IDENTIDAD DIGITAL GLOBAL

# Identidad Digital Global: Un Enfoque Integral para la Protección y Gestión en el Siglo XXI"

# JAIME ZAMUDIO

# OSCAR CAMARGO

# WILFREDO SAMBONI

# CARLOS RODRÍGUEZ

# JOSE GALVIS

# Escuela Superior de Guerra

# Resumen

La identidad digital ha evolucionado en respuesta a la creciente digitalización y los avances tecnológicos. Este artículo analiza los principales desafíos en su gestión, como el fraude de identidad, la interoperabilidad entre sistemas y el equilibrio entre seguridad y usabilidad. Asimismo, explora las tendencias emergentes, como el uso de blockchain e inteligencia artificial para mejorar la protección y control de datos personales. A pesar de las mejoras en seguridad, persisten problemas que requieren un marco regulatorio más robusto. La identidad digital se consolida como un pilar clave en la economía global, con su futuro marcado por la innovación tecnológica y la regulación efectiva.

# **Identidad Digital Global: Un Enfoque Integral para la Protección y Gestión en el Siglo XXI"**

**Abstract**

# La identidad digital ha evolucionado continuamente debido a la revolución tecnológica y los cambios en la protección y gestión de información personal. Este documento describe los desafíos actuales y las tendencias futuras asociadas con la identidad digital. Para ello, se exploran cuatro elementos clave, a saber, la conceptualización de la identidad digital en el ámbito digital global, los desafíos para su correcta administración, el marco regulatorio y su evolución, y las tendencias tecnológicas emergentes que también moldean el futuro de una identidad digital. En el actual entorno digital, la identidad digital se trata de una mezcla de información personal, información biométrica y social que permite a los usuarios interactuar uns unos con otros en el mundo virtual. Tecnologías avanzadas como la blockchain, la identificación basada en blockchain y la autenticación multifactorial han permitido más ámbitos seguros para los administradores de identidad, aunque han presentado nuevos problemas en términos de interoperabilidad y protección de datos. En cuanto a la gestión de identidad digital, los desafíos incluyen el fraude de identidad, la suplantación de identidad y los problemas con los sistemas de autenticación. Por otro lado, la protección de privacidad y interoperabilidad entre diferentes marcos de identificación es también un desafío, como lo es la necesidad de equilibrar la seguridad con la comodidad. La seguridad cibernética y problemas legales también son sujetos no menos importantes. En el caso de las regulaciones y marcos de la identidad digital en general y en las reglamentaciones locales y globales en particular, existen además datos sobre los esfuerzos recientes, la normativa general de protección de datos generales y los esfuerzos en Europa como punto de referencia. Además, la idea de autoposeer la identidad digital, como, por ejemplo, la Identidad Soberana Digital, se está volviendo más común, lo que se considera una solución en la que los propios usuarios tienen el control de su identidad digital, pero necesitan un marco de implementación y regulación más detallado in lugar de fomento cubierto. Finalmente, las tendencias emergentes, como el uso de IA en la autenticación y la descentralización a través de blockchain, están redefiniendo las formas en que se manejan las identidades digitales. Aunque se espera que todas estas tendencias mejoren la seguridad y la privacidad, la integración de identidades digitales a nivel gubernamental podría ser la única solución viable a largo plazo en términos de seguridad y eficiencia. Al mismo tiempo, todos los desafíos de seguridad y privacidad deben abordarse desde un enfoque integral, que por ahora puede ser suministrado solo por el gobierno.

**Identidad digital en un contexto global**

En el mundo actual, la identidad digital se ha convertido en un tema de suma importancia entre todas las personas debido a la necesidad y la relación con la vida digital y las cosas conectadas a internet como las redes sociales y todas las actividades financieras entre muchas otras. Esto se debe a que cada vez más actividades personales y profesionales giran en torno a un individuo creado y relacionado con la identidad cibernética.

**Significado y componentes de la identidad digital**

La identidad digital es la imagen virtual de un individuo o una entidad en un ambiente virtual. La imagen abarca datos personales, datos biométricos, así como rastros digitales de las interacciones en línea. Para Goode, la identidad digital es un reflejo más amplio de la identidad real; sin embargo, existe el riesgo de identidad no asegurada en las plataformas digitales. Para proveer tiempo de identidad, se deben crear credenciales de identidad que serán usadas posteriormente para autenticar y permitir el acceso a los sistemas y servicios.

**Importancia de la identidad digital para la economía global**

En la economía digital, la identidad digital es esencial ya que permite a los individuos y entidades realizar actividades y transacciones sin tener que estar en un lugar físico. La autenticación y la verificación son fundamentales para garantizar que los procesos digitales sean seguros. Plataformas digitales como servicios de comercio electrónico, plataformas de identidades bancarias, y redes sociables sean protegidas mediante su identidad digital (Nielsen, 2019).

Sin embargo, la identidad digital también ha demostrado ser vulnerable, ya que las amenazas a la seguridad, como el robo de identidad, han aumentado exponencialmente en los últimos años. Los ciberdelincuentes aprovechan las lagunas en los sistemas de autenticación para obtener acceso no autorizado a cuentas y datos personales. En este sentido, es fundamental que las empresas inviertan en tecnologías avanzadas de seguridad digital que fortalezcan la protección de las identidades digitales.

**Tecnologías emergentes y su impacto en la identidad digital**

Tecnologías emergentes como el blockchain han generado un impacto significativo en la forma en que se gestionan las identidades digitales. El blockchain, por ejemplo, permite la creación de registros inmutables de identidad que no pueden ser alterados ni manipulados, ofreciendo una capa adicional de seguridad frente a ataques cibernéticos. Según Snehi y colaboradores (2012), las soluciones basadas en blockchain para la gestión de identidades digitales no solo proporcionan seguridad, sino que también ofrecen la posibilidad de un mayor control sobre los datos personales por parte de los usuarios. Otra tecnología clave que ha revolucionado la gestión de identidades es la autenticación multifactorial, que combina varios métodos de verificación, como contraseñas, tokens de seguridad y datos biométricos. Estas tecnologías han mejorado la seguridad de las identidades digitales al reducir la dependencia de una sola forma de autenticación. Sin embargo, a pesar de estos avances, persisten desafíos relacionados con la interoperabilidad entre sistemas y su usabilidad.

**El papel de las plataformas sociales en la construcción de identidades digitales**

Las redes sociales son importantes para construir personas en línea. Las personas crean versiones digitales de sí mismas en estos sitios, que pueden ser como las de la vida real o totalmente diferentes. Sin embargo, esta configuración también tiene peligros, ya que las redes sociales a menudo son atacadas, lo que puede dañar la privacidad de sus usuarios. Como explica Morabito (2014), las identidades en línea pueden cambiar rápidamente, lo que dificulta que las empresas y los legisladores mantengan segura la información. Es preciso indicar, entoces, la dificultad de establecer una identidad digital dado que las personas pueden generar múltiples identidades digitales configuradas deacuerdo a su propia voluntad, que impiden comprobar la autenticidad, situación que incrementan la ventaja para los atacantes o los delincuentes en el ciber espacio.

**Retos en la gestión seguridad de la identidad digital**

De los principales problemas a los que se enfrenta la identidad digital se relaciona con sus seguridad y eficacia, que junto al constante desarrollo tecnológico incrementa las amenaza cibernéticas, originando un conjunto de desafíos críticos para la misma.

***Fraude de identidad y ataques de suplantación***

El fraude de identidad y los ataques de suplantación de identidad, incluido el phishing, son problemas importantes en la gestión de identidades digitales. En estos ataques cibernéticos, los piratas informáticos se hacen pasar por fuentes confiables para robar los detalles de inicio de sesión del usuario. Las personas suelen utilizar contraseñas simples o idénticas para diferentes cuentas, lo que facilita a los piratas informáticos hacerse pasar por ellos. Según Goode (2019), la división del mercado de soluciones de identidad y la ausencia de directrices compartidas dificultan la lucha contra el fraude de identidad.

En respuesta, el uso de la autenticación multifactor (MFA) se ha vuelto más frecuente. Esto hace que sea más difícil para las personas malintencionadas ingresar a las cuentas, incluso si encuentran solo una forma de demostrar que son el usuario. Sin embargo, la adopción de MFA no es universal y sigue habiendo una resistencia significativa debido a la fricción que introduce en la experiencia del usuario (Snehi et al., 2012).

***Vulnerabilidad en los sistemas de autenticación***

Además del fraude, estos sistemas pueden tener debilidades que los piratas informáticos podrían aprovechar. La piratería de sistemas que gestionan identidades en línea es frecuente y puede generar grandes problemas. En 2018, por ejemplo, una brecha en Facebook expuso la información personal de millones de usuarios, demostrando cómo las identidades digitales pueden ser comprometidas a gran escala (Korac et al., 2021).

Uno de los grandes retos a la hora de proteger la identidad digital es gestionar la relación entre la seguridad y la usabilidad. Cuantas más capas de seguridad se instauren, más difícil puede llegar a ser el acceso de la persona a su cuenta, lo cual a menudo se traduce en el hecho de que las personas adquieren conductas de riesgo, como desactivar la autenticación multifactor o bien elegir contraseñas sin las características de complejidad que podría tener una contraseña apropiada. Dicha tensión entre la seguridad y la usabilidad pone de manifiesto la búsqueda de soluciones que sean tanto seguras como usables.

***Interoperabilidad entre sistemas de gestión de identidad***

Otro gran reto es la interoperabilidad entre distintos sistemas de gestión de identidad. En el entorno digital global, los usuarios suelen interactuar con numerosa plataformas y servicios, que exigen la creación de identidades digitales múltiples.

Dicha situación no sólo fragmenta la identidad, sino que también crea puntos de vulnerabilidad adicionales. Según Knight y Saxby (2014), la falta de interoperabilidad entre sistemas de gestión de identidad hace que los usuarios tengan que mantener varias credenciales, lo que aumenta la posibilidad de errores humanos y de que las credenciales sean comprometidas.

Las soluciones fundamentadas en blockchain están empezando a abordar este problema, ofreciendo un registro único e inalterable de la identidad, que puede ser usado en diferentes plataformas sin menoscabar la privacidad del usuario. No obstante, lo anterior, éstas se encuentran en sus primeras etapas de integración, dependiendo de superar barreras tanto reguladoras como tecnológicas para poder ser integradas de forma generalizada.

**Conclusiones**

La identidad digital ha surgido como uno de los elementos vertebradores del nuevo ecosistema digital, afectando a diversas actividades, desde el e-commerce, a la interacción en redes sociales, hasta el acceso a servicios de las administraciones públicas. En el transcurso del extenso artículo ya mencionado hemos señalado la forma en que la identidad digital ha llegado a ser lo que es como consecuencia de las necesidades de un mundo cada vez más digitalizado, y hemos podido identificar los retos fundamentales a los que se enfrenta la misma y las tendencias tecnológicas que ella misma marcará.

Una de las cuestiones que hemos podido destacar es la importancia de la seguridad en la gestión de la identidad digital. Cada vez más personas y organizaciones están interactuando de manera digital, lo que ha incrementado considerablemente el riesgo de fraudes y de suplantación de identidad. Herramientas como la autenticación multifactor o el uso de inteligencia artificial para la detección de amenazas han demostrado ser útiles para mitigar estos riesgos, pero aún queda mucho por hacer para asegurarse de que los sistemas sean realmente seguros. El equilibrio entre seguridad y usabilidad sigue siendo un desafío crucial que las empresas y los desarrolladores de tecnología deben abordar (Goode, 2019).

Otro aspecto crítico analizado ha sido la pregunta de la privacidad y el control de los datos personales. Un contexto donde los datos de los usuarios se convierten en un recurso muy valorado, el conceder que las personas tengan el dominio sobre su propio dato se hace crucial. En este sentido, el Reglamento General de la Protección de Datos (RGPD) ha sido una mejora en términos de la protección de la privacidad, aunque por sí solo no es suficiente. La identidad soberana digital (o digital sovereign identity, en inglés) hace un paso más en la promesa de poder devolver el control de los datos a los usuarios, pudiendo gestionar las identidades de forma autónoma sin tener que depender de un intermediario. No obstante, la SSI enfrenta desafíos en términos de interoperabilidad y adopción a gran escala (Knight & Saxby, 2014).

Por un lado, el futuro de la identidad digital, sin duda, va a ser determinado por la inteligencia artificial y la descentralización de la identidad digital que ofrecen las tecnologías como el blockchain. Por otro lado, la inteligencia artificial puede servir para perfeccionar los sistemas de autenticación (y por tanto, del sistema de gestión de las identidades) volviéndolos más adaptables y eficientes. También, el blockchain puede proporcionar una infraestructura más segura y transparente para manejar las identidades. Las nuevas tecnologías no solo mejoran la seguridad en el manejo de la identidad digital, sino que también contribuirán a que los usuarios reduzcan su dependencia de las plataformas centralizadas volviendo a los individuos el control de sus identidades. Sin embargo, la adopción de estas tecnologías también traerá nuevos desafíos regulatorios y éticos que deberán ser abordados con cuidado (Morabito, 2016).

Finalmente podemos entender que la identidad digital está en constante evolución y su futuro dependerá en gran medida de la capacidad de las organizaciones, los gobiernos y los desarrolladores de tecnología para abordar los desafíos actuales de seguridad, privacidad e interoperabilidad. Las tendencias emergentes, como la inteligencia artificial y el blockchain, ofrecen soluciones prometedoras, pero es fundamental que se desarrollen marcos regulatorios adecuados para garantizar que estas tecnologías se utilicen de forma ética y efectiva. La identidad digital es y seguirá siendo un pilar clave en la economía digital global y su evolución será fundamental para garantizar un futuro más seguro y eficiente en nuestras interacciones en línea.

# Referencias

# Goode, A. (2019). Digital identity: solving the problem of trust. *Biometric Technology Today*, *2019*(10), 5–8. https://doi.org/10.1016/s0969-4765(19)30142-0

# Knight, A., & Saxby, S. (2014). Identity crisis: Global challenges of identity protection in a networked world1. *Computer Law and Security Report*, *30*(6), 617–632. https://doi.org/10.1016/j.clsr.2014.09.001

# Korać, D., Damjanović, B., & Simić, D. (2022). A model of digital identity for better information security in e-learning systems. *The Journal of Supercomputing*, *78*(3), 3325–3354. https://doi.org/10.1007/s11227-021-03981-4

# Morabito, V. (2016). *The future of digital business innovation*. Springer International Publishing.

# Nielsen, M. M. (2019). Tackling identity management, service delivery, and social security challenges: Technology trends and partnership models. *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, *2017*, 1–5.

# Snehi, M., Snehi, J., & Dhir, R. (2012). Issues and emerging Trends in Identity Management. *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, *3*, 294–297. https://doi.org/10.24297/IJCT.V3I2B.67