Pronósticos de seguridad/ciberseguridad 2020

Article · October 2019

CITATIONS
0

READS
11

1 author:

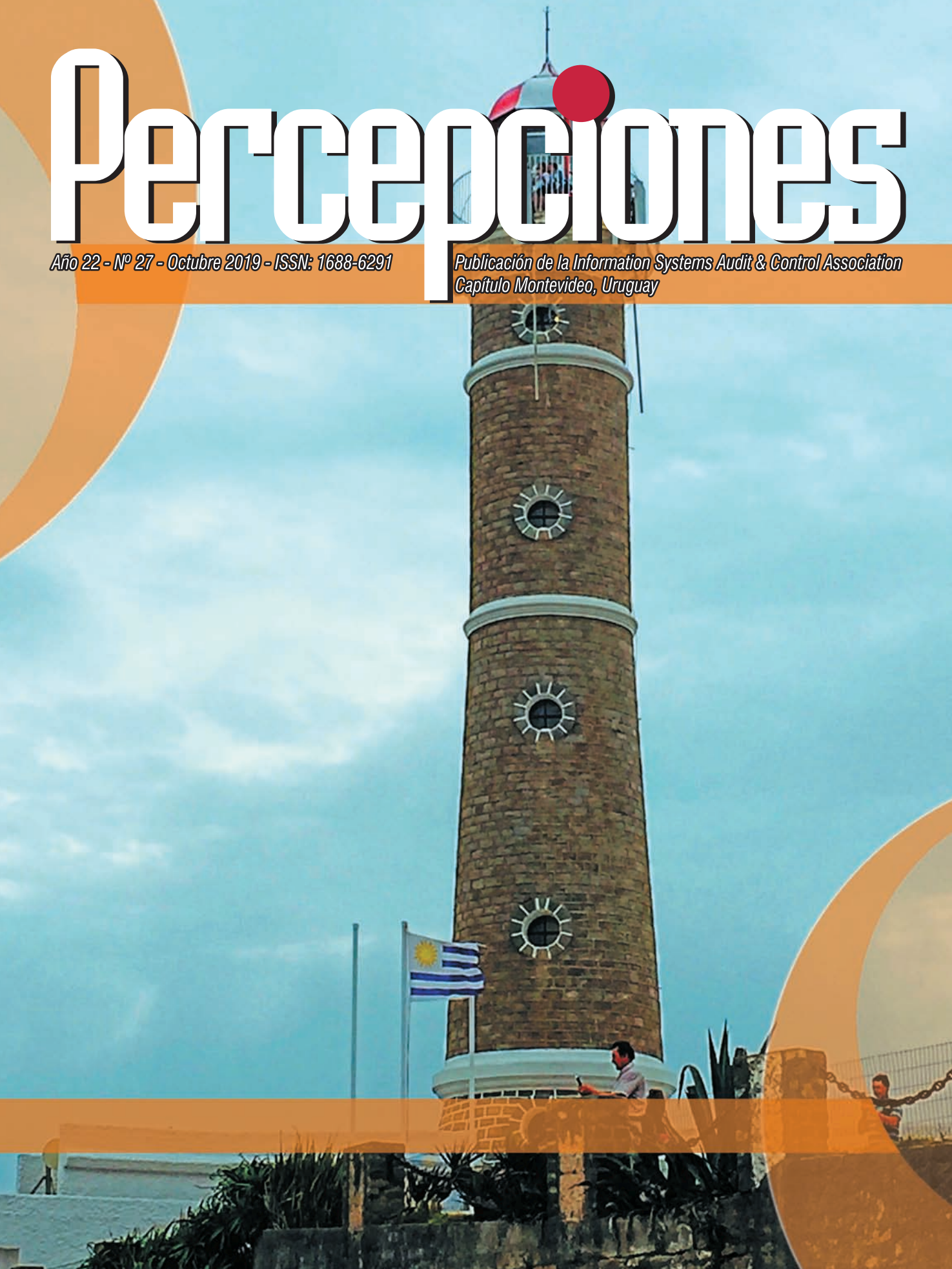
Jeimy J. Cano M.
Universidad de los Andes
71 PUBLICATIONS **100** CITATIONS

SEE PROFILE

Percepciones

Año 22 - Nº 27 - Octubre 2019 - ISSN: 1688-6291

Publicación de la Information Systems Audit & Control Association
Capítulo Montevideo, Uruguay



Percepciones
Publicación de la Information Systems Audit & Control Association
Capítulo Montevideo, Uruguay

Año 22 Nº 27 - Octubre 2019
ISSN: 1688-6291

Percepciones es una publicación de

ISACA®
Confianza en, y valor de los sistemas de información
Montevideo Chapter
200 CHAPTERS STRONG

ISACA - Capítulo Montevideo, Uruguay
Cerrito 420 of. 505
Telefax: 29150319
CP 11000 - Montevideo, Uruguay
E-mail: info@isaca.org.uy
Internet: www.isaca.org.uy
www.facebook.com/isacamontevideo

Registro en el Ministerio de Educación y Cultura según Art. 4º, Ley 16.099, Tomo XI, Fojas 243

Sumario

"ISACA - Capítulo Montevideo, Uruguay es una Asociación sin fines de lucro de miembros profesionales dedicados a la práctica de la Auditoría, Control y Seguridad de Sistemas de Información, y comprometidos con la Educación, la Certificación y los Estándares"
"Nuestra visión es ser el líder global reconocido en Gobernabilidad, Control y Aseguramiento de la Tecnología de la Información."

Pronósticos de seguridad/ ciberseguridad 2020

Jeimy J. Cano M.

Introducción

En un contexto digital asistido por la *desintermediación*, la *distribución*, la *desinformación*, la *deslocalización* y la *desinstalación*, los flujos de información y las plataformas tecnológicas operadas por terceros adquieren una mayor relevancia y atención, no sólo por los ejecutivos de las empresas, sino por los adversarios. Este nuevo escenario de negocios, que no es responsabilidad exclusiva del área de TI, establece nuevas relaciones y retos para crear experiencias novedosas en los clientes y abrir posibilidades inexistentes para las empresas.

Lo anterior exige crear un "retorno de la experiencia", es decir, un nuevo ROI (Retorno de la inversión) que consiste en mapear el viaje de compra de los clientes, aislar los puntos de contacto y los factores que impulsan la experiencia (Maxwell, 2019), de tal manera que se puedan crear patrones y condiciones particulares para todos los participantes, con lo cual la experiencia de compra sea conveniente, ágil y de valor para el comprador.

Este entorno donde se ha superado el uso de los navegadores, por el uso de aplicaciones móviles (de ahora en adelante apps), establece un escenario digitalmente denso donde la conectividad, los flujos de información, los datos personales y las personalizaciones hacen ahora parte de la cotidianidad del mundo actual. Sin perjuicio de que algunos estén o no de acuerdo con esa nueva realidad, es claro que habrá una mayor exposición de las características de las personas y sus gustos, así como el uso de algoritmos especializados para mantener la atención y potencial de compra activado en cada uno de los ciudadanos de internet.

Esta dependencia en aumento de los terceros de confianza, la necesidad de agilidad en el despliegue de soluciones, el uso de la inteligencia artificial para afinar las decisiones, la confiabilidad de la información y el ingreso de la tecnología 5G como habilitador de las futuras ciudades digitales, configura un entorno rico en propuestas de negocios y nuevos vectores de ataques que serán diseñados, para lograr sus objetivos, basados en la economía del adversario, donde se hacen los mínimos esfuerzos para obtener el máximo beneficio.

De esta manera, se presenta a continuación este documento con algunos pronósticos de seguridad/ciberseguridad para el año 2020, como una excusa académica y reflexión

práctica, posiblemente incompleta y limitada, que trata de explorar y conectar ciertos puntos inconexos en el espacio actual de posibilidades, con el fin de motivar reflexiones tanto en los profesionales de seguridad/ciberseguridad, así como en los ejecutivos de las empresas para visualizar escenarios adversos donde un agresor puede tomar ventaja y así estar preparados para cambiar su ecuación de riesgos.

A continuación se presentan las cinco (5) tendencias o pronósticos identificados para un contexto digital e hiperconectado donde más que probabilidades, se debe pensar en posibilidades.

1. Criptominería en IoT

La criptominería es una actividad que se ha venido consolidando desde hace algunos años como una forma de construir base monetaria, algunas veces de manera no autorizada o por debajo de los radares de los reguladores financieros. Para ello la capacidad de cómputo es un elemento fundamental, dado que la generación de criptomoneda demanda dicha capacidad para resolver los retos matemáticos que implica su producción.

"*Los mineros suelen crearse equipos de minería consistentes en múltiples tarjetas gráficas unidas a una misma placa base mediante extensores PCIe, y los fabricantes de placas base han estado aprovechando el boom de Ethereum para sacar modelos específicos para equipos de minería*" (Baños, s.f.). Sin perjuicio de lo anterior, los mineros cada vez más diversifican sus capacidades de procesamiento, con el fin de contar con mayores recursos en su reto por alcanzar nuevos registros de criptomonedas.

En este contexto, con una alta densidad digital cada vez más evidente y mayor conectividad de objetivos físicos con características inteligentes, se advierte una acción proclive de los mineros sobre dispositivos de internet de las cosas, que si bien son pequeños y con limitadas capacidades, es viable construir un *grid* de computación amplio y denso de tal forma que se puedan tener "*granjas de minería*" en segundo plano trabajando en la generación de criptomonedas nuevas o más maduras, como apoyo a otras estrategias ya consolidadas con servidores y equipos de computación caseros capturados mediante engaños a muchas personas.

Este nueva propuesta criptominera tiene la ventaja de poder utilizar capacidad de procesamiento posiblemente imperceptible para los dueños de los dispositivos, habida cuenta que no se cuenta con una práctica regular de medición y seguimiento de las capacidades de estos dispositivos de internet de la cosas, creando un escenario propicio para "robar" procesamiento de bajo perfil de forma no autorizada.

2. Engaños basados en terceros de confianza (Cadena de suministro y actualizaciones de firmware)

Con la transformación digital como fundamento de la propuesta de valor de muchas organizaciones a nivel global, los terceros de confianza se convierten en los aliados estratégicos de muchas de ellas, como base de la configuración y despliegue de soluciones y propuestas innovadoras para sorprender a sus clientes. En este ejercicio, tanto las empresas como los terceros despliegan productos y servicios digitalmente modificados, que por lo general se basan en los fundamentos de las metodologías ágiles, para lograr el efecto deseado de forma efectiva y en tiempos de mercado.

En este contexto, las empresas delegan y confían en sus terceros muchos de los aspectos de seguridad y control, dejando una brecha de monitorización y verificación en el proceso, comoquiera que éstos pueden o no estar certificados y/o cuenten con reportes internacionales que validan sus buenas prácticas al interior de sus procesos y productos. No obstante lo anterior, los adversarios sabiendo que la aplicación de los estándares y buenas prácticas pueden generar cegueras cognitivas y crear una zona de confort para estos

actores, configuran nuevos vectores de ataque que cambian la ecuación de riesgos de la empresa y sus aliados estratégicos aumentando la probabilidad de un incidentes no identificado.

Dichos incidentes, generalmente basados en la confianza y reconocimiento mutuo de los implicados, crea engaños que pueden pasar por actualizaciones de microcódigo en sistemas de control industrial, descarga de aplicaciones actualizadas o ajustes en configuraciones en puntos críticos de conexión entre la infraestructura del tercero y la empresa, de tal forma, que bajo la apariencia de comunicaciones y conexiones confiables (Darkreading, 2019), es posibles crear un evento no deseado que surge por la falta de ejercicios de novedad o inestabilidad, que permita mantener atenta a las partes sobre nuevas tensiones que se crean los posibles adversarios.

Si bien esta tendencia no es nueva, si es consistente con los eventos que se han venido presentando a lo largo del año y que si no se cambian las prácticas vigentes, continuará desarrollándose y avanzando en los procesos cada vez más automatizados y menos monitoreados, particularmente en sectores como el industrial y manufactura, el de la salud y posiblemente el de tecnología dado el incremento de empresas emergentes que buscan desarrollar ecosistemas digitales con aplicaciones y productos de apropiación rápida y expansión viral.

3. Uso adversarial de la inteligencia artificial

La inteligencia artificial como fenómeno tecnológico que ha salido de los laboratorios para convertirse en un producto comercial, da cuenta de una realidad de transformación acelerada de cambios y actividades que antes tomaban tiempo para realizarse. Este ejercicio de automatización e inteligencia basada en el poder de los algoritmos que aprenden tanto de manera supervisada como no supervisada, establece una nueva frontera para crear apuestas particulares en diferentes campos y dominios de la ciencia.

El uso positivo de las capacidades de la inteligencia artificial pasa por diagnósticos médicos, sistemas de detección de intrusos avanzadas, propuestas de pronósticos de eventos en sistemas financieros, entre otras aplicaciones. No se escapan los teléfonos inteligentes, ahora con asistentes basados en este tipo de inteligencia, que atienden las dinámicas de las personas, programan citas y recuerdan aspectos propios de la vida personal y profesional. Los algoritmos de inteligencia artificial están en medio de la dinámica de la sociedad actual, los cuales bien utilizados, se convierten en poderosas herramientas para avanzar y correlacionar eventos de formas novedosas.

Cuando el atacante hace uso de esta misma tecnología y la usa para adelantar sus acciones contrarias, estamos en un campo donde el incierto, el engaño y la premeditación se hacen presentes. Es un ejercicio donde el atacante puede crear contexto de distracción y acciones evasivas que pueden engañar las prácticas actuales de los sistemas más avanzados de detección y análisis. Esto supone aspectos como malware construido para autogenerarse y reconfigurarse, código inteligente que se reescribe a sí mismo en entornos controlados, engaños a otros algoritmos de detección, guerras de información asimétrica, manipulación de tendencias y mercados, entre otras acciones que revelan un campo inestable donde no tenemos reglas concretas para jugar o desafiar (Li, Zhao, Cai, Yu & Leung, 2018).

Avanzar frente a esta nueva amenaza implica desarrollar el concepto de contrainteligencia cognitiva, que adaptando la definición de Jiménez (2019) sobre contrainteligencia, definimos podemos definir como "*el conjunto de actividades que tiene como finalidad localizar, identificar y monitorizar, para neutralizar y, en su caso, contrarrestar y reportar, las actividades no autorizadas de los algoritmos de aprendizaje automático, es decir, aquellas que rompen con las reglas inicial-*

mente establecidas y materializan los riesgos inherentes al desarrollo y puesta en operación de los algoritmos de inteligencia artificial».

4. Compromiso de la integridad de la información

De las características de la información que hoy está más expuesta es la integridad. La confidencialidad y la disponibilidad, si bien igualmente son relevantes, se hace evidente en la actualidad revisar dos atributos más propuestos por Parker (1998) como son la utilidad y la posesión, los cuales son convergentes con la esencia de la integridad. Bajo esta perspectiva, una información es íntegra si en todo su ciclo de vida no ha sido alterada o deteriorada, y si fuese el caso, se tiene registro y trazabilidad de dicha condición.

La *utilidad* definida como el "uso de la información para un propósito" y la *posesión* como "la tenencia o titularidad, el control y la capacidad de utilizar la información" (Parker, 1998, p.240) se vuelven relevantes a la hora de comprender las tendencias actuales donde la manipulación de la información se convierte en un arma estratégica para posicionar un producto o servicios, o un vector de ataque que busca confundir, crear un engaño o facilitar el posicionamiento de intereses de actores con intenciones poco confiables.

Cuando se entiende la degradación o deterioro de la información como estrategia para limitar su utilidad y habilitar usos distintos a los inicialmente establecidos, así como motivar un cambio de titularidad de la misma a un tercero mediante engaños o suplantaciones, con el fin de adelantar acciones no autorizadas a nombre de un intruso, es posible advertir tendencias que afectan la identidad, la veracidad y el control de los imaginarios de las personas en un contexto particular. Cambiar la esencia de la información con fines no conocidos es una realidad que exige más que controles de acceso para poder protegerla y asegurarla.

Parker (1998) de forma visionaria estableció que revelar información sobre un propietario de forma inadvertida, en medios abiertos o sin controles, establece un campo de acción para un adversario donde cualquier uso o utilidad se puede concretar, creando un escenario de negligencia y gestión que se devuelve a su dueño. En consecuencia, perder posesión de la información, no es sólo el acceso a la misma, sino en brindarla a terceros de forma no intencional o inadvertida con la cual se crea conocimiento o se construye nuevas versiones de la misma que están más allá de los propósitos iniciales y legítimos que se tenían.

Enfrentar este desafío, implica pasar del control de acceso al control de uso, donde se hace necesario desarrollos los atributos de posesión y utilidad propuestos hace más de dos décadas, con el fin de fortalecer no solamente la integridad, sino la confidencialidad y la disponibilidad ahora con un propósito y fines superiores y sensibles cuando puede ser utilizada y controlada fuera de un espacio de comprensión y conocimiento autorizado.

5. Redes 5G: hiperconectados y ultravulnerables

El advenimiento de las ciudades inteligentes, la conexión masiva de objetos físicos y la necesidad de pobladores hiperconectados, configura un escenario de alto flujo de información, de infraestructuras basadas en terceros y agilidad en la transmisión de los datos con el fin de concretar la visión de una realidad aumentada, informada y en tiempo real para los moradores de esas ciudades. Por tanto, la aparición de las redes 5G es la respuesta tecnológica que se requiere para cumplir con la promesa de ese entorno hiperconectado, con baja latencia de interacción entre los móviles, la nube y los objetos, y sobremanera, de agilidad y eficiencia en los servicios dispuestos en estas ciudades.

La redes 5G se configuran como la pieza clave del rompecabezas para potenciar servicios y productos en diferentes industrias para

potenciar las capacidades y oportunidades de las personas para acceder a espacios de interacción inexistentes con vehículos autónomos, cirugías asistidas por brazos mecánicos a distancia, sistemas industriales robotizados, sistemas de emergencias conectados y masivos, entre otras actividades. De esta forma, estas nuevas redes potenciarán el desarrollo de una economía digital, donde los bienes intangibles y el internet de las cosas serán parte natural de esta nueva dinámica.

A la fecha cinco son las empresas que están a la vanguardia de esta nueva tecnología: Nokia, Ericsson, Samsung, Huawei y ZTE, la dos últimas representan intereses chinos, con lo cual se crean tensiones geopolíticas, donde "*la posibilidad de que los fabricantes chinos introduzcan en sus productos dispositivos que permitan el envío de información de forma encubierta o que, sencillamente, puedan escapar al control del operador de esos equipos poniendo en peligro la seguridad, integridad o confidencialidad de los sistemas*" (Moret, 2019) de las empresas y las naciones.

Considerando que la infraestructura de las redes 5G configura un ecosistema de ecosistemas, dado que se virtualizan las infraestructuras de redes y se transforman en software de gestión y transmisión, que disminuyen la latencia, reducen un 90% el consumo de energía de la red, ofrecen un tasa de datos de hasta 10Gbs (Gemalto, 2019), entre otras características, se funda un escenario emergente de amenazas dado las limitadas opciones de seguridad y control consideradas en el diseño y desarrollo de esta tecnología.

Un reciente estudio del Instituto Brookings (Wheeler & Simpson, 2019) establece cinco razones por las cuales las redes 5G serán más vulnerables a ciberataques que sus predecesoras. Las razones son:

- La red se ha alejado de la conmutación centralizada basada en hardware y ha pasado a un enrutamiento digital distribuido y definido por software.
- Virtualización en software de funciones de red de alto nivel que anteriormente realizaban los dispositivos físicos.
- Gestión de la red basada en software.
- Expansión del ancho banda de forma dinámica.
- Conexión de miles de millones de dispositivos IoT.

Dado este entorno de software sobre una red distribuida, proclive a los ataques, las organizaciones y naciones deben tomar sus precauciones y acciones concretas para avanzar en una estrategia de protección proactiva en el despliegue de los sistemas socio-técnicos sobre este nuevo ecosistema: infraestructura, aplicaciones y servicios. Surge un deber cibernético de cuidado de todos lo participantes para compartir y asegurar la dinámica de este entorno que aún está por conocerse y descubrirse.

Reflexiones finales

Entender estas cinco tendencias revisadas previamente es reconocer que es necesario superar el enfoque de control y cumplimiento vigente en las empresas, para movilizar a las organizaciones y naciones hacia estrategias accionables que las configuren como corporaciones y naciones resilientes, donde se privilegian las relaciones con el entorno y la generación de valor para sus clientes y ciudadanos (Deloitte, 2018).

La nueva generación de disrupciones tecnológicas creará nuevos entornos desafiantes para los cuales no se puede estar preparados. Por tanto, es clave que las naciones y empresas emprendan con frecuencia un viaje al futuro desde las simulaciones y la experimentación, con el fin de exponer las inestabilidades e inciertos que se pueden presentar con el fin de encontrar patrones y tendencias sobre las cuales poder trabajar de forma previa y aprender de ellas.

Los cinco pronósticos detallados en este breve reporte son una reflexión limitada de

un entorno cada vez más volátil e inestable, que busca comprender posibles vectores de ataques y contextos en los cuales los adversarios pueden tomar ventaja para incrementar la incertidumbre en las variables de gestión de riesgo de los analistas organizacionales.

En consecuencia, la invitación es a construir y actualizar de forma permanente el mapa de amenazas digitales del entorno actual, sobre un territorio que cambia de forma dinámica y muchas veces rizomática creando zonas grises y ocultas, propias de las cegueras cognitivas, para tensionar y desconectar aquello conocido y así, intentar descubrir los patrones y retos de los adversarios.

Referencias

Baños, D. (s.f.). ¿Qué es la criptominería? *Revista Muy Interesante*. Recuperado de: https://www.muyinteresante.es/tecnologia/articulo/que-es-la-criptomineria

Darkreading (2019). Firmware Vulnerabilities Show Supply Chain Risks. Darkreading. Recuperado de: https://www.darkreading.com/vulnerabilities—threats/firmware-vulnerabilities-show-supply-chain-risks/d/d-id/1335313

Deloitte (2018) Auditing the risks of disruptive technologies. Internal Audit in the age of digitalization. *Report*. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-auditing-the-risks-of-disruptive-technologies.pdf

Gemalto (2019). Red 5G – Características y usos de esta tecnología. Recuperado de: https://www.gemalto.com/latam/telecom/inspiracion/5g

Jiménez, F. (2019). *Manual de inteligencia y contrainteligencia*. Sevilla, España. CISDE

Li, P., Zhao, W., Cai, W., Yu, S. & Leung, V. (2018). A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. *IEEE Access*. 6, 12103-12117. Doi: 10.1109/ACCESS.2018.2805680

Maxwell, J. (2019). ROX is the new ROI: Prioritizing customer experience. *Strategy + Business*. Recuperado de: https://www.strategy-business.com/blog/ROX-Is-the-New-ROI-Prioritizing-Customer-Experience

Moret, V. (2019). El despliegue de las redes 5G, o la geopolítica digital. *Real Instituto Elcano*. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari31-2019-moret-despliegue-de-redes-5g-geopolitica-digital

Parker, D. (1998). *Fighting computer crime: a new framework for protecting information*. New York, USA: John Wiley & Sons.

Wheeler, T. & Simpson, D. (2019). Why 5G requires new approaches to cybersecurity. Racing to protect the most important network of the 21st century. *Report*. Brookings Institute. Recuperado de: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

Jeimy J. Cano M., Ph.D, CFE

Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes, Colombia. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Administración de Negocio por Newport University, CA. USA. y Ph.D en Educación (Ed.D) por la Universidad Santo Tomás, Colombia. Cuenta con más de 20 años de experiencia como académico, profesional y ejecutivo en temas de seguridad de la información, privacidad, ciberseguridad, sistemas de información, gobierno y Auditoría de TI. En 2016 recibió el reconocimiento como "Cybersecurity Educator of the Year 2016" para Latinoamérica por el Cybersecurity Excellence Awards. Es examinador certificado de fraude (CFE en inglés). Cuenta con más de 150 publicaciones en revistas y eventos internacionales, así como conferencista invitado a foros y conferencias nacionales e internacionales en temas de seguridad y control en Latinoamérica. Profesor Asociado de la Escuela de Administración de la Universidad del Rosario en Colombia. Profesor Distinguido de la Facultad de Derecho de la Universidad de los Andes en Colombia. Director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas. http://insecurityit.blogspot.com