EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 1, número 1, enero-junio 2022
Bogotá, D.C, Colombia
ISSN: 2955-0270
Página web: https://esdegrevistas.edu.co/index.php/rcit

Entrevista a Marco Emilio Sánchez Acevedo. La ciberseguridad en Colombia

Interview with Marco Emilio Sánchez Acevedo. Cybersecurity in Colombia

Mónica Lissette Flórez Cáceres

CITACIÓN APA:

Flórez Cáceres, M. L. (2022). Entrevista a Marco Emilio Sánchez Acevedo. La ciberseguridad en Colombia. *Ciberespacio, Tecnología e Innovación, 1*(1), 101-104. https://doi.org/10.25062/2955-0270.4782

Publicado en línea: **Junio 30 de 2022**

Enviar un artículo a la Revista

Revista **Ciberespacio, Tecnología e Innovación**
Volumen 1, número 1, enero-junio 2022 (pp. 101-104)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Entrevista a Marco Emilio Sánchez Acevedo. La ciberseguridad en Colombia

Interview with Marco Emilio Sánchez Acevedo. Cybersecurity in Colombia

DOI: https://doi.org/10.25062/2955-0270.4782

Mónica Lissette Flórez Cáceres
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Biografía

Doctor en Tecnologías y Servicios de la Sociedad de la Información – Derecho y TIC de la Universitat de València, España. Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Especialista en Derecho Administrativo y Constitucional de la Universidad Católica de Colombia. Abogado de la Universidad Central, Colombia. Docente de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Entrevista
Recibido: 2 de febrero de 2022 • **Aceptado:** 20 de mayo de 2022
Contacto: Mónica Lissette Flórez Cáceres monica.florez@esdeg.edu.co

Entrevista a Marco Emilio Sánchez Acevedo. La ciberseguridad en Colombia

¿Cuál es el rumbo de la ciberseguridad para en el país?

Colombia hace parte de un entorno tanto regional como mundial en el marco de las garantías para el derecho a la seguridad digital de sus ciudadanos, y bajo esa órbita, el país ha trazado una hoja de ruta desde hace más de 10 años en torno a la seguridad digital, y al fortalecimiento de las capacidades de ciberdefensa. Mencionada hoja de ruta inició con el establecimiento de una institucionalidad, que pasa precisamente por el Centro de Respuestas a Emergencias Cibernéticas de Colombia, el Centro Cibernético de la Policía, el Comando Conjunto de Operaciones Cibernéticas, los Centros de Respuestas a Emergencias Cibernéticas de cada uno de los sectores que se identifiquen como críticos para el país, y por supuesto, de la Fiscalía General de la Nación a través de las unidades de investigación de delitos informáticos.

Luego de ello, se avanzó en la construcción de un plan para gestionar los riesgos de seguridad digital, siendo un proceso que se ha venido dando durante varios años consolidando a su paso una institucionalidad desde la gobernanza de la seguridad digital, y ahí es cuando en el año 2022 aparece lo que significa el papel del Director Nacional de Seguridad Digital y el papel del Comité Nacional de Seguridad Digital del que hacen parte más de 20 entidades nacionales con distintos actores, con lo que se trató inicialmente, de reiterada institucionalidad es el fortalecimiento de las capacidades de gestión de riesgos y gestión de incidentes que sin duda ha venido en constante maduración.

Finalmente, el futuro no puede ser otro que fortalecer cada una de esas capacidades que se han desarrollado en el proceso desde hace bastantes años. No puede ser otro que el de enfrentar los desafíos que genera el uso de tecnologías de manera masiva a partir del uso de tecnologías emergentes, y así mismo, a partir de la construcción de ciudades y territorios inteligentes. De igual modo, el establecimiento de todas las actividades sociales por medios electrónicos: el comercio electrónico, la educación digital, la justicia digital, la salud digital, entre otros. Es decir, fortalecimiento de las capacidades para hacer frente a los desafíos que genera usar tecnologías en todos los sectores sociales y económicos del país.

Desde su experiencia profesional y académica, ¿cuáles considera que son los retos en torno a la regulación normativa para la ciberseguridad a nivel nacional?

Son bastantes. En esencia, las normas son de distinta naturaleza: normas internacionales, nacionales, y dentro de estas, leyes de la República, decretos reglamentarios

y actos administrativos que incorporen lineamientos y estándares, eso quiere decir que los retos son todos en todos estos frentes.

Primero, en lo que corresponde al frente internacional, la aplicación y materialización del Convenio de Budapest sigue siendo un instrumento normativo supranacional que permite combatir los delitos informáticos de manera articulada y colaborativa con los distintos actores de diversos Estados. Segundo, en los retos nacionales se ubica la necesidad de una ley de seguridad digital, particularmente para involucrar al sector privado en obligaciones de seguridad y defensa del Estado, dado que, muchísimas infraestructuras críticas y servicios esenciales son hoy en día administrados y gestionados por este sector, y ellos, sin duda, deben involucrarse desde la protección de las infraestructuras y servicios esenciales que están en sus manos.

De igual manera, en la legislación nacional es necesaria la identificación de infraestructuras críticas, entendiendo que no se puede proteger lo que no se conoce, y en consecuencia, se deben delimitar cuáles son los sectores y subsectores que están conectados a las tecnologías de la información y las comunicaciones, pues se convierten en sectores y servicios críticos que hay que proteger desde la seguridad y la defensa para el mantenimiento del orden constitucional, legal y lógicamente de la garantía de los derechos ciudadanos.

Por otra parte, en los instrumentos normativos de menor nivel existentes varios retos muy importantes porque la seguridad y defensa nacional pasa por diversos estándares y estos tienen que estar condicionados tanto para el sector público como para el sector privado, a partir de regulaciones homogéneas en torno a la gestión de los riesgos que genera el uso de tecnologías, pero al mismo tiempo la gestión de los incidentes. Partiendo de esto, mencionados lineamientos permitirán entender ¿qué hacer de manera colaborativa para enfrentar un ataque cibernético de gran escala? ¿Cómo incorporan los actores públicos y privados los estándares técnicos que permiten hacer frente a las emergencias cibernéticas?

Con todo lo anterior, y ante la inclusión de más sectores y actores económicos o del sector empresarial que se están conectando a tecnologías de manera masiva, se genera la necesidad de establecer unos estándares o lineamientos técnicos muy importantes para garantizar la seguridad digital.

Con ocasión a la actual situación y los retos evidenciados, ¿cuál considera usted que es la herramienta oportuna para mitigar a largo plazo las visicitudes que diaramente proliferan en torno a la ciberseguridad?

Desde mi criterio, la formación se convierte en un elemento fundamental para la construcción de capacidades a todo nivel. Esto quiere decir que el uso de la tecnología no responde a una moda, sino que aborda todo un modelo de desarrollo

planteado para la sociedad del siglo XXI, obligándo entonces a adquirir fortalezas y capacidades desde la formación de la ciudadanía y del personal militar.

Específicamente, programas como la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto"es una de las maestrías líderes, quizás la primera en Latinoamérica que abandera ese proceso de formación para personal del nivel estratégico, del nivel táctico y del nivel operativo, mismo que va a ser requerido por actores públicos y privados para el cumplimiento de las obligaciones derivadas de la seguridad y defensa nacional, así como de la protección de los derechos de los ciudadanos en el ciberespacio. En este sentido, contar con programas actualizados funge como respuesta a las necesidades de adquirir capacidades con los expertos referentes, posibilitando una formación especializada de más alto nivel.

Autora de la entrevista

Mónica Lissette Flórez Cáceres. Magister en Acción Política y fortalecimiento institucional de la Universidad Francisco de Vitoria, España. Especialista en Comercio Internacional y Profesional en Relaciones Internacionales y Estudios Políticos de la Universidad Militar Nueva Granada, Colombia. Docente de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

ORCID: https://orcid.org/0000-0003-4777-2481
Contacto: monica.florez@esdeg.edu.co