

Claves en el marco de la seguridad híbrida

DOI: 10.29236/sistemas.n167a3

Un pensamiento creativo, inquieto, basado sobre todo en la innovación y la prospectiva es fundamental en el marco de la seguridad híbrida, indica el Cr.(RA) Fredy Bautista García.

Sara Gallardo M.

La amplia experiencia de Fredy Bautista García, actual director del Departamento de Protección y Seguridad del Banco de la República, lo ha llevado por diferentes espacios en los que ha dejado una huella muy importante.

Es Coronel de la Reserva Activa de la Policía Nacional; ha sido presi-

dente en dos oportunidades del Grupo de Trabajo de Cibercrimen en INTERPOL para las Américas; primer Jefe del Centro Cibernético de la Policía Nacional y gestor de Ciberseguridad en el sector público en Colombia. Así mismo, ha participado en iniciativas para la promulgación de los lineamientos de política pública en ciberseguridad y



ciberdefensa, seguridad digital y confianza digital.

Más allá de la seguridad y la ciberseguridad, disfruta de textos históricos, de ahí que su género literario favorito sea la novela histórica y policíaca. “Entiendo que el mundo cambió en solo tres años. Hemos vivido una pandemia, un conflicto bélico que amenaza con extenderse; una guerra híbrida basada en el ciberespionaje y la lucha por la hegemonía ideológica y económica

de grandes potencias que trascienden a Latinoamérica y fomentan el rápido cambio del mundo como lo percibíamos. Sin embargo, reconozco que la resiliencia es tal vez la mayor cualidad del ser humano y su rápida adaptación debe ayudar a que las futuras generaciones dispongan de más recursos y de mejores líderes”, fue muy enfático en señalar antes de responder las inquietudes planteadas por la revista.

Revista Sistemas: *¿En su práctica actual qué se entiende como una amenaza híbrida? ¿Qué características tiene?*

Fredy Bautista García: En el contexto actual una amenaza híbrida se entiende como un conjunto de factores que pueden constituir una posible causa de materialización de un riesgo para nuestra organización y sus activos, valiéndose de situaciones no convencionales o poco comunes. Por ejemplo: una campaña de descrédito o desinformación en redes sociales que propicie o impulse un ataque en contra de la infraestructura física o un ciberataque enfocado a explotar una vulnerabilidad en sistemas de seguridad y detección electrónica, que faciliten el actuar de criminales en entornos físicos incrementando el riesgo de intrusión.

RS: *¿Piensa usted que el paradigma de la prevención se ha venido agotando? ¿Se deben habilitar nuevas propuestas para la seguridad?*

FBG: La prevención debe evolucionar hacia unos escenarios de seguridad basados en prospectiva estratégica que faciliten el diseño y aplicación de acciones para anticipar el riesgo en el futuro.

Hoy en día las amenazas tradicionales como el terrorismo o las acciones del crimen organizado aprovechan la realidad social en la región, para impulsar acciones malin-

tencionadas en contra de infraestructuras críticas; para generar el caos y facilitar una intrusión violenta a una sede de especial interés en una organización (incluso un servicio esencial) o para que los esfuerzos de seguridad se distraigan y se concentren en situaciones específicas que permitan aprovechar vulnerabilidades desatendidas.

La posibilidad de anticipar estos escenarios de riesgo y amenaza, conlleva a identificar todas las oportunidades para la prevención, dando lugar a que se integren importantes desarrollos tecnológicos con las tareas de monitoreo y vigilancia física, de manera que las organizaciones trasciendan su perímetro para entender cómo esta realidad económica, política y social de nuestros países puede afectar o comprometer la seguridad en la organización.

RS: *¿Qué es lo más retador en el tratamiento de una amenaza híbrida?*

FBG: Sin duda alguna, el principal reto es incorporar este tipo de amenazas en el espectro de la gestión de los riesgos en la organización. Podrían ser considerados como inverosímiles los planteamientos de un analista de seguridad que advierta una potencial amenaza híbrida mediante el empleo de inteligencia artificial. Por ejemplo, alrededor de un DeepFake utilizado para suplantar a un funcionario o a un contratista y vulnerar el perímetro

de seguridad de un área restringida, la probabilidad de ocurrencia puede ser valorada en forma no acertada para que no sean implementados los controles necesarios.

RS: *¿Cómo define en su práctica actual lo que podría ser una seguridad híbrida?*

FBG: Una visión de la seguridad de manera íntegra. Es decir, que articule las capacidades desarrolladas en la seguridad física con las facilidades tecnológicas de detección y alertamiento. Sin duda, el perímetro se asegura con barreras que impidan los ingresos no autorizados; identificar cómo evoluciona el crimen en el entorno actual, el amplio uso de la tecnología y las vulnerabilidades inherentes, permite proteger procesos esenciales en la cadena logística que provee insumos y recursos a una planta de producción o asegura el traslado de productos hacia las áreas dispuestas para su distribución. Anticipar un bloqueo de vías, por ejemplo, contempla integridad en la trazabilidad en el proceso de traslado de bienes y valores, lo cual exige que la organización prevea nuevas herramientas para fortalecer la seguridad y la defensa.

RS: *¿Cuáles nuevos saberes y conocimientos son necesarios para avanzar en una seguridad híbrida?*

FBG: Considero que lo más importante es tener un pensamiento creativo, inquieto y basado sobre

todo en la innovación y la prospectiva. Debemos adaptar la seguridad hacia tecnologías inteligentes que aprovechen por ejemplo la analítica de datos y los comportamientos para identificar potenciales riesgos.

Históricamente, la seguridad se concebía como un inamovible; hoy en día la inteligencia anticipativa, facilita entender cómo un evento futuro puede afectar la seguridad en la organización y se debe entonces adaptar los esquemas de seguridad y la tecnología aplicada para su mejor aprovechamiento. Es importante igualmente avanzar en la integración de tecnologías para la detección con las capacidades de monitoreo a través de operadores tecnológicos altamente capacitados.

RS: *¿Cuáles retos ve a futuro para las empresas en el contexto las amenazas y la seguridad híbridas?*

FBG: Indudablemente, la infoxicación basada en Fake News y la desinformación pueden generar escenarios de amenazas híbridas muy complejos, como los presentados en 2020 y 2021, en el denominado “Estallido Social”, en el cual muchas sedes financieras y estatales fueron vandalizadas e interrumpidos los servicios, particularmente en las ciudades de Cali y Bucaramanga, por citar solo algunas de las poblaciones más afectadas.

Igualmente, la operación logística y el abastecimiento de materias pri-

mas puede afectar los suministros necesarios para una adecuada gestión operativa en una organización, y ello conlleva a anticipar diferentes alternativas de rutas y medios de transporte que deben ser asegurados para mantener los estándares requeridos en la seguridad operacional.

La suplantación de identidad, con alcance virtual y físico pueden ser facilitadores de robos de activos informáticos o sabotaje y afectación a centros de datos o infraestructuras digitales. Sumados también a la robotización y uso creciente de in-

teligencia artificial en procesos críticos que pueden ser objeto de ciberataques o errores de configuración comprometiendo la seguridad en la organización.

Finalmente, el Malware “as a Service” seguirá creciendo y el crimen organizado podrá acceder a desarrollos de programas maliciosos enfocados en vulnerar la seguridad especialmente los sistemas electrónicos de monitoreo como los CCTV (Circuitos Cerrados de Televisión) o centros de datos de las organizaciones. 🌐

Sara Gallardo M. Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro “Lo que cuesta el abuso del poder”. Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; en la actualidad es asesora y editora en escritura y producción de libros. Es editora de esta revista.

REDUC@TE 2023

Col - Mex

¿Qué es Reduc@te?

es un evento experiencial que aborda las últimas tendencias para enriquecer el uso de las tecnologías digitales y su convergencia en la educación.

**9-14
Octubre**



Más información en:
www.ACIS.org.co
o escríbenos a:
301 5530540
Suscripciones@acis.org.co
Cursos@acis.org.co