Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DESAFÍOS Y TENDENCIAS EN LA IDENTIDAD DIGITAL PARA LA SEGURIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS.

MY CAROLINA VASQUEZ RUIZ
MY ANTONIO PEREZ FONTALVO
CC. VICTOR GONZALEZ BADRAN
MY MANUEL SUÁREZ RODRÍGUEZ

Artículo Electiva:

Habilidades y Prácticas en el Ciberespacio

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2024

DESAFÍOS Y TENDENCIAS EN LA IDENTIDAD DIGITAL PARA LA SEGURIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS.

CHALLENGES AND TRENDS IN DIGITAL IDENTITY FOR THE SECURITY OF CRITICAL INFRASTRUCTURES.

Resumen: La importancia de la identidad digital y la seguridad de las infraestructuras críticas en el contexto colombiano es innegable. La creciente digitalización de sectores como el financiero y el energético ha expuesto vulnerabilidades que demandan una respuesta integral por parte del gobierno y las entidades privadas. En este sentido, la iniciativa de desarrollar una Política Nacional de Seguridad Digital y una Guía para la Identificación de Infraestructura Crítica Cibernética refleja un enfoque más estructurado y proactivo en la protección de los activos digitales críticos del país. Sin embargo, los desafíos persisten, especialmente en el sector financiero, donde la colaboración internacional es esencial para salvaguardar la integridad de los sistemas. La tendencia hacia un enfoque holístico de la seguridad digital, que va más allá de la mera protección de activos, es evidente en la necesidad de desarrollar capacidades regionales en seguridad cibernética y proteger a los menores en Internet. La adopción de marcos de trabajo internacionales, como el propuesto por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, representa tanto un desafío como una oportunidad para fortalecer la postura de seguridad digital en Colombia. El cual, el panorama de la identidad digital y la seguridad de las infraestructuras críticas en Colombia se caracteriza por una creciente conciencia de los riesgos cibernéticos, una tendencia hacia la colaboración internacional y regional, y la adopción de enfoques más estructurados y holísticos para la gestión de la seguridad digital. No obstante, persisten desafíos significativos que requieren atención inmediata y estratégica, como la necesidad de inversión en tecnologías avanzadas, la formación de talento

especializado en ciberseguridad y la armonización de las políticas nacionales con las mejores prácticas internacionales.

1. **Palabras clave:** Ciberseguridad, Infraestructura crítica, Identidad digital, Política nacional, Colaboración internacional.

.

Abstract: The importance of digital identity and the security of critical infrastructures in the Colombian context is undeniable. The increasing digitization of sectors such as finance and energy has exposed vulnerabilities that demand a comprehensive response from the government and private entities. In this regard, the initiative to develop a National Digital Security Policy and a Guide for the Identification of Critical Cyber Infrastructure reflects a more structured and proactive approach to protecting the country's critical digital assets. However, challenges persist, especially in the financial sector, where international collaboration is essential to safeguard the integrity of systems. The trend towards a holistic approach to digital security, which goes beyond mere asset protection, is evident in the need to develop regional cybersecurity capabilities and protect minors on the Internet. The adoption of international frameworks, such as the one proposed by the National Institute of Standards and Technology (NIST) of the United States, represents both a challenge and an opportunity to strengthen Colombia's digital security posture. In conclusion, the landscape of digital identity and critical infrastructure security in Colombia is characterized by a growing awareness of cyber risks, a trend towards international and regional collaboration, and the adoption of more structured and holistic approaches to digital security management. Nevertheless, significant challenges persist that require immediate and strategic attention, such as the need for investment in advanced technologies, the training of specialized cybersecurity talent, and the harmonization of national policies with international best practices.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Keywords: Cybersecurity, Critical infrastructure, Digital identity, National policy, International collaboration.

INTRODUCCIÓN

La seguridad de las infraestructuras críticas en la actual era digital es un reto esencial para gobiernos y entidades globales. La creciente interconexión ha creado nuevas vulnerabilidades que precisan enfoques innovadores para resguardar los activos clave de un país. En este marco, la identidad digital se presenta como un componente crucial en la estrategia de ciberseguridad, ofreciendo tanto oportunidades como desafíos.

Las crecientes amenazas cibernéticas subrayan la urgencia de desarrollar robustos mecanismos de autenticación y control de acceso. Sectores como energía, transporte, telecomunicaciones y finanzas son especialmente vulnerables a ataques malintencionados. La complejidad y relevancia de estos sistemas para la sociedad moderna requieren medidas de seguridad avanzadas que superen las soluciones tradicionales.

En América Latina y el Caribe, experiencias como las descritas en el informe "Tendencias de Seguridad Cibernética en América Latina y el Caribe" de 2014 muestran un aumento significativo en la frecuencia y sofisticación de los ciberataques. Consecuentemente, gobiernos y organizaciones han revisado sus estrategias, destacando la implementación de sistemas robustos de identidad digital como respuestas esenciales.

El documento CONPES 3854 de Colombia resalta la importancia de un enfoque digital integrador, enfocado en gestionar riesgos y en el rol central de la identidad digital tanto en la autenticación como en la gestión de accesos y la trazabilidad de acciones en sistemas críticos. La meta es establecer un entorno digital seguro donde la identidad digital proteja activos y privacidad ciudadana.

Uno de los mayores desafíos es equilibrar seguridad y usabilidad. Los sistemas necesitan ser lo suficientemente robustos para resistir sofisticados ataques y, al mismo tiempo, ser accesibles para el personal autorizado, evitando que se

conviertan en obstáculos operativos. El uso de tecnologías biométricas refuerza la seguridad al asociar la identidad digital con características individuales únicos. Sin embargo, estas tecnologías exigen abordar delicadamente cuestiones éticas y de privacidad, especialmente en infraestructuras críticas.

La interoperatividad digital entre distintos sectores y países es otro punto crucial. La creciente interconexión genera la necesidad de estándares comunes que optimicen la eficiencia y la respuesta a incidentes multi-sectoriales y transnacionales. El Marco para la Mejora de la Seguridad Cibernética en Infraestructuras Críticas del NIST enfoca en un método basado en riesgos, optimizando la adaptación continua según la evolución de nuevas amenazas y tecnologías. Donde, la gestión del ciclo de vida de las identidades digitales en infraestructuras críticas demanda atención meticulosa desde la credencial inicial hasta la revocación de accesos. Factoras como rotación de personal, valer modificar la responsabilidad y acceso de emergencia, exige sistemas tanto flexibles como seguros.

DESARROLLO

La seguridad cibernética en Colombia enfrenta retos significativos en la protección de la identidad digital y de infraestructuras críticas. La política nacional del documento CONPES 3701 ha sido crucial para guiar las acciones de ciberseguridad y ciberdefensa, estableciendo directrices y áreas prioritarias para la acción gubernamental.

El Centro Cibernético Policial (CCP), bajo la Dirección de Investigación Criminal e INTERPOL (DIJIN), juega un papel central en la lucha contra los delitos cibernéticos. Capacitado por organismos internacionales como el Departamento de Estado de los Estados Unidos y el FBI, el CCP ha fortalecido sus capacidades en análisis forense digital y respuesta a incidentes.

La infraestructura colombiana, especialmente el sector bancario, enfrenta un aumento en los ataques cibernéticos debido a la expansión de las TIC. Los incidentes de fraude electrónico, empleando técnicas como keyloggers y spyware, subrayan la necesidad de mejorar las defensas cibernéticas. Se ha registrado un incremento en ataques de ransomware, como Cryptolocker, que afectan a pequeñas y medianas empresas, comprometiendo datos críticos y generando costos significativos.

La cooperación internacional, bajo el auspicio de INTERPOL, ha sido esencial en la lucha contra el cibercrimen. A nivel nacional, la Ley 1273 de 2009 ofrece un marco jurídico sólido, aunque la falta de cultura de seguridad cibernética y la actualización constante de capacidades técnicas y legales siguen siendo desafíos.

El incremento en los arrestos por delitos cibernéticos, con 422 en 2013 en comparación con 323 en 2012 y 252 en 2011, refleja tanto el aumento de actividad delictiva como la mejora en las capacidades de respuesta.

Tendencias en la Identidad Digital y la Protección de Infraestructuras Críticas en Colombia

En la actualidad, se ha evidenciado un marcado incremento en el uso de técnicas de phishing, malware y hackeo de sitios web gubernamentales. Esta situación constituye una seria amenaza para la seguridad de las infraestructuras críticas y debilita la confianza en los sistemas digitales.

El Documento CONPES 3854 de 2016, denominado "Política Nacional de Seguridad Digital", aborda de manera exhaustiva los retos y tendencias en identidad digital para asegurar la protección de las infraestructuras esenciales en Colombia. Dicho documento, elaborado con el concurso de diversas entidades gubernamentales, subraya la creciente relevancia del ámbito digital en la vida económica y social del país, al mismo tiempo que señala los riesgos y peligros inherentes a este entorno.

La Política Nacional de Seguridad Digital se fundamenta en cuatro principios claves y abarca cinco dimensiones estratégicas. Entre dichos principios destacan la participación activa de todas las partes implicadas y la distribución responsabilidad colectiva. Las dimensiones estratégicas incluyen desde la instauración de un marco institucional preciso hasta el fortalecimiento de la defensa y seguridad nacional en el entorno digital, además de la creación de mecanismos continuos de cooperación y ayuda en temas de seguridad digital, tanto a nivel nacional como global.

Cabe señalar que, mientras las políticas anteriores se orientaban principalmente a contrarrestar las amenazas cibernéticas desde una defensa y combate contra el cibercrimen, la nueva política introduce la gestión de riesgos como un elemento esencial. Esto responde al reconocimiento de que el creciente uso de las Tecnologías de la Información y Comunicación (TIC) ha propiciado el surgimiento de formas nuevas y más complejas que pueden interrumpir el desarrollo normal de las actividades económicas y sociales en el ámbito digital.

Para llevar a efecto esta política, se ha diseñado un plan de acción a ejecutarse entre 2016 y 2019, con una inversión total de 85.070 millones de pesos. Entre las principales entidades responsables de la ejecución se encuentran el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación. Se apuesta a que la implementación efectiva de esta política repercutirá positivamente en la economía colombiana, anticipando la creación de aproximadamente 307.000 empleos y un incremento del 0,1% en la tasa anual promedio de variación del PIB para el año 2020.

Asimismo, el documento subraya la necesidad de reforzar las capacidades en ciberseguridad y ciberdefensa, mediante la creación de nuevas estructuras y la optimización de las existentes. Esto incluye la formación y capacitación de personal especializado, junto con la ejecución de campañas de concientización y sensibilización dirigidas tanto a la ciudadanía como a entidades públicas y privadas.

La importancia de la cooperación internacional y el marco normativo en seguridad digital

La seguridad digital requiere de cooperación internacional para enfrentar los desafíos del entorno digital actual. Adherirse a convenios como el Convenio de Budapest, que guía la prevención y sanción de delitos informáticos, es fundamental.

Participar en organismos y redes de intercambio de información fortalece las capacidades de seguridad digital mediante la compartición de buenas prácticas y alertas tempranas. Establecer canales de comunicación efectivos entre el gobierno, el sector privado y la academia es clave para desarrollar estrategias integrales de protección de información e infraestructura crítica. Además, actualizar el marco normativo para abordar delitos cibernéticos es crucial. Esto permite una actuación eficaz de los organismos de seguridad del Estado.

Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) en su versión 1.1 se presenta como una herramienta fundamental para la gestión de riesgos en seguridad cibernética dentro de infraestructuras críticas. Esta estructura detallada y comprensiva consta de tres partes principales: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco, cada uno desempeñando un rol crucial para crear entornos seguros y resilientes frente a amenazas cibernéticas.

El Núcleo del Marco categoriza las actividades de ciberseguridad en cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar. Estas funciones proporcionan una visión estratégica integral del ciclo de vida de la gestión de riesgos en seguridad cibernética. Dentro de cada función se segmentan categorías y subcategorías que especifican los resultados esperados para mejorar la postura de seguridad cibernética.

Los Niveles de Implementación del Marco ofrecen una perspectiva sobre cómo una organización percibe el riesgo en ciberseguridad y los procesos establecidos para su gestión, posibilitando a las organizaciones priorizar sus esfuerzos y recursos según sus necesidades y tolerancia al riesgo específicos.

En otra faceta, los Perfiles del Marco representan los resultados que una organización ha seleccionado de las categorías y subcategorías del Núcleo del Marco, alineándolos con sus requisitos empresariales, tolerancias al riesgo y recursos necesitados. Estos perfiles permiten elaborar una hoja de ruta para reducir el riesgo cibernético y alcanzar objetivos de gestión de riesgo de manera efectiva y eficiente.

El Marco integra una metodología para la autoevaluación del riesgo de ciberseguridad, ofrece guía para que las organizaciones comprendan y evalúen su riesgo en seguridad cibernética, y utilizan mediciones para perfeccionar la toma de decisiones sobre las prioridades de inversión.

Asimismo, el Marco aborda la gestión del riesgo de cadena de suministro cibernética (SCRM), destacando la imperiosa necesidad de identificar, evaluar y mitigar los riesgos que puedan surgir de terceros. La SCRM en ciberseguridad es esencial para asegurar que los productos y servicios utilizados por una organización no solo cumplan con requisitos de seguridad cibernética, sino también para evitar la introducción de vulnerabilidades adicionales.

La relevancia de la identidad digital para los investigadores en el ámbito académico contemporáneo

En el ecosistema académico actual, la identidad digital de los investigadores ha adquirido una importancia trascendental. Gestionarla adecuadamente no solo mejora la visibilidad y reputación del investigador, sino que también afecta la percepción y prestigio de las instituciones a las que pertenecen. Por ello, la creación y el mantenimiento de perfiles digitales en diversas plataformas se han convertido en tareas fundamentales que requieren un análisis meticuloso y una estrategia bien definida.

Un ejemplo clave es el perfil en ORCID, esencial para la normalización y desambiguación de los investigadores. Este identificador digital persistente, reconocido globalmente, proporciona una identificación clara y sin ambigüedades de los autores, y facilita la interoperabilidad entre distintos sistemas de información académica. ORCID, actuando como un nodo central, enlaza otros perfiles y bases de datos, lo que garantiza la coherencia y actualidad de la información académica del investigador.

De igual importancia son ResearcherID y Scopus Author ID, que aunque son sistemas propietarios, ofrecen valiosos servicios para medir el impacto de la producción científica. Estos identificadores permiten a los investigadores obtener indicadores esenciales como el índice H y el número de citas, los cuales son cruciales en cualquier evaluación académica. La integración de estos perfiles con ORCID permite la transferencia fluida de información y asegura la congruencia de los datos entre las plataformas.

Por su parte, Google Scholar se ha consolidado como una de las bases de datos más extensas y accesibles para publicaciones científicas. Su capacidad de indexar múltiples fuentes, incluida la literatura gris, elimina barreras para disciplinas específicas y autores que publican en otros idiomas que no sean inglés. Sin embargo, la actualización automática de perfiles en Google Scholar puede

introducir errores, lo que requiere una supervisión constante de los investigadores para garantizar que sus perfiles sean precisos y actualizados.

Otras plataformas significativas en este ecosistema digital académico incluyen ResearchGate y Publons. ResearchGate, como red social para investigadores, facilita la visibilidad y el intercambio de contenido científico, mientras que Publons resalta el trabajo de los revisores, un aspecto crucial pero frecuentemente subestimado en la comunidad científica. Ambos sistemas contribuyen significativamente a la construcción de una identidad digital robusta y multifacética.

En definitiva, gestionar la identidad digital de los investigadores no es una tarea sencilla; requiere planificación estratégica y un esfuerzo sostenible para mantener la coherencia y actualidad de los perfiles. Cada plataforma presenta ventajas específicas y exige un compromiso ético para garantizar que la información publicada sea veraz. En este contexto, la selección de las plataformas donde se desea tener presencia debe ser una decisión informada y deliberada.

El entorno digital contemporáneo exige una presencia activa y bien gestionada en múltiples plataformas para maximizar la visibilidad y el impacto de la producción científica. La identidad digital de un investigador, además de reflejar su reputación y relevancia en la comunidad académica, influye en la percepción de las instituciones a las que pertenece. Por lo tanto, invertir en una identidad digital sólida es esencial para cualquier carrera académica.

La importancia de la identidad digital y la seguridad de las infraestructuras críticas en el entorno cibernético de América Latina y Colombia

La relevancia creciente de la identidad digital y su relación con la seguridad de las infraestructuras críticas ha producido un impacto notable en el panorama

cibernético de América Latina, particularmente en Colombia. La identidad digital engloba un conjunto de información y credenciales electrónicas que permiten identificar a personas o entidades en el ciberespacio, facilitando así transacciones y accesos a servicios digitales. Sin embargo, esta característica también convierte a la identidad digital en un objetivo atractivo para ciberdelincuentes que buscan explotar vulnerabilidades en infraestructuras críticas, especialmente en el sector financiero.

Uno de los mayores retos es la gestión y protección de las identidades digitales. En un entorno donde la mayoría de las transacciones y operaciones bancarias se realizan por vía digital, es fundamental asegurar que las identidades de los usuarios no sean comprometidas. Por lo tanto, bancos e instituciones financieras deben implementar medidas robustas de autenticación y verificación de identidad para prevenir accesos no autorizados y fraudes. Esto incluye el uso de tecnologías avanzadas como la autenticación multifactor (MFA), el reconocimiento biométrico y la inteligencia artificial para detectar patrones de comportamiento anómalos.

En América Latina, y específicamente en Colombia, el sector financiero ha liderado la adopción de tecnologías digitales, ofreciendo múltiples beneficios y riesgos. La digitalización ha potenciado la inclusión financiera y facilitado el acceso a servicios bancarios desde dispositivos móviles, pero también ha ampliado la superficie de ataque para los ciberdelincuentes. Los ataques cibernéticos, como el phishing, el malware y el ransomware, han evolucionado en sofisticación, afectando tanto a los bancos como a los usuarios finales.

La cooperación internacional es otro factor esencial en la gestión del riesgo cibernético. Como las amenazas cibernéticas no respetan fronteras, la colaboración entre países para compartir información sobre amenazas, mejores prácticas y estrategias es vital. Organizaciones como la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) han

sido fundamentales en el fortalecimiento de capacidades de ciberseguridad en la región, promoviendo la creación de marcos normativos y políticas nacionales de ciberseguridad.

La regulación y supervisión también juegan un papel crucial en la protección de infraestructuras críticas. Las entidades regulatorias deben establecer y hacer cumplir normas de seguridad cibernética que obliguen a instituciones financieras a implementar adecuadas medidas de protección para identidades digitales y datos sensibles. En Colombia, la Superintendencia Financiera ha emitido directrices explícitas sobre la gestión de riesgo cibernético, instando a las entidades a incorporar políticas y procedimientos robustos.

CONCLUSIONES

La ciberseguridad en Colombia afronta retos importantes en la protección de la identidad digital y las infraestructuras críticas. La política nacional, orientada por documentos clave como CONPES 3701 y CONPES 3854, ha establecido directrices esenciales y áreas prioritarias en ciberseguridad y ciberdefensa. Organismos como el Centro Cibernético Policial (CCP) y la Ley 1273 de 2009 han potenciado las capacidades nacionales para combatir el cibercrimen, aunque aún existen desafíos relacionados con la cultura de seguridad y la actualización de capacidades técnicas.

El sector bancario colombiano ha visto un incremento en los ataques cibernéticos, lo que resalta la necesidad de fortalecer las defensas contra fraudes electrónicos y ransomware. La cooperación internacional, especialmente bajo la coordinación de INTERPOL, y la adhesión a convenios como el de Budapest son fundamentales para enfrentar estos desafíos de manera efectiva.

El Marco de Ciberseguridad del NIST ofrece una estructura integral para la gestión de riesgos en infraestructuras críticas, enfatizando la importancia de identificar, proteger, detectar, responder y recuperarse frente a amenazas cibernéticas. Además, la gestión del riesgo en la cadena de suministro cibernética es crucial para prevenir vulnerabilidades adicionales.

En el ámbito académico, la gestión de la identidad digital de los investigadores es vital para su visibilidad y reputación. Plataformas como ORCID, ResearcherID y Scopus Author ID desempeñan un papel fundamental en la normalización y la medición del impacto de la producción científica. La adecuada gestión de estos perfiles es esencial para mantener la coherencia y actualización de la información académica.

Por lo tanto, la protección de la identidad digital y las infraestructuras críticas en Colombia requiere una combinación de políticas nacionales efectivas, cooperación internacional, marcos normativos actualizados y una gestión estratégica de la identidad digital en el ámbito académico. La implementación de medidas de autenticación robustas y la colaboración entre sectores son indispensables para mitigar los riesgos cibernéticos y garantizar un entorno digital seguro y resiliente.

REFERENCIAS

https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf?locale

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf?locale

https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Cyber%20Security%20and%20Critical%20Infrastructure%20in%20North%20America.pdf

Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors*, *22*(14), 5105.