate, su titular y el acto que lo perjudica, con el objetivo de determinar el régimen aplicable a su protección en cada caso particular. Las categorías propuestas son, general, común e individual.
La categoría "general" incluirá los datos personales que estén protegidos por la mayoría

de las leyes tanto a nivel nacional como internacional.

En la categoría "común" se incluyen los datos personales que, de acuerdo con las prácticas y tradiciones de una comunidad específica, requieren protección. Estos datos estarán amparados por la legislación civil y penal, así como por la Constitución nacional.

Finalmente, en la categoría "individual" se incluirán aquellos datos que un individuo en particular considere como personales. Estos datos estarán protegidos exclusivamente por la legislación civil y penal, así como por la Constitución Nacional.

Intimidad y privacidad
La distinción entre ataques a la identidad y ataques a la privacidad o intimidad, especialmente en casos donde se produce un daño a la información, para diferenciar estos conceptos se resaltarán puntos fundamentales tales como:
Solo el estado puede afectar la identidad de una persona salvo en casos específicos.
Un ataque a la identidad implica un cambio en la situación dada.
El daño a la privacidad o intimidad implica la publicación de un dato.
El dato publicado debe ser verdadero, ya que, si es falso, se estaría atacando la imagen o reputación del individuo.
Ernesto Liceda menciona también que, mediante un fallo judicial se establece que la reputación de las personas no se daña mediante opiniones o evaluaciones, sino únicamente a través de la difusión maliciosa de información falsa.

Identidad digital en entornos empresariales

Dentro de los ambientes empresariales la gestión de la identidad digital ha pasado a ser un punto de revisión importante, centrándose en la búsqueda de diferentes opciones para abordar los desafíos emergentes, todo con el objetivo de garantizar la seguridad y el control de los recursos digitales de las organizaciones.

Con el apoyo del articulo “A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity”, se evidencia que en esta revisión sistemática se identifican varios requisitos claves de gestión de identidad y acceso, como la autenticación robusta, la cual es un método de verificación de identidad que utiliza múltiples factores para la confirmación de la identidad, la autorización granular que refiere a la capacidad de asignar permisos y roles específicos a usuarios y la gestión centralizada de identidades que implica monitorear los permisos otorgados a los usuarios desde un sistema centralizado.

Estos requisitos nombrados anteriormente representan la complejidad de los entornos de TI, la falta de interoperabilidad entre sistemas y las preocupaciones de los datos.

Como opción de solución sobresale el concepto de identidad soberana que su enfoque es otorgar a las personas el control total sobre su identidad digital, esto combinado con alguna otra tecnología, permitiría cubrir y solucionar los desafíos presentados.

Identidad digital y blockchain

Hay una tecnología que ha surgido con planes de cubrir estas incertidumbres y afrontar las preocupaciones asociados con la gestión de identidades digitales en la era digital, todo lo que incluye la privacidad, la seguridad y la interoperabilidad entre sistemas.

Los autores del articulo Research on Digital Identity Authentication Technology Based On Block Chain (2021) indican que, “Las Amenazas causadas por los datos de privacidad personal del usuario estén demasiado centralizados y son vulnerables. para atacar, y la centralización de datos conducirá a la redundancia de datos, mala permeabilidad, la falta de control maestro por parte del usuario, el alto costo general y las amenazas potenciales de abuso de la central. “(2021, p. 2) donde se evidencia que la centralización de Información es una

vulnerabilidad actual y es el foco de los ciberdelincuentes.

Según el artículo “Digital Identity and the Blockchain: Universal Identity Management and the Concept of the “Self-Sovereign” Individual” la tecnología blockchain puede abordar estos desafíos al proporcionar un marco descentralizado y seguro para la gestión de identidades. La blockchain permite la creación de registros inalterables y transparentes de identidades digitales, donde cada individuo puede tener control total sobre su información personal.

Existe un concepto llamado, identidad soberana que deriva de la relación entre la identidad digital y la tecnología blockchain, este concepto se refiere a la idea de que cada persona debe tener el poder y autonomía para controlar su propia identidad digital y ya no depender de terceros como gobiernos o corporaciones. La identidad soberana se basa en principios de descentralización, interoperabilidad y privacidad, permitiendo a cada uno gestionar y compartir su información de forma segura.

Tomando como base la identidad soberana, se discute como esta podría transformar la gestión de identidades digitales al eliminar intermediarios y proporcionar una capa de confianza basada en la criptografía y la tecnología blockchain. Algunos ejemplos de casos potenciales del uso de la identidad soberana son sectores como los servicios financieros, servicios de salud y gubernamental, teniendo como beneficios la eficiencia, seguridad y protección.

Adicional a lo anterior, se involucran cuestiones éticas y legales relacionadas con la implementación de la identidad soberana, sobre todo en la privacidad y el consentimiento informado.

III. Características

Privacidad en línea:

Este subtema se centra en la protección de la información personal en el mundo digital. Incluye la gestión de la privacidad en redes sociales, navegadores web, correos electrónicos y otros servicios en línea.
Gestión de configuraciones de privacidad, control de datos personales, políticas de privacidad de las plataformas, riesgos de filtración de datos.

Seguridad cibernética:

Este subtema aborda la protección de la identidad digital contra amenazas como el phishing, el malware, el robo de identidad y otros ataques cibernéticos.
Uso de contraseñas seguras, autenticación de dos factores, software antivirus, protección contra malware, educación sobre ciberseguridad.

Reputación en línea:

Este subtema examina cómo las actividades en línea pueden afectar la percepción que otros tienen sobre una persona, ya sea en el ámbito personal o profesional.
Gestión de perfiles en redes sociales, monitoreo de comentarios y menciones, construcción de una reputación digital positiva, resolución de conflictos en línea.

Autenticación digital:

Se refiere a los métodos utilizados para verificar la identidad de una persona en el mundo digital, como contraseñas, huellas dactilares, reconocimiento facial, etc.
Métodos de autenticación seguros, biometría, tokens de seguridad, autenticación multifactor.

Ética en línea:
Este subtema aborda cuestiones morales y éticas relacionadas con el comportamiento en línea, como el ciberacoso, la difusión de

desinformación y el comportamiento ético en redes sociales.

Respeto a la privacidad y los derechos de los demás en línea, combate a la desinformación, promoción de la empatía y la inclusión digital.

Identidad digital en contextos específicos:

Se refiere a cómo la identidad digital se aplica en contextos específicos como el ámbito laboral, educativo, gubernamental, etc.
Políticas de seguridad y privacidad específicas para cada contexto, gestión de identidades digitales en entornos institucionales, regulaciones gubernamentales sobre identidad digital.

IV. Conclusión

La identidad digital representa y se constituye de tola información de un individuo que se almacena en la red, sea personal laboral, bancaria, de salud, todo tipo de información que nos involucre pertenece a nuestra identidad digital. Es algo que puedes encontrar en cualquier lugar ya que se basa en cualquier servicio tecnológico que utilizas como el uso de las redes sociales, transacciones bancarias, compra de productos, citas médicas, etc. Cualquier tipo de servicio que utilices de manera virtual que sea vinculada a algún proceso aplicación o identidad también se han generado varios procesos de seguridad como el doble factor de autentificación, datos biométricos para verificar la autenticidad de la persona que está realizando el trámite o transacciones.

El concepto de identidad del ser humano a evolucionado con el tiempo, esto producto de nuestras interacciones con el entorno que nos rodea, actualmente en esta era digital se ha visto necesario que reflexionemos sobre esto para afrontar de mejor manera ciertas interacciones que hemos ejercido de maneras inadecuadas, por esto mismo, se ha adecuado a que utilicemos la tecnología para encarar inconvenientes como el fraude, extorsiones etc., debido a esto, es imperativo que entendamos como es que nosotros nos relacionamos con el entorno digital, que realmente, es una extensión del entorno en el que ya estamos, y que podamos entender nuestro papel y los demás con el fin de generar un ambiente ideal para todos.

La inclusión de nuevas tecnologías como blockchain a la gestión de identidades digitales, pueden representar una gran transformación para empoderar a las personas y mejorar esta gestión en un mundo cada vez más conectado y digitalizado, sin embargo, aún quedan dudas por analizar y resolver para poder tener claro el funcionamiento de esta tecnología sobre este concepto.

La identidad digital es un fenómeno complejo que se entrelaza con elementos cualitativos y cuantitativos, influenciados por la interacción social y la tecnología. Desde la perspectiva de Simón Ian Gellar, la formación de esta identidad comienza con la interacción entre individuos y se ve moldeada por algoritmos sofisticados que recopilan y procesan datos personales. Este proceso se relaciona con teorías sociológicas como la del Yo espejo de Cooley, que destacan la importancia de la percepción social en la construcción de la identidad. En el mundo digital actual, la tecnología amplifica la expresión individual, pero también plantea desafíos éticos en términos de privacidad y autenticidad. En conclusión, la gestión consciente de nuestra identidad digital es esencial para cultivar un entorno en línea que promueva la autenticidad y el respeto mutuo, manteniendo así la integridad de la interacción humana en el mundo digital.

V. Referencias

Gellar, S. I. (2019). Conceptions of Digital Self: Understanding Identity Formation, Performance and Online Social Reality (Tesis de maestría). Universidad de Kent, Escuela de Política Social, Sociología e Investigación Social.

Naghmouchi, M., Laurent, M., Levallois-Barth, C., & Kaaniche, N. (2023). Comparative analysis of technical and legal frameworks of various national digital identity solutions. Samovar, Télécom SudParis, Institut Polytechnique de Paris, France, Palaiseau 91120.

Auerbach, N. (2004). Anonymous digital identity in e-Government (Dissertation, Wirtschaftswissenschaftlichen Fakultat, Universitat ZUrich).

Chango, M. (2022). Building a Credential Exchange Infrastructure for Digital Identity: A Sociohistorical Perspective and Policy Guidelines. DigiLexis Consulting, Lome, Togo. Received: 16 November 2020. Accepted: 28 December 2021. Published: 14 February 2022.

Chebib, T.N. (2020). 'Digital Identity_ A Human-Centered Risk Awareness Study', Digital Commons University of South Florida, November.

Ernesto Liceda (2011). La identidad digital. 41st edn.

Boysen. A. (2019). The Need for a National Digital Identity Infrastructure.

Glöckler, J.; Sedlmeir, J.; Frank, M.; Fridgen, G. 2023. A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. Business & Information Systems Engineering. 20 páginas.

Zwitter, A.; Gstrein, O.J.; Yap, E. 2020. Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. University of Groningen, 15 páginas.

Torroglosa, E (2017). Digital Identity Management Through the Interoperability of Heterogeneous Authentication and Authorization Infrastructures

S.O. De Boer (2021). Digital Identity A cyber resilience evaluation of the European digital identity e-commerce requirements

Zaixing. C Shaofei. W Research on Digital Identity Authentication Technology Based On Block Chain

Escobar., E. (2020) Charles H. CooleyUna aproximación (bases para una teoría comunicativa de lo social)

Álvarez de Toledo, M. L. (2013). Cómo difundir y promocionar la identidad digital e investigadora del profesorado universitario. Identificadores académicos.