"La Identidad Digital como el Sistema Nervioso de un Futuro Conectado: Desafíos, Regulación y Autenticación en la Era de las Máquinas Autónomas"

Tatiana Sánchez

Miguel Amaya

Cristian Toro

Andrés Parrado

Escuela Superior de Guerra

Maestría de Ciberseguridad y Ciberdefensa

Octubre 18, 2024

Resumen

Estamos conscientes de los desafíos que tenemos en el mundo digital y qué tan segura es nuestra identidad digital? Para dar respuesta a estas preguntas abordaremos en este artículo como nuestra identidad no es solo física sino que se extiende a la virtualidad como un "sistema nervioso" a través de diversos dispositivos, robots y tecnologías emergentes, logrando un mundo cada vez más interconectado. Este sistema, como su nombre lo dice, es un conjunto de elementos y componentes interrelacionados que deben trabajar sincronizados y en perfecto equilibrio hacia un objetivo común, de no ser así avanzamos en un ecosistema vulnerable y fragmentado; por lo tanto hablaremos del marco legal en Colombia y los retos asociados a su adaptabilidad a la velocidad de nuevas tecnologías como la inteligencia artificial (AI); así como métodos de autenticación biométrica, asistentes de voz e identidad autogestionada, siendo estos los sensores del sistema nervioso digital que hacen parte importante de la Ciberseguridad.

Palabras clave: identidad digital, sistema nervioso digital, ciberseguridad, regulación, Colombia, IA.

"La Identidad Digital como Sistema Nervioso Hiperconectado: Desafíos, Regulación y Autenticación en la Era de las Máquinas Autónomas"

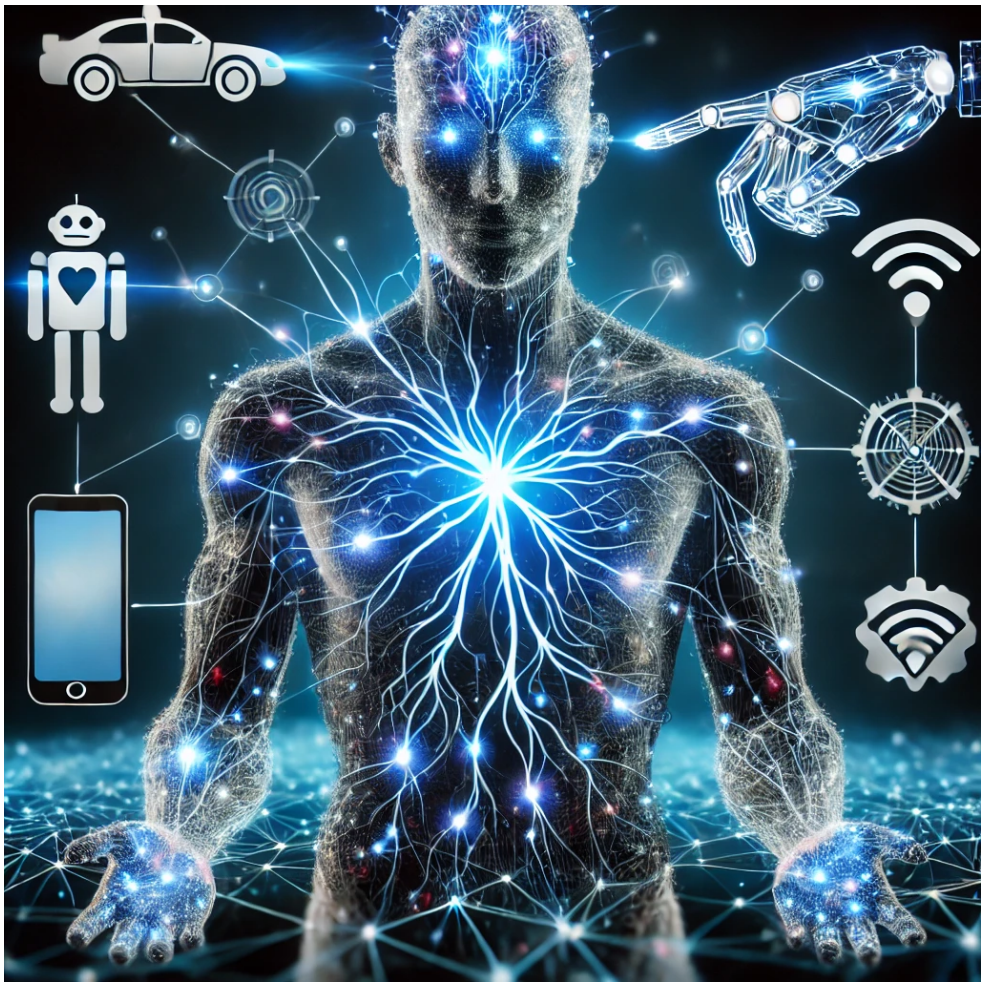
Nos encontramos en un mundo donde la **identidad digital** se extiende más allá de nuestras pantallas y dispositivos, conectándose con **máquinas autónomas**, **robots inteligentes** y **tecnologías emergentes**, por lo tanto debemos repensar cómo se gestiona y protege esta identidad. Podemos visualizar la identidad digital como un **sistema nervioso**, una red compleja que conecta cada "órgano" tecnológico, desde teléfonos móviles hasta coches autónomos, y coordina nuestras interacciones en el mundo digital.

Al igual que el sistema nervioso humano, que transmite impulsos eléctricos entre el cerebro y el cuerpo, la identidad digital fluye de manera continua entre los dispositivos, y con diversos sensores puede lograr autenticarse y protegerse. Sin embargo, este sistema nervioso también puede enfrentar amenazas que interrumpan su flujo, desde ciberataques hasta suplantación de identidad.

Exploraremos en este artículo la diversidad de este sistema nervioso digital, los mecanismos de defensa y las regulaciones en Colombia buscando adaptarse para proteger este nuevo ecosistema.

La Identidad Digital como Sistema Nervioso: Conexiones y Sinapsis entre Dispositivos

Nuestra identidad digital es como el sistema nervioso de tu cuerpo. A medida que interactúas con el mundo, tu sistema nervioso transmite información a cada parte del cuerpo, asegurando que todo funcione de manera fluida y coordinada. En el mundo tecnológico, cada dispositivo que utilizas, desde tu teléfono móvil hasta un asistente virtual o robot autónomo, es una extensión de este sistema nervioso, transmitiendo datos y verificando tu identidad en tiempo real.



Cada interacción digital que realizas, como tu auto inteligente o realizar pago a través de tu teléfono, son un impulso eléctrico que viaja a través del sistema nervioso digital. Dispositivos inteligentes como asistentes de voz, los robots autónomos de Tesla, y electrodomésticos conectados (Internet de las Cosas (IoT) actúa como una extensión de nuestra identidad digital, creando una red de interacciones que requieren una coordinación perfecta y protocolos de seguridad que puedan manejar millones de impulsos simultáneos sin comprometer la privacidad ni la seguridad.

Este ecosistema interconectado en nuestro sistema nervioso humano está diseñado para que fluya de manera continua asegurando que solo tú tengas acceso; por lo tanto debemos hacer lo mismo en la interconexión con el mundo digital.

Fortaleciendo el Sistema Nervioso de la Identidad Digital en Colombia: Regulación y Legalidad

Al igual que el sistema nervioso humano necesita estar protegido para garantizar el correcto funcionamiento del cuerpo, el ecosistema digital de Colombia requiere un marco regulatorio robusto que proteja la identidad digital de los ciudadanos ante amenazas externas. A hoy las leyes de protección de datos y autenticación digital en Colombia actúan como los nervios centrales buscan aseguran la integridad y el flujo seguro de información en el ecosistema digital del país; sin embargo no están avanzando a la velocidad de las tecnologías y estamos quedando sin mayor protección.

La Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales, cumple un rol fundamental al proteger la integridad de la información personal, garantizando que los datos sean tratados de manera confidencial y segura; de manera similar a cómo los impulsos nerviosos no pueden ser interceptados sin consecuencias para el cuerpo, esta ley protege los datos personales para que no sean vulnerados por terceros. Esto permite que el sistema nervioso digital

funcione sin interrupciones, manteniendo la seguridad en cada interacción. Ahora bien, si hacemos una comparación con el Reglamento General de Protección de Datos de la Unión Europea (GDPR) tendríamos varios puntos por mejorar como su aplicabilidad únicamente en el país y no global, debe ser más implícito de cómo lograr el consentimiento de uso de los datos, no contiene disposiciones específicas en el derecho de portabilidad de los datos o el derecho al olvido y deberían existir sanciones más estrictas.

Existen de igual forma, normativas como el Decreto 620 de 2020 refuerzan la validez de las firmas digitales y electrónicas, asegurando que las transacciones en línea sean verificadas y confiables. Estas leyes son esenciales para mantener el equilibrio del sistema nervioso digital de Colombia, garantizando que las interacciones entre los ciudadanos y las plataformas digitales se realicen de forma segura y protegida.

Desafíos Regulatorios en un Ecosistema en Evolución

Con el avance tecnológico, Colombia se enfrenta a un reto significativo: la legislación no avanza lo suficientemente rápido para cubrir nuevas áreas de vulnerabilidad. Este desfase entre el progreso tecnológico y la regulación es como un sistema nervioso digital sin protección adecuada, dejando a los ciudadanos expuestos a ciberataques y robo de identidad. Esta situación es especialmente preocupante dado el rápido ritmo de adopción de tecnologías que no están adecuadamente cubiertas por el marco legal actual.

El ecosistema digital de Colombia ha crecido significativamente, multiplicando los dispositivos y plataformas que interactúan con la identidad digital de los ciudadanos. Sin embargo, la falta de regulación específica para tecnologías emergentes como la inteligencia artificial (IA), el blockchain y las identidades autogestionadas (SSI) ha creado un vacío que deja al sistema en una posición vulnerable.

Impacto en la Protección de Datos

Leyes existentes, como la Ley 1581 de 2012 y el Decreto 620 de 2020, son fundamentales para la protección de datos y la regulación de firmas digitales, pero no abordan adecuadamente el uso de tecnologías emergentes en la gestión de identidades digitales. Esto limita el control ciudadano sobre su información personal en un entorno cada vez más descentralizado.

Confianza Debilitada en los Sistemas Digitales

Este desfase regulatorio también erosiona la confianza en el ecosistema digital. Sin garantías suficientes sobre la gestión y protección de sus datos, los ciudadanos experimentan incertidumbre en sus interacciones digitales, aumentando su vulnerabilidad frente a amenazas externas.

Tecnologías Emergentes No Reguladas

Colombia aún no regula eficazmente tecnologías emergentes como el blockchain o la inteligencia artificial (IA) en la gestión de identidad digital, lo que crea un vacío crítico en seguridad y control sobre los datos. La actualización de la Ley 1581 para incluir estas tecnologías y alinearse con normativas internacionales como el GDPR será esencial para enfrentar futuros desafíos. Adicionalmente, adoptar principios como el Consumer Data Right (CDR) de Australia podría otorgar a los ciudadanos mayor control sobre sus datos digitales, permitiéndoles decidir cómo y cuándo compartir su información con terceros.

Desafíos y futuras tendencias en la regulación de la identidad digital

A medida que el sistema digital se extiende a nuevos dispositivos y tecnologías, los marcos regulatorios deben evolucionar para mantenerse a la par de estos avances. En Colombia, aunque las normativas vigentes han sido efectivas en proteger la privacidad y seguridad de los datos personales, enfrentan desafíos importantes:

- Interoperabilidad: La Ley 1928 de 2019 intentó mejorar la interoperabilidad entre las plataformas digitales del Estado, pero aún se requiere avanzar en la estandarización global para que las identidades digitales puedan transitar con seguridad entre diversos sistemas y plataformas.
- Blockchain y SSI: La legislación actual no contempla suficientemente tecnologías emergentes como blockchain o identidades autogestionadas, lo que limita a los usuarios en el control descentralizado de sus propios datos.

Métodos de Autenticación: Los Sensores del Sistema Nervioso Digital

En el ciberespacio, los métodos de autenticación de la identidad digital son como los sensores del sistema nervioso humano, que aseguran que cada acción sea legítima y los métodos de autenticación más básicos serían equivalentes a los sensores más simples, aquellos que responden de manera básica y primaria ante estímulos simples, pero son más vulnerables a interferencias. Las contraseñas estáticas asimilan ser un sensor básico que responde a una señal; por ejemplo, requieren que el usuario memorice una clave para autenticar su identidad en un sistema. Sin embargo, al igual que un sensor sencillo, es fácil de vulnerar mediante ataques de fuerza bruta o phishing. "Los ciberdelincuentes han creado muchas herramientas que pueden ayudar a adivinar contraseñas. Por otra parte, una contraseña compleja puede olvidarse, y el usuario tendrá que restablecerla" (Zuriati et al., 2022, p. 3). Como consecuencia de lo anterior se crearon las contraseñas dinámicas, aunque agregan una capa de protección extra generando un nuevo canal de transmisión independiente, siguen siendo señales transmitidas que pueden ser interceptadas. Estas contraseñas cambian en cada sesión dependiendo de la rutina, pero si la transmisión no es cifrada siguen siendo vulnerables, como un sensor que envía señales sin protección ante interferencias externas. Los anteriores métodos al igual que los sensores básicos del sistema nervioso, logran cumplir su función, pero no ofrecen la capacidad defensiva necesaria contra los ataques más complejos, por lo que requieren de mejoras, como sensores avanzados

para asegurar la autenticación con mayores capacidades de ciberseguridad. Ante estos desafíos, métodos más seguros que los anteriores han ido ganando terreno. La autenticación biométrica, a través de huellas dactilares, reconocimiento facial o voz, son de los avances más importantes que permiten que este sistema funcione sin interrupciones.

La autenticación biométrica está consolidada como uno de los pilares fundamentales, debido a su integración típica en la gran mayoría de los sistemas de cómputo móviles. Una de las grandes ventajas, es el nivel de exclusividad en el valor de autenticación, es decir: el sistema humano, mantiene valores únicos por individuos como el rostro, huellas dactilares, iris, entre otros. Permitiendo que cada aspecto biológico puede llegar a relacionar un valor de autenticación para el acceso en un sistema, generando llaves de identificación únicas.

Los smartphones son uno de los muchos puntos de acceso al ciberespacio y uno de los principales sistemas que más utiliza sensores de autenticación biométrica, que asumirán ser centro de control del sistema nervioso digital. Cada vez que desbloqueas tu teléfono con una huella dactilar o reconocimiento facial, estás utilizando un método biométrico que actúa como un punto de verificación personal y único, que a su vez permite el acceso a otros sistemas, aplicaciones, infraestructuras o redes. “Los riesgos de utilizar datos biométricos son enormes. Una vez violados, no se pueden recuperar. Los datos no son renovables y, por tanto, no pueden utilizarse una vez robados.” (Zuriati et al., 2022, p. 4) Al igual que un nervio dañado u órgano en el cuerpo no pueden regenerarse, pero la integración de los diferentes métodos de autenticación permite el agregar capas y capas de seguridad. Se puede mejorar cómo la combinación de varios métodos (como contraseñas dinámicas y biometría) permite mitigar algunos de los riesgos de los otros métodos de autenticación, pero también introduce desafíos relacionados con la experiencia del usuario. “Los usuarios tendrán que autenticarse dos o más veces utilizando este método MFA” (Zuriati et al., 2022, p. 6). Permitiendo que métodos de autenticación con menos interacción con el usuario sean más atractivos para utilizar, debido al bajo nivel de complejidad de uso. “Hoy en

día, la gente está familiarizada principalmente con métodos de autenticación que requieren una interacción (al menos mínima) por parte del usuario.” (Butcher et al., 2023, p. 80)

La domótica, Internet de las cosas y la integración del uso de aplicaciones que permiten su control y gestión por comandos de voz, aumentaron el avance de la tecnología. Aumentando una mayor veracidad y autenticidad de la información recolectada por esta y utilizarla con el fin de autenticar al hablante por medio de las señales únicas generadas por el mismo. Sin embargo; este nuevo método de autenticación mantiene riesgos considerables, el riesgo de que los códigos de verificación dictados o frases de identificación por voz sean escuchados, por un tercero durante el proceso de autenticación y luego imitados por un software malicioso o personas malintencionadas, que luego podrían ser imitados por un software o una persona para realizar un acceso no legítimo. En un inicio este método fue calificado como sencillo de usar, posteriormente fue categorizado como altamente vulnerable debido a los avances actuales en IA, lo que refleja el desafío constante de equilibrar seguridad y conveniencia en la autenticación.

En paralelo, la Identidad Autogestionada (Self-Sovereign Identity, SSI) está redefiniendo el control de los datos, permitiendo combinar sistemas de autenticación con el manejo de acceso en los sistemas de terceros. En este nuevo sistema, cada individuo es como el cerebro que controla el flujo de su información, decidiendo qué compartir, cuándo y con quién. Es como tener un sistema nervioso descentralizado; es decir, sin un tercero externo del sistema que autentique los valores o maneje los datos, donde cada credencial y dato del usuario fluye bajo el control exclusivo del mismo usuario, eliminando intermediarios innecesarios y garantizando la privacidad del manejo de los valores de autenticación y de cada transmisión de datos.

Conclusión: El Futuro del Sistema Nervioso Digital

La identidad digital a futuro funcionará como un sistema nervioso interconectado que se amplía por cada dispositivo que utilizamos, desde nuestros teléfonos móviles hasta robots autónomos y dispositivos IoT. En esta red de interacciones digitales será esencial para nuestra vida cotidiana, donde cada "nodo" o dispositivo que forme parte del ecosistema digital y donde la identidad digital, deberá ser protegido y coordinado con precisión.

Por otra parte, este sistema nervioso digital, en su estado actual, enfrenta un desafío importante: es un ecosistema vulnerable y fragmentado. Al igual que en un sistema biológico, donde los nervios dañados o desconectados pueden llevar a disfunciones en el cuerpo, en el ecosistema digital, la falta de interoperabilidad, las brechas en la regulación y la desigualdad en la infraestructura tecnológica han creado puntos frágiles que amenazan la seguridad y la eficiencia de la identidad digital.

La fragmentación del sistema digital, donde las identidades están dispersas en múltiples plataformas con diferentes niveles de seguridad, es como un sistema nervioso mal coordinado. Esta falta de cohesión dificulta el flujo de la identidad digital entre plataformas, exponiendo a los usuarios a ciberataques, suplantaciones de identidad y pérdida de control sobre sus datos. Esta fragmentación también disminuye la confianza de los ciudadanos en los sistemas digitales, ya que no tienen garantías suficientes sobre la protección y el uso de su información.

Para superar este escenario vulnerable, el futuro del sistema nervioso digital dependerá de nuestra capacidad para fortalecer tanto las tecnologías de autenticación avanzadas como las regulaciones sólidas. Se necesitará un enfoque descentralizado que permita a los usuarios tomar el control total de sus identidades, utilizando tecnologías como el blockchain y SSI (Identidad Autosoberana). Este enfoque, al igual que un sistema nervioso robusto, permitirá que la identidad digital fluya de manera segura y coordinada a través de todos los dispositivos, sin interrupciones.

Asimismo, es fundamental que las regulaciones evolucionen a la misma velocidad que las tecnologías emergentes. Solo con un marco regulatorio sólido que abarque las nuevas realidades tecnológicas podremos proteger de manera efectiva este sistema nervioso digital interconectado y evitar que continúe fragmentado y vulnerable.

Interoperabilidad

La Ley 1928 de 2019 intentó mejorar la interoperabilidad entre las plataformas digitales del Estado, pero todavía es necesario trabajar en la estandarización global para que las identidades digitales puedan moverse de manera segura entre diferentes sistemas y plataformas, tanto nacionales como internacionales.

Blockchain y SSI

La legislación actual tampoco contempla adecuadamente las tecnologías emergentes como el blockchain o las identidades autogestionadas (SSI), lo que limita la capacidad de los usuarios para tener un control más descentralizado y seguro de su identidad digital. Actualizar las normativas para incluir estas tecnologías será fundamental para garantizar la seguridad en un ecosistema digital en constante cambio.

En resumen, el futuro de la identidad digital y su sistema nervioso dependerán de la creación de un ecosistema cohesionado y seguro, donde las tecnologías avanzadas y las regulaciones modernizadas trabajen juntas para proteger nuestras identidades en un mundo cada vez más interconectado. Con estas medidas, será posible restaurar la confianza en el ecosistema digital y asegurar que cada parte del sistema funcione de manera sincronizada y segura.

Referencias

Congreso de la República de Colombia. (2008). Ley 1266 de 2008. https://dapre.presidencia.gov.co/normativa/normativa/LEY%201266%20DEL%2031%20DE%20DICIEMBRE%20DE%202008.pdf

Congreso de la República de Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49936

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013. https://www.sic.gov.co/sites/default/files/files/normatividad/Decreto_1377_2013.pdf

Congreso de la República de Colombia. (2019). Ley 1928 de 2019. https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202019.pdf

Presidencia de la República de Colombia. (2020). Decreto 620 de 2020. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20620%20DEL%2030%20DE%20ABRIL%20DE%202020.pdf

European Parliament. (2016). General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Wang, D., Jiang, R., Sun, W., Zhang, X., Lu, C., & Zou, Y. (2023). Industrial internet identity resolution+5G full connection digital factory research. *Applied Sciences*, 13(8), 4945. https://doi.org/10.3390/app13084945