Editorial

Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital

Cybersecurity and cyberdefense. Challenges and perspectives in a digital world

Jeimy J. Cano M.[1], Alvaro Rocha[2]

jcano@uniandes.edu.co, amrocha@dei.uc.pt

[1] Facultad de Derecho, Universidad de los Andes, Bogotá, Cra 1E No. 18A-10, Bogotá, Colombia.

[2] Universidade de Coimbra, Departamento de Engenharia Informática, Pólo II - Pinhal de Marrocos, 3030-290 Coimbra, Portugal.

DOI: 10.17013/risti.32.0

1. Introducción

La acelerada evolución de la convergencia tecnológica, el aumento de la densidad digital y la asimetría de la información en una sociedad cada vez más digital y tecnológicamente modificada, establece un escenario de análisis más elaborado y complejo, que exige de parte de los analistas de negocio, de seguridad de la información y de ciberseguridad, una vista mucho más holística y el entendimiento de relaciones emergentes antes ignoradas por los saberes disciplinares y segmentados.

En este sentido, se establecen nuevos retos en el contexto de la ciberseguridad y ciberdefensa, donde ya no es suficiente conocer y entender las amenazas conocidas del entorno, sino configurar propuestas actualizadas o novedosas que permitan, no solo proteger y asegurar los activos de información, sino defender y anticipar escenarios desconocidos o inciertos, que habiliten a las organizaciones y a los países para identificar y gestionar riesgos latentes y emergentes con una vista más sistémica.

En este marco, la trigésima segunda edición de la RISTI (Revista Ibérica de Sistemas y Tecnologías de la Información) se centra en las reflexiones, propuestas y avances en los temas de seguridad de la información, ciberseguridad y ciberdefensa, que busca conectar las realidades digitales de las organizaciones y las naciones, con las disrupciones, amenazas y riesgos derivados de un escenario cada vez más volátil, incierto, complejo y ambiguo.

El conjunto de ocho artículos publicados en este número de RISTI fue el resultado de un exigente proceso de evaluación por parte de los miembros del comité científico de los treinta y cinco trabajos presentados por los autores, procedentes de una colaboración entre España y México, tres de Argentina, un trabajo conjunto entre Colombia y España, Ecuador, Cuba y Chile, lo que corresponde a una tasa de aceptación del 22%.

2. Estructura

El primer artículo, con el título "Validación del contenido de un guion de entrevista sobre la competencia digital docente en Educación Superior", presenta un estudio para obtener evidencias de validez del contenido de un guión de entrevista en profundidad, en el marco de una investigación sobre el desarrollo de la competencia digital de profesores universitarios. Como resultado se obtuvo una versión acotada del guión propuesto y se identificaron aspectos en debate sobre la conceptualización de esta competencia docente en la Educación Superior.

El segundo artículo, con el título "Herramienta para el Análisis Forense de Correos Electrónicos", introduce una herramienta para el análisis forense de correos electrónicos a partir de la cabecera de los mismos y la utiliza para instanciar una ontología definida para responder a los puntos de pericia solicitados sobre éstos correos. El documento detalla cada componente de la herramienta y se ejemplifica su uso mediante un caso de estudio sobre análisis forense de un correo electrónico.

El tercer artículo, con el título "Auditorías en Ciberseguridad. Un modelo de aplicación general para empresas y naciones", detalla los resultados de un estudio de implementación y validación del Modelo de Auditoría de Ciberseguridad (CSAM), en un ejercicio de casos múltiples en una universidad canadiense. El artículo concluye ilustrando los resultados de la aplicación del modelo en sus diferentes vistas, con información relevante para la toma de decisiones futuras, que permita ajustar las limitaciones de ciberseguridad identificadas, mejorar sus dominios y controles, y de esta manera, implementar y probar de manera eficiente este modelo en cualquier organización o país.

El cuarto artículo, con el título "Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada", aborda del reto de repensar la estructura jerárquica y centralizada de una infraestructura de llave pública (en inglés Public Key Infrastructure) hacia una propuesta descentralizada y distribuida basada en tecnología de cadena de bloques (en inglés blockchain) que permita mayor transparencia en la emisión de certificados, disminución del riesgo y aumento de la confiabilidad. Como resultado, la arquitectura propuesta proporciona a los usuarios mayor eficiencia en el proceso de gestión de certificados, con ahorro de tiempo y simplificación de trámites y configuraciones vigentes en el modelo tradicional.

El quinto artículo, con el título "Balanceo De Carga Basado En Criterios Combinados, Para Servidores, Utilizando Tecnologías De Redes Definidas Por Software", ilustra un algoritmo de balanceo de carga basado en un sistema de criterios combinados, que utiliza tecnologías de redes definidas por software para obtener en tiempo de ejecución, parámetros desde distintos puntos de la red y seleccionar el servidor con las mejores condiciones para responder. Los resultados del experimento utilizando la herramienta

Mininet, demuestran que el balanceador de carga basado en criterios combinados, reduce, hasta en un 50%, el tiempo de respuesta del servidor en comparación con el método tradicional Round Robin.

El sexto artículo, con el título "Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM", desarrolla la implementación de una estrategia de defensa en profundidad para la protección del sistema de control industrial de la planta de producción de Cloro-Sosa de la empresa ELQUIM. Para ello, se sigue la aplicación de la guía de seguridad para sistemas de control industrial del NIST, articulando sus resultados con software hecho en el país y software para asegurar la soberanía tecnológica de la solución.

El séptimo artículo, con el título "KE-SER: Un sistema basado en el conocimiento y la experiencia para dar soporte a arquitectos de software en aspectos de seguridad", propone un sistema experto, denominado KE-SER (por sus siglas en inglés *Knowledge & Experience – SEcurity Recommendations*) para brindar apoyo, desde el punto de vista de la seguridad, a los arquitectos de software para que puedan tomar decisiones durante el diseño arquitectónico de forma consciente e informada. En este trabajo, se describe un sistema capaz de realizar recomendaciones para satisfacer los requerimientos de seguridad de los sistemas a construir. Las recomendaciones pueden estar basadas en el conocimiento capturado de expertos en seguridad o en experiencias pasadas de arquitectos que diseñaron arquitecturas de sistemas con requerimientos similares.

Finalmente, el último artículo, con el título "Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información", detalla una nueva versión del enfoque de programación de conjunto de respuestas (en inglés ASP - *Answer Set Programming*) para tomar una decisión sobre inversiones en seguridad de la información en un escenario con restricciones presupuestarias. La propuesta se compara con el desarrollo del problema utilizando programación lineal (LP), ilustrando la fase de modelado y el rendimiento computacional de ambas soluciones. El modelo ASP presenta tiempos de resolución del tipo exponencial a medida que aumenta el número de controles sobre los que debe decidirse, lo que implica que si se quieren respuestas rápidas, se debe usar una baja cantidad de controles.

3. Agradecimientos

Esta introducción termina expresando nuestra gratitud a todos los autores y revisores involucrados en esta edición, esperando que este número de RISTI sea una lectura interesante para todos aquellos que se movilizan en torno a los retos de la ciberseguridad y la ciberdefensa. Un agradecimiento especial a AISTI, propietaria y promotora de RISTI, así como a las Bases de Datos de Revistas Académicas como CiteFactor, Compendex, Dialnet, DOAJ, DOI, EBSCO, GALE, IndexCopernicus, Index of Information Systems Journals, ISI Web of Knowledge, Latindex, ProQuest, QUALIS, SciELO, SCImago y Scopus, entidades que han contribuido a convertir a RISTI en un referente en este competitivo mercado de revistas científicas.