Capítulo 2

Desafíos y tendencias en la identidad digital para la seguridad de las infraestructuras críticas*

DOI: https://doi.org/10.25062/9786287818002.02

Jaider Ospina Navas

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: En un contexto global marcado por la creciente digitalización, las infraestructuras críticas cibernéticas (ICC) enfrentan importantes desafíos en materia de protección, impulsados por la convergencia entre las tecnologías operativas (TO) y las tecnologías de la información (TI). Este capítulo analiza el papel fundamental de la gestión de la identidad digital en la seguridad de estas infraestructuras, abordando su evolución, vulnerabilidades y tendencias emergentes. Se examinan las ciberamenazas asociadas a la autenticación, la autorización y la suplantación de identidad, así como la interdependencia crítica entre los sistemas físicos y digitales. Asimismo, se presentan soluciones innovadoras basadas en inteligencia artificial, *blockchain,* biometría y autenticación multifactor adaptativa, que fortalecen la resiliencia de las ICC frente a los ciberataques. Por último, se abordan los retos normativos y técnicos que dificultan la adopción de tecnologías avanzadas, destacando la necesidad de marcos abiertos y estrategias integrales que garanticen la continuidad y la seguridad de los servicios esenciales.

Palabras clave: cibernética; ciberriesgos; infraestructura crítica; internet de las cosas; SCADA; tecnologías de la información.

* Capítulo de libro resultado del proyecto de investigación *"Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales"* del grupo de investigación "Ciberespacio Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Jaider Ospina Navas
Doctorando en Sistemas de Información. Magíster en Ciencias de la Información y las Comunicaciones e ingeniero electrónico, Universidad Distrital Francisco José de Caldas, Colombia. Consultor en ciberseguridad y arquitecto en soluciones en la nube.
https://orcid.org/0000-3251-3017 - Contacto: **jaider.ospina@esdeg.edu.co**

Citación APA: Ospina Navas, J. (2025). Desafíos y tendencias en la identidad digital para la seguridad de las infraestructuras críticas. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 43-78). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818002.02

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES
ISBN impreso: 978-628-7602-99-1
ISBN digital: 978-628-7818-00-2
DOI: https://doi.org/10.25062/9786287818002

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

CC BY NC ND

Introducción

En la era de la digitalización, las IC, como las redes de energía, las telecomunicaciones, el transporte y el suministro de agua, se han convertido en sistemas altamente interconectados y automatizados.

Esta creciente dependencia de la tecnología digital, si bien mejora la eficiencia operativa, también incrementa su vulnerabilidad ante amenazas cibernéticas. En este contexto, la gestión de la identidad digital de los actores que interactúan con estas infraestructuras adquiere un papel fundamental en su protección y seguridad.

El propósito de este artículo es analizar el rol de la identidad digital en la protección de las ICC, examinando los desafíos que enfrenta, así como las tendencias emergentes en ciberseguridad y ciberdefensa, orientadas a fortalecer la resiliencia de estos sistemas frente a posibles ciberataques.

Identidad digital y su importancia de ciberseguridad para las infraestructuras críticas cibernéticas

Infraestructuras críticas cibernéticas vs. infraestructuras críticas

Este documento centra su análisis en las ICC, entendidas como los componentes digitales que controlan o gestionan las IC, por lo que resulta pertinente identificar sus diferencias y similitudes.

Infraestructuras críticas

Las IC son sistemas físicos y virtuales esenciales para el funcionamiento de una sociedad, como las redes eléctricas, el suministro de agua, el transporte y las telecomunicaciones (Rinaldi et al., 2001).

Estos sistemas son vitales para el bienestar económico, la seguridad y la salud pública de una nación. Por esta razón, su interrupción o destrucción podría tener un impacto significativo en la seguridad nacional, la estabilidad económica y el tejido social.

Según la Directiva 2008/114/CE, las IC son elementos vitales para el mantenimiento de las funciones sociales, así como para la salud, la seguridad y el bienestar económico. La USA PATRIOT Act las define de la siguiente manera:

> Sistemas y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de estas. (Moteff & Parfomak, 2004)

El Proyecto de Ley 245 de 2019 define las IC de la siguiente manera:

> Aquellas instalaciones, redes, servicios esenciales, y equipos físicos y de tecnología de la información, en los sectores público y privado, cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las instituciones del Estado, en todos sus niveles de administración pública.

En Colombia, al igual que en otros países, la importancia de definir y proteger estas infraestructuras ha sido ampliamente reconocida. Diversos estudios destacan la necesidad de contar con una legislación clara que garantice su protección y conservación (Alirio et al., 2016).

Infraestructuras críticas cibernéticas

Las ICC son los sistemas y activos digitales que controlan, gestionan y soportan el funcionamiento de las IC a través de medios digitales, como las redes de comunicación y los sistemas informáticos interconectados.

Según *la Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia*, las ICC son:

> […] las infraestructuras estratégicas soportadas por tecnologías de la información y las comunicaciones (TIC) o tecnologías de operación (TO), cuyo funcionamiento es indispensable, por lo que su suspensión, afectación, o destrucción tendría un grave impacto o efecto perturbador sobre los servicios esenciales del Estado. (Comando Conjunto Cibernético [CCOC], 2015)

En esencia, las ICC son los componentes digitales que hacen posible el funcionamiento eficiente y seguro de las infraestructuras físicas. Por ejemplo, una red eléctrica moderna es controlada y gestionada por sistemas cibernéticos que monitorean el flujo de la electricidad y garantizan un suministro continuo y seguro mediante acciones de gobernanza y mecanismos de aseguramiento.

Una característica relevante de las ICC es su capacidad para generar un efecto en *cascada,* con repercusiones significativas en otras IC. Por ejemplo, una falla en el sistema de semaforización podría incrementar considerablemente la cantidad de accidentes de tránsito, lo que, a su vez, saturaría el sistema hospitalario de emergencias y provocaría un uso excesivo de la red celular, comprometiendo su funcionamiento o incluso llevándola al colapso.

Diferencias entre las infraestructuras críticas y las infraestructuras críticas cibernéticas

Las IC suelen ser tangibles, como una planta de tratamiento de agua, una central hidroeléctrica o un reactor nuclear. En cambio, las ICC son intangibles y están compuestas por un *software,* un flujo de datos y redes de comunicación.

Para comprender los elementos que conforman el ecosistema de las IC, es pertinente considerar la siguiente definición de infraestructura estratégica (IE): "Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre los cuales se soporta el funcionamiento de los servicios esenciales" (CCOC, 2015).

La figura 1 permite visualizar la relación entre las definiciones previamente mencionadas. Se observa que las infraestructuras se dividen en dos categorías: físicas y cibernéticas. Estas últimas, para efectos del presente estudio, se clasifican en críticas y no críticas.

Figura 1. *Diagrama de conceptos*

Fuente: Tomado de la CCOC (2015).

Finalmente, es importante destacar la interrelación entre las infraestructuras previamente mencionadas, la cual se establece mediante un acoplamiento derivado de las funciones de gobernanza, monitoreo y comunicación provistas por las ICC. Esto da lugar a la conformación de sistemas físico-cibernéticos (CPS) altamente interdependientes (Palleti et al., 2021).

Los resultados expuestos revelan una correlación directa entre la disrupción de las IC y las consecuencias adversas en los sistemas físicos. En este contexto, un ataque cibernético dirigido contra una red de control industrial puede desencadenar interrupciones significativas en procesos críticos, como la generación de energía o el transporte, lo que evidencia la intrincada interdependencia entre ambos dominios (Lewis, 2010). Esta vulnerabilidad subraya la imperiosa necesidad de comprender dicha correlación y de fortalecer la resiliencia de las IC ante amenazas cibernéticas (Vesić & Bjelajac, 2023).

Protección de las infraestructuras críticas

La protección de las ICC es fundamental debido a su estrecha relación con las IE y los servicios esenciales. Las ICC, sustentadas en las TIC y las TO, desempeñan un papel crucial en el mantenimiento de dichos servicios. Su interrupción, daño o destrucción puede tener un impacto significativo y altamente disruptivo, comprometiendo la estabilidad social y económica.

Las IE comprenden las instalaciones, redes, sistemas y equipos, tanto físicos como tecnológicos, que son necesarios para el funcionamiento continuo de los servicios esenciales. Estos servicios, vitales para el desarrollo de actividades sociales y económicas, dependen de las TIC y las TO.

Un fallo en su infraestructura podría paralizar actividades clave, lo que subraya la necesidad de una protección integral y coordinada de las IC y las IE, a fin de garantizar la continuidad y resiliencia de los servicios esenciales del país (Ashibani & Mahmoud, 2017; Chen & Abu-Nimeh, 2011; Humayed et al., 2017).

La función del Estado y las Fuerzas Armadas en la protección de las infraestructuras críticas

En términos generales, la protección de las IC se considera una responsabilidad del Estado, dado que son esenciales para garantizar el bienestar de la sociedad y el funcionamiento de la economía.

El Estado, a través de sus políticas y regulaciones, establece los marcos legales y operativos necesarios para identificar, evaluar y mitigar los riesgos que puedan afectar a estas infraestructuras. Además, coordina esfuerzos entre diversas entidades gubernamentales y privadas, a fin de implementar medidas de seguridad efectivas.

Según Juárez (2024), la seguridad humana y la protección de las IC requieren un enfoque integral que combine la promoción del desarrollo humano con la capacidad operativa de las instituciones estatales.

Por su parte, las Fuerzas Armadas desempeñan un papel crucial en la protección de las IC, especialmente en situaciones de emergencia o conflicto. Su capacidad para movilizar recursos y personal especializado garantiza una respuesta rápida y efectiva ante amenazas que puedan comprometer la seguridad nacional. Asimismo, su vasta experiencia en planificación estratégica y operaciones tácticas es fundamental para la implementación de medidas preventivas y correctivas.

De este modo, las Fuerzas Armadas amplían su misión tradicional hacia el quinto dominio y la defensa híbrida, lo que les permite intervenir en la protección de las IC de tres maneras:

1. Ciberdefensa nacional
    - Los comandos militares son responsables de proteger las redes críticas del Estado, como las de defensa e inteligencia. Además, colaboran con entidades civiles cuando se enfrentan a amenazas complejas.

- Realización de operaciones ofensivas y defensivas para desarticular actores hostiles.

2. Respuesta ante emergencias
   - En caso de sabotaje, ataques físicos o digitales, las Fuerzas Armadas pueden:
     - Asegurar las instalaciones críticas.
     - Proteger al personal técnico.
     - Apoyar la restauración de servicios básicos.
3. Disuasión estratégica
   - El despliegue de capacidades militares en ciberdefensa y protección física tiene un efecto disuasorio sobre grupos terroristas, cibercriminales o Estados hostiles.

Características de las infraestructuras críticas cibernéticas

Las ICC constituyen un entramado complejo y heterogéneo de sistemas que integran las TI y las TO, como las redes industriales, el internet de las cosas (IoT), el internet industrial de las cosas (IIoT), los sistemas de control industrial (SCI) y los sistemas SCADA.

Esta convergencia tecnológica plantea una serie de desafíos únicos en términos de seguridad debido a la diversidad de protocolos, interfaces y niveles de criticidad de los componentes que las conforman (Kebande & Awad, 2024).

Algunos de sus focos de vulnerabilidad son:

- Vulnerabilidades de la seguridad en la capa de percepción: esta capa, responsable de recopilar datos del entorno físico a través de sensores y actuadores, es susceptible a diversos ataques, incluyendo:
  - Manipulación y bloqueo que interrumpen la transmisión de datos entre los nodos.
  - Los adversarios capturan los nodos y, en consecuencia, obtienen control sobre los dispositivos.
  - Mediante la inyección de datos falsos, los adversarios buscan manipular las lecturas de los sensores.
  - Clonación de etiquetas para crear dispositivos falsos.
  - Acceso no autorizado a sistemas con el fin de obtener información sensible (Farooq et al., 2015).

- Vulnerabilidades de la seguridad en la capa de red: esta capa, encargada de la comunicación entre los diferentes componentes del sistema, es susceptible a amenazas en los protocolos de comunicación, transporte y *routing* (Aydin & Sertbaş, 2022; Farooq et al., 2015). Estas amenazas incluyen:
  - Inseguridad en los protocolos que permite a los atacantes explotar las debilidades de los protocolos de comunicación, como la falta de autenticidad.
  - El *spoofing* de RFID consiste en la suplantación de nodos RFID legítimos.
  - Ataques de *sinkholing* (sumideros de DNS) que redirigen el tráfico hacia un nodo malicioso.
  - Cuellos de botella en la comunicación entre los nodos, lo que provoca retrasos o interrupciones en la transmisión de los datos, afectando así la disponibilidad y degradando el servicio.
  - Ataques de tipo *hombre en el medio* (MITM) que interceptan y manipulan la comunicación entre dos nodos, comprometiendo la disponibilidad, la integridad y la confidencialidad.
- Vulnerabilidades de la seguridad cibernética: la integración de los entornos de las TI y las TO amplía la superficie de ataque, aumentando la vulnerabilidad de las redes, los SCI, las aplicaciones y los servidores basados en sistemas industriales, así como de los recursos en entornos como Cloud, Edge y Fog Computing (Maglaras et al., 2022.) Esta expansión incrementa la probabilidad de puntos de ataque mediante:
  - Ataques de suplantación de identidad.
  - Ataques de *phishing.*
  - Inyección de *malware.*
  - Secuestro de sesión.
  - Denegación de servicio (DoS).
  - Fallos en el SCI.
  - Robo de datos.

- Vulnerabilidades de la seguridad física: las características del IoT y de los dispositivos inteligentes empleados en las IC incluyen, *a priori,* elementos físicos con restricciones de energía y potencia. La seguridad de los sensores, los actuadores, los SCI y los SCADA es fundamental, ya que procesan datos en tiempo real que afectan tanto la infraestructura física como a los usuarios. Sin embargo, la implementación de medidas de seguridad y

monitoreo se ve limitada por estas restricciones, lo que exacerba las vulnerabilidades existentes y tiene un impacto directo sobre aspectos como lo mencionados a continuación:

- La manipulación de los dispositivos puede modificar las lecturas de los sensores o alterar el comportamiento de los actuadores.
- El bloqueo del servicio tiene el potencial de paralizar el funcionamiento normal del sistema.
- El robo de información puede poner en riesgo datos confidenciales.
- El compromiso de un dispositivo otorga a los atacantes la capacidad de controlar dispositivos críticos.
- La alteración del sistema de control puede tener consecuencias devastadoras, incluyendo la pérdida de vidas humanas.
- El compromiso del *firmware* puede alterar el funcionamiento del dispositivo.
- La falta de disponibilidad del servicio tiene el potencial de interrumpir operaciones críticas.

Normatividad aplicable al aseguramiento de las infraestructuras críticas

A nivel mundial y nacional, se han desarrollado diversas iniciativas, a fin de garantizar la protección de las IC (tabla 1).

Tabla 1. *Normatividad aplicable al aseguramiento de las infraestructuras críticas*

Ámbito	Normativa	Enfoque principal	Detalles adicionales
Internacional	Marco de Ciberseguridad del NIST (CFS) 2.0	Estándares, directrices y mejores prácticas, a fin de gestionar los riesgos de ciberseguridad aplicables a IC.	• Proporciona un enfoque flexible y basado en riesgos para que las organizaciones adapten las medidas de seguridad a sus necesidades. • Consta de seis funciones principales: identificar, proteger, detectar, responder, recuperar y gobernar. • Es una referencia internacional utilizada para la gestión de la ciberseguridad en las IC.
Internacional	*Presidential Policy Directive 21*	IC nacionales.	• Fortalecer la seguridad y la resiliencia en 16 sectores esenciales. • Enfocado en la colaboración interinstitucional y una respuesta integrada.

Ámbito	Normativa	Enfoque principal	Detalles adicionales
Internacional	Directiva NIS2	Armonización de las medidas de ciberseguridad en la Unión Europea, abarcando sectores críticos como energía, transporte, salud y banca.	• Fortalecer la resiliencia y la supervisión de operadores esenciales. • Establece requisitos más estrictos en gestión de riesgos, notificación de incidentes y supervisión. • Fomenta la cooperación y el intercambio de información entre los Estados miembros.
Internacional	Convenio de Budapest sobre la Ciberdelincuencia	Tratado internacional orientado a fomentar la cooperación entre las naciones, a fin de combatir los delitos informáticos, incluidos aquellos que amenazan a las IC.	• Armonizar las legislaciones nacionales en materia de delitos informáticos. • Establece procedimientos que promuevan la cooperación internacional en la investigación y el enjuiciamiento por delitos informáticos. • Contempla disposiciones sobre la obtención de pruebas electrónicas y la asistencia entre Estados.
Nacional	CONPES 3995	La Política de Seguridad Digital tiene como objetivo fortalecer la capacidad del país para prevenir, detectar y responder a los riesgos y amenazas en el entorno digital, con especial énfasis en la protección de las IC.	• Define los objetivos y las estrategias que orientan la protección y el fortalecimiento de la seguridad digital en Colombia. • Establece un marco para la cooperación entre el sector público y el sector privado. • Promueve el desarrollo de capacidades en materia de seguridad digital.
Nacional	Decreto 338 de 2022	Establece lineamientos para fortalecer la gobernanza de la seguridad digital; identificar ICC y servicios esenciales; gestionar los riesgos asociados; y responder eficazmente a los incidentes de seguridad digital.	• Busca fortalecer la coordinación entre las entidades del Estado en materia de seguridad digital. • Define las responsabilidades de las partes interesadas en la protección de las ICC. • Establece la obligación de implementar medidas de seguridad para salvaguardar los sistemas de información y los datos.
Nacional	Decreto 472 de 2024	Define las directrices para la identificación, designación y protección de las ICC en Bogotá.	• Establece un marco para la gestión de riesgos y la respuesta a incidentes de seguridad cibernética, específicamente en el contexto de las ICC. • Define las responsabilidades de las entidades distritales en la protección de las ICC.

Fuente: Elaboración propia.

A pesar de los avances significativos, Colombia aún carece de una legislación que garantice la protección de las IC, tanto físicas como digitales. A nivel internacional, la tendencia apunta hacia la integración de la protección física, cibernética y de datos personales bajo un marco de resiliencia nacional. En este contexto, normativas como la NIS2 y el NIST CSF se consolidan como referencias clave para la formulación de políticas públicas en América Latina.

Gestión de la identidad en las infraestructuras críticas cibernéticas

Al igual que cualquier sistema de información o aplicación cibernética, toda ICC utiliza mecanismos de autenticación y autorización basados en la gestión de identidades, los cuales se agrupan bajo el concepto de *identidad digital.* Esta última permite o deniega acciones específicas de autenticación y autorización en los distintos componentes de una IC.

A continuación, se evalúan los requisitos y aspectos clave de la gestión de identidad en las ICC.

Requisitos para la gestión de la identidad en las infraestructuras criticas cibernéticas

En las ICC, la gestión de la identidad es un proceso fundamental para garantizar la seguridad y la continuidad de los servicios esenciales. Este proceso incluye la autenticación, que consiste en verificar la identidad de un usuario o dispositivo, y la autorización, que determina los permisos y privilegios otorgados a una entidad autenticada.

Dada la naturaleza crítica de estos sistemas, la gestión de la identidad debe ser robusta y adaptable para hacer frente a amenazas cibernéticas en constante evolución. Sin embargo, en estas infraestructuras, la convergencia entre las TI y las TO plantea desafíos únicos, como la heterogeneidad de los sistemas y la necesidad de equilibrar la seguridad y la usabilidad.

Investigaciones recientes han destacado la importancia de implementar soluciones de gestión de identidad basadas en estándares, que integren tecnologías como la autenticación multifactor (MFA) y la gestión de privilegios. A diferencia de los enfoques tradicionales, estas soluciones ofrecen una mayor protección contra amenazas como el robo de credenciales y los ataques de fuerza bruta.

- Definición de privilegios: la política de control de acceso más adecuada debe asignar permisos y derechos con base en los roles, las tareas y los atributos de los usuarios. Un principio clave es la política de menor

privilegio, que establece que los usuarios solo deben contar con los accesos estrictamente necesarios para desempeñar sus funciones.
En este contexto, el control de acceso basado en atributos (ABAC) permite definir privilegios con un alto nivel de granularidad, ya que las decisiones relacionadas con el acceso se toman a partir de condiciones booleanas aplicadas a los valores de distintos atributos. Esta flexibilidad es fundamental para garantizar la seguridad en los esquemas de control de acceso de los CPS.

- MFA: los esquemas de autenticación basados en un solo factor no son lo suficientemente resistentes como para hacer frente a ataques cibernéticos. Por esta razón, se requiere la combinación de dos o más factores, como *lo que eres* (huellas dactilares, escaneo del iris, etc.), *lo que sabes* (*passwords*), y *lo que tienes* (tokens), con el fin de incrementar la robustez del proceso. Esta estrategia es esencial para reducir falsos positivos y dificultar los intentos de acceso no autorizado, ya que permite establecer múltiples niveles de autenticación.
- Proceso de *hashing* dinámico y contraseñas fuertes: periódicamente, las contraseñas deben ser sometidas a un proceso de rehashing, utilizando un nuevo *nonce* dinámico para cada usuario y funciones *hash* criptográficas seguras, como SHA-3 y SHA-2 (variante 512). Este enfoque ayuda a prevenir ataques como los de las tablas arco iris, los de colisión o de cumpleaños.
- Auditoría segura y protegida: para mitigar los intentos de acceso no autorizado desde el interior de un CPS y preservar la evidencia digital de ataques tanto internos como externos, es necesario contar con un sistema de gestión de auditoría que recopile y almacene los registros en un sistema distribuido. Este aspecto, relacionado con la auditoría en ciberseguridad, es perentorio.
- Soluciones no criptográficas mejoradas: para prevenir brechas de seguridad derivadas de la explotación de vulnerabilidades, es fundamental implementar sistemas híbridos (IDS/IPS) o basados en IA, utilizando algoritmos de aprendizaje automático, junto con *firewalls* avanzados y *honeypots* dinámicos. Estos elementos deben ser considerados como un ecosistema dinámico y altamente interactivo.
- Copias de seguridad seguras y verificadas: es esencial garantizar la disponibilidad de los datos del CPS y prevenir su destrucción o alteración. Por esta razón, es necesario implementar soluciones de protección eficientes y ligeras que aseguren la integridad de las copias de seguridad. Así, se preserva su robustez frente a ataques DoS/DDoS y *ransomware*.

- Esfuerzos forenses: son esenciales para la recolección de evidencias. Es necesario implementar soluciones innovadoras que neutralicen las técnicas antiforenses, garantizando así la preservación de la evidencia digital y reduciendo al mínimo los intentos de reconocimiento por parte de los atacantes.

El objetivo de estos requisitos es garantizar la integridad, confidencialidad y disponibilidad de los sistemas ciberfísicos ante diversas amenazas y ataques, asegurando así su operación en un entorno seguro y confiable.

Conceptualización de la identidad digital

La identidad digital hace referencia a la representación electrónica de la información personal y profesional que define a un individuo o entidad en entornos virtuales. Está compuesta por un conjunto de atributos digitales, como credenciales de acceso, perfiles de usuario, historiales de transacciones y cualquier otro dato que pueda ser utilizado para identificar a una persona o a un dispositivo dentro de un sistema digital (Elwell, 2014).

Con respecto a la ciberseguridad, la identidad digital es un componente esencial, ya que determina quién puede acceder a qué recursos y bajo qué condiciones. En términos generales, la identidad digital está compuesta por dos elementos fundamentales: la autenticación, que verifica la identidad del usuario, y la autorización, que permite o restringe el acceso a los recursos.

Otra definición relevante es la de credenciales digitales, que hace referencia a los mecanismos utilizados para autenticar y verificar una identidad digital. Estas adoptan diversas formas, como contraseñas, certificados digitales, claves criptográficas o datos biométricos.

Con la creciente digitalización de las IC, el control efectivo de estas credenciales es crucial para la seguridad operativa, ya que cualquier vulnerabilidad podría ser aprovechada por actores maliciosos que buscan acceder indebidamente a sistemas sensibles (NIST, 2018).

Evolución histórica

El concepto de *identidad digital* ha evolucionado considerablemente. En un principio, las identidades digitales se limitaban a nombres de usuario y contraseñas simples, un método de autenticación que, aunque eficaz en su momento, ha demostrado ser insuficiente para satisfacer las necesidades de seguridad actuales.

En los primeros sistemas informáticos, las identidades se gestionaban de forma centralizada. Si bien esto facilitaba su administración, también introducía vulnerabilidades, como el riesgo de un único punto de fallo (Fang et al., 2009).

Con el auge de la conectividad global y el desarrollo del Internet en la década de 1990, surgió la necesidad de mejorar las técnicas de autenticación y autorización. A medida que las organizaciones comenzaron a depender de sistemas más complejos y distribuidos, las contraseñas dejaron de ser seguras.

Fue entonces cuando se introdujo la autenticación de dos factores (2FA) y, más tarde, la MFA, que incorporó elementos adicionales, como *lo que soy* (huellas dactilares y reconocimiento facial), *lo que tengo* (tokens de seguridad) y *lo que sé* (contraseñas) (Roman et al., 2013).

Esta evolución ha sido impulsada por el crecimiento de la computación en la nube, en la niebla y el IoT, así como por las infraestructuras distribuidas, que requieren una gestión descentralizada o itinerante de las identidades digitales.

En las últimas dos décadas, ha surgido un enfoque más sofisticado y seguro para la gestión de identidades digitales, basado en criptoidentidades y *blockchain.* Estas tecnologías permiten una gestión descentralizada, proporcionando a los usuarios un mayor control y seguridad sobre su información personal (Zhang et al., 2020).

Simultáneamente, la IA y el aprendizaje automático se utilizan para detectar patrones anómalos en el comportamiento de las identidades digitales, lo que refuerza la prevención de ataques como la suplantación de identidad y el acceso no autorizado.

Datos como los lugares frecuentados, los tipos de comercio, los artículos adquiridos y la frecuencia de tipeo se convierten en indicadores clave para definir el comportamiento esperado, generando métricas de desviación que permiten identificar posibles violaciones a la seguridad.

La evolución de la identidad digital refleja una adaptación constante a las crecientes amenazas a la seguridad cibernética y a la complejidad de los sistemas interconectados. En el ámbito de las ICC, esta evolución ha sido acelerada, debido a que la seguridad de estos sistemas es fundamental para garantizar la continuidad de los servicios esenciales de un país.

Urge generar alertas sobre el rezago tecnológico que afecta a las IC de la mayoría de los países, lo que las hace altamente vulnerables debido a la convergencia forzada de las TI y las TO, así como a la falta de un componente de ciberseguridad adecuado.

Relevancia actual de la identidad digital

La identidad digital, responsable de la autenticación y del acceso a los CPS, constituye el pilar sobre el cual se asientan las políticas de ciberseguridad en IC, previniendo el acceso no autorizado.

Una gestión adecuada de la identidad digital no solo facilita el control del acceso a sistemas sensibles, sino que también protege la integridad y confidencialidad de los datos. Las amenazas más comunes, como la suplantación de identidad y el uso indebido de credenciales robadas, destacan la necesidad de una gestión robusta y actualizada (Ponemon Institute, 2021).

Con el aumento de la digitalización, la importancia de la identidad digital trasciende el ámbito técnico. La ética y la privacidad de la identidad digital se han convertido en áreas de gran preocupación, especialmente en las IC, dado que un acceso indebido podría comprometer tanto los datos personales como la seguridad física de las instalaciones (Elwell, 2014).

La implementación de regulaciones como la Ley 1273 de 2009 y el Reglamento General de Protección de Datos (Parlamento Europeo, 2016) subraya la necesidad de una gestión segura y ética de las identidades digitales. Esto requiere que las organizaciones no solo acaten las normativas legales, sino que también garanticen la protección de los derechos de los usuarios.

Desafíos actuales en la identidad digital

La gestión de la identidad digital es fundamental para garantizar la seguridad y resiliencia de las IC ante amenazas cibernéticas. Sin embargo, enfrenta desafíos importantes, como la complejidad de los procesos de autenticación y autorización, la protección de la privacidad, la interoperabilidad entre sistemas heterogéneos y la prevención de la suplantación de identidad.

Las tendencias emergentes en IA, *blockchain* y autenticación sin contraseñas abren paso a soluciones más seguras y eficientes. Sin embargo, su éxito depende, en gran medida, de la coordinación organizacional y la adopción de estándares abiertos, la implementación de tecnologías avanzadas de detección y mitigación, y el fomento de una cultura de seguridad tanto a nivel organizacional como individual.

Autenticación y autorización

La autenticación permite el acceso a un sistema, mientras que la autorización define los privilegios otorgados. En esencia, estos procesos constituyen el objetivo fundamental de una identidad digital y representan un desafío significativo ante

la creciente sofisticación de las amenazas que buscan vulnerar la integridad, la confidencialidad y la disponibilidad de los sistemas. La autenticación garantiza que solo los usuarios legítimos accedan a los sistemas críticos, mientras que la autorización delimita sus acciones.

Las IC demandan soluciones de autenticación avanzadas, como la MFA, que combina factores de conocimiento (contraseñas), posesión (dispositivos) y biometría (huellas dactilares y reconocimiento facial) (Roman et al., 2013). Sin embargo, la implementación de la MFA en entornos operativos sensibles puede ser compleja y generar fricciones, especialmente en situaciones de emergencia, donde el acceso rápido y seguro es crucial.

Se recomienda implementar sistemas de autorización multinivel que requieran múltiples fuente de confirmación. Sin embargo, al igual que en el caso anterior, este enfoque puede generar complicaciones en situaciones de emergencia que demanden una respuesta rápida.

Por otro lado, la autorización demanda un control granular que permita administrar las acciones permitidas a cada usuario según su rol en la infraestructura. Los sistemas basados en políticas de control de acceso, como el Role-Based Access Control (RBAC) o el Attribute-Based Access Control (ABAC), son fundamentales para garantizar la seguridad de estos sistemas.

Sin embargo, la integración progresiva de las IC con tecnologías emergentes, como el IoT, incrementa exponencialmente la cantidad de dispositivos y actores que requieren autenticación y autorización, lo que, a su vez, eleva la complejidad y el riesgo de fallos en la seguridad.

Privacidad y protección de datos

La gestión de la identidad digital plantea desafíos significativos en materia de privacidad y protección de datos. Este proceso implica el manejo de grandes volúmenes de información personal y profesional, los cuales son susceptibles a accesos no autorizados y posibles violaciones de la confidencialidad.

En el contexto de las IC, esta información puede incluir datos sensibles de empleados, contratistas o usuarios que acceden a las redes. Además, como se mencionó anteriormente, la mayoría de estas infraestructuras están sujetas a estrictas regulaciones en materia de privacidad, como el Reglamento General de Protección de Datos, la Ley 1581 de 2012 y la Ley 1273 de 2009, las cuales exigen un tratamiento seguro y ético de los datos personales.

El incumplimiento de estas regulaciones, ya sea por ciberataques o por una gestión inadecuada de las identidades digitales, puede tener graves consecuencias legales y financieras para las organizaciones encargadas de gestionar las IC (O'Reilly et al., 2021). Además, la vulneración de la privacidad pueden erosionar la confianza de los empleados y el público en general, comprometiendo la integridad y la fiabilidad de los sistemas.

Para mitigar estos riesgos, es necesario que las organizaciones implementen técnicas avanzadas de cifrado y anonimización de datos, junto con políticas de protección de datos que garanticen el cumplimiento de las normativas vigentes en materia de privacidad.

Interoperabilidad entre sistemas

La complejidad inherente a las ICC, compuesta por sistemas heterogéneos operados por múltiples entidades o fabricantes, representa un obstáculo para la implementación de soluciones coherentes y estandarizadas. Esta fragmentación también amplifica los riesgos asociados a la cadena de suministro.

En este contexto, la interoperabilidad es fundamental para garantizar una autenticación consistente de los usuarios en diversas plataformas y dispositivos, sin sacrificar la seguridad ni la eficiencia operativa.

La falta de estándares universales en la gestión de la identidad digital agrava este problema. A menudo, las organizaciones utilizan sistemas de autenticación y autorización incompatibles, lo que puede dar lugar a brechas de seguridad o a la necesidad de desarrollar soluciones *ad hoc* para integrar sistemas heterogéneos (Suleski et al., 2023; Wang & Zhao, 2023; Zhang et al., 2020).

Una posible solución radica en la adopción de estándares abiertos, como OAuth 2.0 y OpenID Connect, que facilitan la interoperabilidad y permiten gestionar las identidades digitales, de manera más flexible y segura, en entornos heterogéneos. Sin embargo, la implementación de estos estándares demanda un compromiso y una coordinación sustancial entre las partes interesadas.

Prevención de la suplantación de identidad

La suplantación de identidad representa un riesgo significativo para la seguridad de las ICC, especialmente en lo que respecta a los procesos de autenticación y autorización. Los atacantes pueden robar o falsificar credenciales para hacerse pasar por usuarios legítimos y acceder a sistemas y redes sensibles.

El *phishing,* el robo de contraseñas y la explotación de vulnerabilidades en los sistemas de autenticación y protocolos de comunicación son algunos de los

métodos más utilizados para llevar a cabo este tipo de ataques (Shameli-Sendi et al., 2016).

Para mitigar estos riesgos, es fundamental implementar enfoques avanzados de detección de anomalías, en los que la IA y el aprendizaje automático desempeñan un papel clave. Estas tecnologías analizan patrones de comportamiento en tiempo real, identificando actividades sospechosas indicativas de suplantación de identidad.

Por ejemplo, si un usuario accede a un sistema desde una ubicación inusual o realiza acciones que no coinciden con su comportamiento habitual, el sistema puede bloquear el acceso o generar alertas. Este tipo de soluciones adaptativas y proactivas es cada vez más necesario para proteger las identidades digitales de ataques sofisticados.

Además, las soluciones sin contraseñas, basadas en claves criptográficas o biometría, están ganando popularidad debido a su capacidad para mitigar los riesgos asociados a las contraseñas tradicionales, que son susceptibles a suplantaciones y robo. Estas tecnologías proporcionan una capa adicional de seguridad al eliminar uno de los puntos más exánimes en los procesos de autenticación: el uso de contraseñas débiles o filtradas.

Impacto de las amenazas cibernéticas en la identidad digital

El crecimiento de las ICC y la dependencia de identidades digitales ha incrementado el riesgo de ataques cibernéticos. Factores como la hiperconectividad —es decir, el aumento de dispositivos conectados a un sistema— y la administración remota a través de redes de comunicación han ampliado significativamente la superficie de ataque. Esto ha dado lugar a la aparición de nuevas amenazas, siendo los ataques dirigidos a la identidad digital una de las formas más comunes y efectivas de comprometer estos sistemas.

A continuación, se presentan las tipologías de ataques cibernéticos y algunos estudios de caso relevantes.

Tipologías de ataques cibernéticos

Las ciberamenazas contra la identidad digital se clasifican en tipologías que explotan las vulnerabilidades en los procesos de autenticación, autorización y protección de datos.

A continuación, se analizan las más comunes:

- *Phishing* y *spear phishing:* técnicas de ingeniería social diseñadas para engañar a los usuarios y obtener sus credenciales de acceso. La principal

diferencia entre el *spear phishing* y el *phishing* radica en que el primero adopta un enfoque más dirigido, en lugar de centrarse en la calidad.
En el contexto de las IC, los ataques de *spear phishing* suelen estar dirigidos a empleados con acceso privilegiado. Al comprometer sus credenciales, los atacantes pueden obtener acceso a sistemas sensibles.

- Ataques de fuerza bruta y *credential stuffing:* los ataques de fuerza bruta consisten en probar repetidamente combinaciones de nombres de usuario y contraseñas hasta encontrar la correcta. Por otro lado, el *credential stuffing* implica el uso de credenciales robadas de otras plataformas para intentar acceder a un sistema.
  Ambos métodos explotan las malas prácticas en la gestión de contraseñas, como la reutilización de credenciales en múltiples sistemas. En el caso de los ataques de fuerza bruta, una forma efectiva de contrarrestarlos es mediante *el bloqueo de sesión.*
- Ataque de MITM: estos ataques interceptan las comunicaciones entre un usuario y el sistema, lo que permite al atacante capturar credenciales en tiempo real o interceptar el flujo de datos. Esto puede afectar la disponibilidad, la confidencialidad y la integridad, dependiendo de cómo se manipulen las unidades de datos del protocolo (PDU). En el contexto de las IC, los ataques MITM pueden comprometer los SCI, que dependen de comunicaciones seguras.
- Suplantación de identidad: implica la creación de identidades falsas o el uso de credenciales robadas para hacer pasar por un usuario legítimo. Este tipo de ataque puede tener consecuencias devastadoras en las IC, ya que permite el acceso subrepticio a sistemas sensibles.
- Explotación de vulnerabilidades en *software* de autenticación: las fallas en los sistemas de autenticación, como las debilidades en la implementación de la MFA o en los protocolos de cifrado, pueden ser explotadas por los atacantes para acceder a identidades digitales y a recursos críticos.

Estudios de caso relevantes

Algunos estudios de caso destacan el impacto de las amenazas cibernéticas en la identidad digital y la seguridad de las IC (tabla 2).

Tabla 2. *Casos de afectación a la identidad digital y su impacto sobre las ICC*

Año	País	Infraestructura crítica afectada	Tipo de ataque	Compromiso de la identidad digital	Impacto
2010	Irán	Planta nuclear de Natanz (Irán)	*Malware* (Stuxnet)	Uso de certificados digitales falsos	Sabotaje de centrifugadoras nucleares
2015	Ucrania	Red eléctrica	Ataque APT (BlackEnergy)	Suplantación de identidades administrativas	Apagones masivos en varias regiones
2019	Noruega	Norsk Hydro (Industria metalúrgica)	*Ransomware* (LockerGoga)	Robo de credenciales	Paralización de operaciones a nivel mundial
2021	EE. UU.	Ataque a Colonial Pipeline (energía)	*Ransomware*	Acceso a través de credenciales comprometidas	Cierre temporal del suministro de combustible
2021	EE. UU.	Planta de agua en Oldsmar, Florida	Acceso remoto no autorizado	Uso indebido de TeamViewer sin 2FA	Intento de envenenamiento del agua potable
2022	Costa Rica	Ministerios y servicios públicos	*Ransomware* (Conti)	Acceso vía a cuentas comprometidas	Paralización de sistemas estatales por semanas
2023	Colombia	EPS Sanitas (salud)	Ciberataque tipo *ransomware*	Posible uso de accesos internos	Afectación a atención médica y fuga de datos personales
2024	Reino Unido	NHS (sistema de salud)	*Phishing* masivo y *ransomware*	Robo de credenciales del personal médico	Fuga de información clínica y su impacto en la atención médica

Fuente: Adaptado de Beerman et al. (2023); Lee et al. (2016) y Zhang et al. (2020).

- Ataque a Colonial Pipeline (2021): este ataque es considerado uno de los más graves contra las IC en los últimos años. Un grupo de *ransomware*, conocido como *DarkSide*, comprometió las credenciales de una cuenta de acceso remoto, lo que permitió a los atacantes infiltrarse en los sistemas de la empresa.

  El vector inicial fue una contraseña filtrada y reutilizada, que otorgó acceso a una VPN sin MFA. Aunque el objetivo principal del ataque era obtener un rescate financiero, sus repercusiones afectaron gravemente el suministro de combustible en Estados Unidos, destacando la importancia de la identidad digital y la autenticación robusta en la seguridad de las IC (Beerman et al., 2023).

- Ataque a la red eléctrica de Ucrania (2015): este ataque, ejecutado por un grupo de ciberespionaje, comprometió las credenciales de los operadores de los sistemas SCADA, que controlaban sectores de la red eléctrica ucraniana. A través de técnicas de *spear phishing* y *malware* avanzado, los atacantes lograron infiltrarse en los sistemas, provocando apagones que afectaron a más de 230 000 personas (Lee et al., 2016; Zhang et al., 2020). Este incidente demostró cómo las identidades digitales comprometidas pueden ser utilizadas para sabotear las IC y causar daños significativos.
- Ataque a Norsk Hydro (2019): la empresa productora de aluminio fue víctima de un ataque de *ransomware* denominado *LockerGoga,* que afectó a terminales con Windows.
  Los atacantes utilizaron las credenciales robadas para desactivar los sistemas de producción de la compañía, lo que provocó la paralización de las operaciones a nivel mundial. Este incidente demostró, una vez más, el impacto de las vulnerabilidades en las ICC cuando las identidades digitales se ven comprometidas.
- Natanz-Stuxnet (Irán, 2010): aunque el objetivo principal de Stuxnet era el sabotaje físico, robó los certificados digitales legítimos de algunas empresas de *hardware* para hacerse pasar por un *software* confiable. Esto permitió que se propagara sin ser detectado, causando daños a las centrifugadoras nucleares. Este ataque marcó un precedente en el uso de la identidad digital como un vector de intrusión sofisticado.
- Planta de agua en Oldsmar, Florida (2021): un actor no identificado accedió remotamente al sistema de control de una planta de tratamiento de agua mediante TeamViewer y credenciales expuestas. Intentó aumentar los niveles de hidróxido de sodio en el agua potable, pero el ataque fue detenido a tiempo. Este incidente reveló la falta de una autenticación segura y de controles de identidad en las IC municipales.
- EPS Sanitas (Colombia, 2023): el sistema de atención de una de las principales EPS del país sufrió un ciberataque, posiblemente relacionado con elementos del *ransomware*. Aunque los detalles técnicos son limitados, se presume que hubo acceso interno no autorizado o suplantación de identidad, lo cual tuvo un impacto negativo en la atención a los pacientes y expuso datos personales y clínicos sensibles.

Estos casos demuestran que la identidad digital es una de las primeras líneas de defensa en la protección de las IC. Los accesos no autorizados, derivados del

robo de credenciales, la suplantación de identidad o el uso indebido de cuentas internas, son cada vez más comunes.

La implementación de controles como la MFA, la gestión de accesos privilegiados (PAM), la segmentación de redes, la detección temprana de anomalías y la capacitación continua son medidas esenciales que deben ser impulsadas y reguladas por el Estado.

Relevancia del fortalecimiento de la identidad digital

Los estudios de caso demuestran cómo las identidades digitales se han convertido en un vector crucial en los ataques a las IC. Es evidente que, cuando los sistemas de autenticación y autorización no son lo suficientemente robustos, los atacantes pueden aprovechar credenciales comprometidas para tener acceso y controlar sistemas críticos.

Esto resalta la importancia de implementar políticas y tecnologías de seguridad más avanzadas, como la MFA, el monitoreo continuo de la identidad digital y la adopción de tecnologías como *blockchain* (Zhang et al., 2020).

Además, las organizaciones responsables de gestionar las IC deben invertir en la capacitación de su personal, a fin de que comprendan los riesgos asociados con la gestión de identidades digitales y adopten buenas prácticas, como el uso de contraseñas fuertes, la MFA y la supervisión de accesos inusuales. Estas medidas preventivas no solo fortalecen la seguridad, sino que también reducen la probabilidad de que un ataque exitoso a las identidades digitales comprometa toda la infraestructura.

Un aspecto fundamental en el funcionamiento de una IC es la implementación de la autorización multinivel, que exige la confirmación de dos o más fuentes para realizar acciones de alto impacto, como el cierre o la apertura de una compuerta. Este proceso debe seguir una lógica AND (todo o nada).

Tecnologías emergentes y su integración

Las tecnologías emergentes están desempeñando un papel fundamental en la transformación de la gestión de las identidades digitales. A medida que los ataques cibernéticos se vuelven más sofisticados y las amenazas evolucionan, las tecnologías avanzadas, como el *blockchain,* la IA, la biometría y los sistemas de identidad federada, ofrecen nuevas herramientas y enfoques para proteger las identidades digitales y optimizar los procesos de autenticación.

En esta sección, se analiza cómo estas tecnologías emergentes se están integrando en la gestión de las identidades digitales y su impacto en la seguridad de las IC.

Blockchain y gestión de identidades

La tecnología *blockchain* emerge como una solución innovadora para la gestión descentralizada de las identidades digitales. Tradicionalmente, esta gestión ha sido centralizada, por lo que no adolece de vulnerabilidades, como el riesgo de un único punto de fallo, en el que un compromiso de la base de datos central podría afectar a todas las identidades almacenadas.

El *blockchain* ofrece una alternativa distribuida, permitiendo que las identidades digitales sean gestionadas a través de una red descentralizada, lo que dificulta la manipulación y el acceso no autorizado a los datos (Sameera et al., 2024).

En el contexto de las IC, el *blockchain* facilita la creación de identidades soberanas, otorgando a los usuarios un mayor control sobre sus credenciales y eliminando la dependencia de un único proveedor de servicios.

Cada transacción o acceso se registra, de forma inmutable, en la cadena de bloques, garantizando la transparencia y la trazabilidad de las interacciones con los sistemas críticos. Esto es especialmente importante en entornos industriales, donde las identidades de los dispositivos IoT pueden gestionarse, de manera segura, mediante el uso del *blockchain.*

Un ejemplo de aplicación es la integración del *blockchain* en los sistemas SCADA, esenciales para el control y el monitoreo de las IC, como las redes eléctricas y los sistemas de distribución de agua.

Al implementar el *blockchain,* tanto las credenciales de los operadores como los dispositivos pueden ser verificados de manera distribuida, lo que reduce significativamente las posibilidades de suplantación de identidad o accesos no autorizados (Zhang et al., 2020).

Finalmente, esta tecnología posibilita la creación de sistemas autosoberanos, capaces de realizar auditorías de forma local (sin necesidad de recurrir a redes *blockchain* de terceros o integradas a redes WAN).

Para garantizar múltiples puntos de confirmación de acciones de alto impacto, como órdenes convergentes e inclusivas, esta tecnología no solo incrementa los puntos de control, sino que también promueve el uso de contratos inteligentes.

Inteligencia artificial en la autenticación

La IA está revolucionando la forma en que los seres humanos interactúan y comprenden el mundo, y la gestión de identidades digitales no es ajena a esta transformación. Su aplicación es especialmente valiosa en los procesos de autenticación y la detección de amenazas.

Los sistemas de autenticación basados en IA son capaces de analizar grandes volúmenes de datos en tiempo real, identificando patrones de comportamiento anómalos que podrían revelar intentos de acceso no autorizado o ataques en curso.

Los algoritmos de aprendizaje automático permiten que estos sistemas se adapten y mejoren de forma continua, ajustando las políticas de autenticación según el comportamiento habitual del usuario o del dispositivo.

Por ejemplo, si un usuario accede a un sistema crítico desde una ubicación o un dispositivo inusual, el sistema basado en IA puede activar una alerta o exigir una autenticación adicional, como la MFA. Este enfoque ayuda a prevenir la suplantación de identidad y el uso indebido de credenciales comprometidas.

Una aplicación relevante de la IA en las IC es la autenticación adaptativa, que ajusta los niveles de seguridad según el contexto del usuario, como la hora, el dispositivo o la ubicación. Este enfoque no solo reduce los riesgos relacionados con el acceso no autorizado, sino que también mejora la experiencia del usuario al evitar pasos de autenticación innecesarios en situaciones de bajo riesgo (Shameli-Sendi et al., 2016).

Además, la IA puede integrarse con sistemas de detección de amenazas internas. Para identificar actividades sospechosas después de la autenticación inicial, estos sistemas, al igual que un sistema de detección de intrusiones (IDS), no solo verifican las credenciales de acceso, sino que también monitorean el comportamiento continuo del usuario o el dispositivo. Esto es crucial para proteger las IC de actores internos maliciosos, quienes, al tener acceso legítimo a los sistemas, podrían abusar de sus privilegios.

Biometría como método de autenticación

El uso de sistemas que incorporan la autenticación basada en *lo que soy* representa, sin duda, una alternativa con altos niveles de seguridad debido a la dificultad de falsificar o suplantar las características biométricas de cada individuo.

Sin embargo, esta dificultad tiende a disminuir con el avance tecnológico, lo que refuerza la necesidad de implementar mecanismos de MFA. Los métodos biométricos, como el reconocimiento de huellas dactilares, iris, rostro y voz, son más difíciles de replicar o sustraer, y ofrecen mayor seguridad que los métodos tradicionales basados únicamente en contraseñas.

En el contexto de las IC, la biometría representa una ventaja significativa al garantizar que solo el personal autorizado pueda acceder físicamente a instalaciones sensibles o virtualmente a sistemas críticos. Por ejemplo, en una planta de

energía nuclear o en una estación de control de agua, el uso de escáneres biométricos asegura que únicamente los operadores con permisos específicos puedan acceder a sistemas SCADA o a áreas restringidas.

Uno de los principales desafíos de la biometría es la protección de los datos biométricos. Si bien métodos como las huellas dactilares o el reconocimiento facial son más seguros que las contraseñas, la exposición de los datos biométricos es irreversible.

Para garantizar un cifrado robusto y una gestión segura, se requiere protección adicional. Además, las organizaciones que implementan biometría deben cumplir con estrictas regulaciones de privacidad.

Otro aspecto importante es la falta de inmutabilidad de algunos registros biométricos, lo cual debe tenerse en cuenta en sistemas críticos con tiempos de interacción más cortos. Por ejemplo, la voz, como factor de autenticación, puede variar debido a fenómenos como un resfriado, lo que debe considerarse al diseñar el sistema de autenticación.

Implementación de los sistemas de identidad federada

Los sistemas de identidad federada permiten que organizaciones o plataformas compartan un conjunto de credenciales de identidad. En lugar de autenticarse repetidamente en diferentes sistemas, los usuarios pueden disfrutar de un único inicio de sesión, reconocido por todos los miembros de la federación. Esto no solo mejora la eficiencia y la experiencia del usuario, sino que también fortalece la seguridad al reducir la cantidad de credenciales a gestionar.

En el ámbito de las IC, la identidad federada es especialmente útil cuando múltiples actores y entidades colaboran en la gestión de un mismo sistema, como ocurre en consorcios de energía o grandes sistemas de transporte.

La federación de identidades permite que estas organizaciones compartan la gestión de credenciales sin comprometer la seguridad. Un ejemplo de este tipo de tecnología es el Security Assertion Markup Language (SAML), que facilita la federación de identidades entre diferentes dominios (Lewis & Lewis, 2009).

La implementación de la identidad federada es esencial para la transición hacia un modelo de confianza cero (*zero trust*), en el que ningún usuario o dispositivo se considera confiable, ni siquiera dentro de la red interna. En un enfoque *zero trust,* cada solicitud de acceso se verifica y autentica individualmente, y las identidades federadas garantizan que estas verificaciones sean eficientes y seguras, especialmente en sistemas distribuidos y complejos.

Otros desarrollos relevantes

Además de las tecnologías previamente mencionadas, otras soluciones emergentes están destacándose en la gestión de identidades digitales para las IC. Los *tokens* de seguridad físicos y las claves criptográficas avanzadas proporcionan una mayor protección contra ataques de suplantación de identidad o interceptación de credenciales. Dispositivos como las llaves de seguridad basadas en el estándar Fast Identity Online 2 (FIDO2) permiten a los usuarios autenticarse mediante claves criptográficas que solo funcionan en el dispositivo autenticado.

Tendencias en la gestión de la identidad digital

Para abordar los desafíos de seguridad, privacidad y eficiencia en entornos cada vez más interconectados, la gestión de identidades digitales está evolucionando a pasos agigantados. Entre las tendencias más destacadas se encuentran las identidades autosoberanas y las identidades federadas y descentralizadas, que ofrecen enfoques innovadores, a fin de superar los problemas asociados con la gestión centralizada de las identidades digitales.

A continuación, se analizan estas tendencias, así como su impacto en la seguridad y la gestión de las IC.

Identidades autosoberanas

La identidad autosoberana es un modelo emergente que otorga a individuos y entidades el control total de sus identidades digitales, eliminando la necesidad de intermediarios centralizados, como empresas o gobiernos.

En este sistema, las credenciales son emitidas por entidades de confianza (como gobiernos, instituciones académicas o empresas), pero son los usuarios quienes las almacenan y gestionan a través de billeteras digitales seguras. La verificación de estas credenciales se realiza mediante tecnologías criptográficas, lo que permite a los usuarios compartir solo la información necesaria para cada interacción o transacción.

Este enfoque de identidad descentralizada aborda algunos de los problemas relacionados con los modelos tradicionales de identidad digital. En primer lugar, reduce la dependencia de proveedores de identidad centralizados, que, a menudo, son blanco de ataques cibernéticos y pueden representar un único punto de fallo.

Además, las identidades autosoberanas otorgan mayor control y privacidad a los usuarios, quienes deciden qué datos compartir y con quién, lo que limita la

exposición de su información personal y reduce el riesgo de violaciones de privacidad (Tobin & Reed, 2017).

El *blockchain* desempeña un papel clave en las identidades autosoberanas al proporcionar una capa de seguridad y verificación descentralizada. La naturaleza inmutable y distribuida de la cadena de bloques permite verificar las credenciales sin necesidad de un ente central.

En el contexto de las IC, la adopción de identidades autosoberanas podría mejorar significativamente la seguridad al eliminar los intermediarios que gestionan las credenciales de acceso. Por ejemplo, en una planta de energía, tanto los operadores como los dispositivos podrían gestionar sus credenciales de manera soberana, verificándolas mediante una red *blockchain.*

Este enfoque no solo incrementaría la seguridad, sino que también promovería la interoperabilidad entre diversos sistemas de identidad, permitiendo el uso de credenciales autosoberanas en distintas IC sin depender de un único proveedor (Dehalwar et al., 2022; Weigl et al., 2023).

Sin embargo, la adopción generalizada de identidades autosoberanas enfrenta desafíos considerables. La complejidad técnica inherente a la gestión de credenciales puede ser un obstáculo, especialmente en las IC, donde la eficiencia y la simplicidad son primordiales. Además, la ausencia de una regulación clara y estandarizada dificulta su implementación a gran escala, dado que distintas jurisdicciones y organizaciones podrían establecer normativas dispares para la gestión y verificación de identidades.

A pesar de estos desafíos, las identidades autosoberanas emergen como una tendencia clave con el potencial de transformar la gestión de las identidades digitales, especialmente en entornos donde la seguridad y la privacidad son primordiales.

Identidades federadas y descentralizadas

Otro enfoque emergente son las identidades federadas y descentralizadas. A diferencia de las autosoberanas, las federadas permiten que un conjunto de organizaciones o sistemas confíen en el mismo proveedor de identidad, lo que facilita el acceso a múltiples plataformas con una sola autenticación. Por lo general, este modelo se implementa en entornos empresariales y académicos mediante protocolos como OAuth 2.0 y SAML.

En una identidad federada, el usuario inicia sesión a través de un proveedor de identidad (como Google o Microsoft), que actúa como un intermediario confiable

para verificar su identidad en múltiples servicios. Este enfoque presenta claras ventajas, como la simplicidad y la reducción de la carga asociada a la gestión de múltiples credenciales.

En el contexto de las IC, la identidad federada resulta especialmente útil cuando varias organizaciones o sistemas colaboran en la gestión de un servicio o una red. Por ejemplo, en la gestión de una red eléctrica que involucra a múltiples empresas y agencias gubernamentales, la identidad federada puede simplificar el acceso de los operadores a sistemas compartidos, sin comprometer la seguridad.

El principal desafío de las identidades federadas radica en la confianza centralizada en los proveedores de identidad. Si el proveedor se ve comprometido, todas las plataformas que dependen de él pueden verse afectadas. Además, este modelo depende de la disponibilidad del proveedor, por lo que, en caso de una interrupción del servicio o un ataque dirigido, los usuarios podrían perder el acceso a los sistemas críticos.

El *blockchain* permite que las identidades descentralizadas otorguen a los usuarios un control total sobre sus credenciales. Este enfoque descentraliza la verificación, eliminando la dependencia de una autoridad central. La verificación de credenciales se realiza a través de una red distribuida. Esto mejora tanto la seguridad como la privacidad al mitigar el riesgo de un único punto de fallo y evitar el almacenamiento centralizado de la información personal.

En las IC, las identidades descentralizadas pueden mejorar la seguridad y reducir la exposición a ciberataques. Por ejemplo, en plantas de energía, los operadores de sistemas SCADA podrían autenticar su acceso a distintos subsistemas mediante identidades descentralizadas. Esto sería especialmente valioso en escenarios de resiliencia cibernética, ya que las identidades descentralizadas seguirían operando, incluso si uno o varios nodos de la red se vieran comprometidos.

No obstante, la implementación de identidades descentralizadas enfrenta importantes desafíos, como la complejidad técnica inherente a estos sistemas. Para su implementación y gestión efectiva, las organizaciones deben invertir en infraestructura y capacitación.

Además, la interoperabilidad entre los sistemas de identidad descentralizada sigue siendo un desafío, puesto que la compatibilidad no es una característica universal. La falta de estándares y normativas claras también representa un riesgo para su implementación en el contexto de las IC, donde la compatibilidad y la seguridad son primordiales.

Otras tendencias relevantes

Además de las identidades autosoberanas, federadas y descentralizadas, varias tendencias emergentes en la gestión de identidades digitales están ganando relevancia. Un ejemplo es la autenticación sin contraseñas, cuya popularidad ha aumentado, especialmente con el desarrollo de estándares como FIDO2. Este enfoque permite la autenticación mediante claves criptográficas y dispositivos de seguridad, eliminando la necesidad de contraseñas, que, a menudo, son un punto débil en los sistemas de autenticación.

Otra tendencia importante es el auge de los sistemas de autenticación adaptativa, que evalúan el riesgo y personalizan el proceso de autenticación basándose en patrones de comportamiento, ubicación geográfica y tipo de dispositivo, entre otros.

A esto se suma el uso avanzado de tecnologías como el aprendizaje automático y la IA. En conjunto, estos avances mejoran tanto la seguridad como la experiencia del usuario al proporcionar un acceso más fluido en escenarios de bajo riesgo y una protección reforzada en situaciones de alto riesgo (Bakar & Haron, 2014).

Autenticación sin contraseñas

La autenticación sin contraseñas es una tendencia en auge, impulsada por la imperiosa necesidad de robustecer la seguridad y mejorar la experiencia del usuario al eliminar las contraseñas, consideradas uno de los eslabones más débiles de la autenticación tradicional. Dada su susceptibilidad a ataques de fuerza bruta, *phishing* y reutilización, las contraseñas representan un riesgo significativo.

En cambio, la autenticación sin contraseñas utiliza claves criptográficas, dispositivos de seguridad físicos, biometría o MFA, como huellas dactilares o reconocimiento facial, para validar la identidad de los usuarios.

El estándar FIDO2 representa uno de los avances más significativos en este campo. Este protocolo utiliza un sistema de claves públicas y privadas, generadas directamente en el dispositivo del usuario. De este modo, se refuerza la seguridad y se elimina el riesgo de robo o interceptación de credenciales.

Ventajas:

- Seguridad reforzada: al eliminar las contraseñas, se reducen significativamente los riesgo de ataques de *phishing,* fuerza bruta y reutilización de credenciales.
- Mejor experiencia para el usuario: al prescindir de la memoria y eliminar la necesidad de gestionar múltiples contraseñas, se optimiza la accesibilidad y se simplifica el uso.

Desafíos:

- Implementación: la adopción generalizada de sistemas sin contraseñas puede representar un desafío para las organizaciones con infraestructuras heredadas que aún dependen de contraseñas tradicionales.
- Acceso en dispositivos compartidos o públicos: la autenticación sin contraseñas debe contemplar cómo garantizar un acceso seguro.

Gestión de las identidades en el internet de las cosas

El crecimiento exponencial del IoT está generando la necesidad de gestionar identidades digitales no solo para humanos, sino también para millones de dispositivos conectados. Cada dispositivo IoT requiere una identidad digital única para su autenticación y autorización en las redes a las que está vinculado. Esto plantea desafíos significativos en términos de escalabilidad, interoperabilidad y seguridad, ya que muchos dispositivos IoT presentan limitaciones en su capacidad de procesamiento y almacenamiento.

Los sistemas de gestión de identidades deben ser capaces de autenticar estos dispositivos de forma rápida y segura, garantizando que solo los autorizados puedan interactuar con los sistemas críticos. En este contexto, se están explorando soluciones como las identidades descentralizadas basadas en *blockchain,* que permiten autenticar dispositivos IoT sin depender de un proveedor centralizado, lo que reduce significativamente el riesgo de suplantación o manipulación de identidades (Roman et al., 2013).

Asimismo, la autenticación de *alcance cercano,* facilitada por el Edge Computing, se presenta como una alternativa para establecer la autenticación en distintos segmentos de red.

Ventajas:

- Escalabilidad: las soluciones avanzadas gestionan millones de dispositivos con distintos niveles de acceso y privilegios.
- Seguridad distribuida: las tecnologías descentralizadas, como el *blockchain,* proporcionan mayor seguridad y reducen el riesgo de compromisos centralizados.

Desafíos:

- Limitaciones de los dispositivos: muchos dispositivos IoT presentan limitaciones técnicas que dificultan la implementación de métodos avanzados de autenticación y cifrado.

- Estándares de interoperabilidad: la falta de estándares universales puede dificultar la implementación y la interoperabilidad entre dispositivos desarrollados por diferentes fabricantes.

Autenticación multifactor adaptativa

A diferencia de la MFA tradicional, que requiere dos o más factores de autenticación, la AMFA ajusta los métodos de autenticación basándose en el contexto y el riesgo evaluado en tiempo real. Este enfoque considera aspectos como la ubicación geográfica, el dispositivo utilizado, la hora del día o el historial de comportamiento del usuario.

Si el sistema detecta una actividad inusual, como un intento de inicio de sesión desde un país diferente o un dispositivo desconocido, puede solicitar autenticación adicional. En situaciones de bajo riesgo, como un inicio de sesión desde una ubicación habitual o un dispositivo confiable, el sistema puede simplificar la autenticación para mejorar la experiencia del usuario (Shameli-Sendi et al., 2016).

Ventajas:

- Mayor seguridad dinámica: la AMFA ajusta la autenticación según las amenazas detectadas en cada contexto, reforzando así la protección contra accesos no autorizados.
- Experiencia de usuario mejorada: simplificar la autenticación en situaciones de bajo riesgo reduce la fricción en las interacciones de los usuarios.

Desafíos:

- Complejidad en la implementación: la AMFA exige sistemas avanzados capaces de analizar múltiples factores en tiempo real y realizar ajustes rápido.
- Privacidad y recopilación de datos: para implementar la autenticación adaptativa, las organizaciones deben recopilar y analizar grandes volúmenes de datos, especialmente los relacionados con el comportamiento del usuario, lo que genera preocupaciones sobre su privacidad.

Conclusiones

La protección de las ICC demanda una estrategia integral que aborde aspectos tecnológicos y humanos, con la gestión de identidades digitales como pilar fundamental. Este enfoque mitiga las vulnerabilidades derivadas de la convergencia entre las TI y las TO, garantizado la seguridad, la confidencialidad y la integridad de los sistemas.

Además, la implementación de tecnologías emergentes, como el *blockchain,* la IA y la autenticación biométrica, refuerza la capacidad de respuesta ante amenazas cibernéticas. Sin embargo, su implementación plantea desafíos técnicos, normativos y de interoperabilidad, lo que destaca la necesidad de marcos regulatorios claros y estándares abiertos que faciliten su integración en entornos heterogéneos y críticos para el funcionamiento de la sociedad.

En lo que respecta a la gestión de la identidad digital para la protección de las IC, esta se ha convertido en un eje transversal en normativas como la NIS2, el NIST CSF V 2.0 y el CONPES 3995 debido a la proliferación de ataques basados en la suplantación de identidad o el robo de credenciales. Además, se observa que las normativas modernas tienden a integrar la protección física y digital, reconociendo la creciente dependencia tecnológica de las IC.

Finalmente, en un escenario en el que el ataque a una IC ya no es una posibilidad, sino una certeza temporal, es imperativo implementar estrategias de mitigación y respuesta. Esto requiere el desarrollo de sistemas resilientes, el uso de tecnologías avanzadas de monitoreo y control, y la adopción de una defensa integrada con la metodología *zero trust*.

Referencias

Alirio, M. H., Sierra, B., & Silva, J. M. (2016). *Importancia de definir la infraestructura crítica en Colombia.*

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68,* 81-97. https://doi.org/10.1016/j.cose.2017.04.005

Aydin, H., & Sertbaş, A. (2022). Cyber security in industrial control systems (ICS): A survey of Rowhammer vulnerability. *Applied Computer Science, 18*(2), 86-100. https://doi.org/10.35784/acs-2022-15

Bakar, K. A. A., & Haron, G. R. (2014). Adaptive authentication based on analysis of user behavior. *Proceedings of 2014 Science and Information Conference (SAI 2014),* 601-606. https://doi.org/10.1109/SAI.2014.6918248

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A review of Colonial Pipeline ransomware attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW),* 8-15. https://doi.org/10.1109/CCGridW59191.2023.00017

Centro Nacional de Inteligencia (CNI). (2008). *Directiva 2008/114/CE del Consejo.*

Check Point Software Technologies. (s.f.). *What is spear phishing?* https://tinyurl.com/2yn9f4et

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer, 44*(4), 91-93. https://doi.org/10.1109/MC.2011.115

Comando Conjunto Cibernético (CCOC). (2015). *Guía para la identificación de infraestructura crítica cibernética (ICC) de Colombia.* Comando General de las Fuerzas Militares. https://tinyurl.com/mvsd3xfb

Dehalwar, V., Kolhe, M. L., Deoli, S., & Jhariya, M. K. (2022). Blockchain-based trust management and authentication of devices in smart grid. *Cleaner Engineering and Technology, 8,* 100481. https://doi.org/10.1016/j.clet.2022.100481

Dragos, Inc. (2021). *Industrial cyber risk management.* https://tinyurl.com/mw7hsnz8

Elwell, J. S. (2014). The transmediated self: Life between the digital and the analog. *Convergence, 20*(2), 233-249. https://doi.org/10.1177/1354856513501423

Fang, J., Yan, C., & Yan, C. (2009). Centralized identity authentication research based on management application platform. *2009 First International Conference on Information Science and Engineering,* 2292-2295.

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications, 111*(7), 1-6. https://doi.org/10.5120/19547-1280

FIDO Alliance. (s.f.). *FIDO2: Moving the world beyond passwords.* https://fidoalliance.org/fido2/

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security -- A survey. *arXiv.* http://arxiv.org/abs/1701.04525

Kebande, V. R., & Awad, A. I. (2024). Industrial Internet of Things ecosystems security and digital forensics: Achievements, open challenges, and future directions. *ACM Computing Surveys, 56*(5). https://doi.org/10.1145/3635030

Lee, R. M., Assante, M. J., & Conway, T. (2016). *SANS ICS 2016 defense use case 4 1: Analysis of the recent reports of attacks on US infrastructure by Iranian actors.* https://www.secureworldexpo.com/tags/bowman-

Lewis, J. E., & Lewis, K. D. (2009). Web single sign-on authentication using SAML. *IJCSI International Journal of Computer Science Issues, 2.* https://doi.org/10.48550/arXiv.0909.2368

Ley 1273. (2009, 5 de enero). *Por medio de la cual se modifica el Código Penal…* Congreso de la República de Colombia. https://tinyurl.com/2bf5r745

Ley 1581. (2012, 17 de octubre). *Por la cual se dictan disposiciones generales para la protección de datos personales.* Congreso de la República de Colombia. https://tinyurl.com/yzqspuwd

Luque Juárez, J. M. (2024). La seguridad humana y su implementación en la operación de las Fuerzas Armadas: análisis documental. *Revista Científica General José María Córdova, 22*(45), 237-258. https://doi.org/10.21830/19006586.1237

Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). *Cyber security and critical infrastructures.* https://www.mdpi.com/topics

Moteff, J., & Parfomak, P. (2004). *CRS report for Congress: Critical infrastructure and key assets: Definition and identification.*

Muth, R., Galal, T., Heiss, J., & Tschorsch, F. (s.f.). *Towards smart contract-based verification of anonymous credentials.* https://github.com/hyperledger/indy-sdk

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity.* U.S. Department of Commerce.

O'Reilly, P., Rigopoulos, K., Feldman, L., & Witte, G. (2021). *2020 cybersecurity and privacy annual report.* https://doi.org/10.6028/NIST.SP.800-214

Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity, 4*(1). https://doi.org/10.1186/s42400-021-00071-z

Parlamento Europeo. (2016). *Reglamento general de protección de datos (GDPR) (Reglamento 2016/679).* https://gdpr-info.eu/

Qu, Y., Gao, L., Luan, T. H., Xiang, Y., Yu, S., Li, B., & Zheng, G. (2020). Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal, 7*(6), 5171-5183.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11-25. https://doi.org/10.1109/37.969131

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks, 57*(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018

Sameera, K. M., Nicolazzo, S., Arazzi, M., Nocera, A., R. R. K., P. V., & Conti, M. (2024). Privacy-preserving in blockchain-based federated learning systems. *Computer Communications.* https://doi.org/10.1016/j.comcom.2024.04.024

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers and Security, 57,* 14-30. https://doi.org/10.1016/j.cose.2015.11.001

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health, 9.* https://doi.org/10.1177/20552076231177144

Tobin, A., & Reed, D. (2017). *The inevitable rise of self-sovereign identity: A white paper from the Sovrin Foundation.*

Vesić, S., & Bjelajac, M. (2023). Cyber security of a critical infrastructure. *Pravo - Teorija i Praksa, 40*(2), 77-88. https://doi.org/10.5937/ptp2302077v

Wang, C., & Zhao, J. (2023). Network approaches in blockchain-based systems: Applications, challenges, and future directions. *Computer Communications, 212,* 141-150. https://doi.org/10.1016/j.comcom.2023.09.018

Weigl, L., Barbereau, T., & Fridgen, G. (2023). The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions. *Government Information Quarterly, 40*(4). https://doi.org/10.1016/j.giq.2023.101873

Zhang, J., Zhong, S., Wang, T., Chao, H. C., & Wang, J. (2020). Blockchain-based systems and applications: A survey. *Journal of Internet Technology, 21*(1), 1-14. https://doi.org/10.3966/160792642020012101001