No. 143 Abril - Junio 2017 ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacionales S.A. No. 2015-186 4-72, vence 31 de Dic. 2017

Cuarta revolución industrial: retos y paradigmas en seguridad y control

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

1st Pure Player MSSP in LATAM

Digiware 5th
Managed Security Services Market in Latin America.
Market Share and Competitive Analysis of Frost & Sullivan.

DIGITAL TRANSFORMATION

MACHINE LEARNING

ARTIFICIAL INTELLIGENCE

DIGIWARE
Your digital security strategic partner

Aseguramos la transformación digital a través de herramientas de Inteligencia Artificial y Machine Learning.

Consultoría
Definición, implementación y oportuno mantenimiento de programas estratégicos de seguridad digital, integradas con el objetivo del negocio.

Soluciones tecnológicas
Digiware provee las mejores soluciones del mercado, ajustadas a las necesidades del cliente, brindadas en cada herramienta, respaldo y soporte constante.

Seguridad Gestionada SOC
Gestionamos inteligencia digital, transformándola en estrategias de negocio con ROI y visibilidad predictiva de incidentes.

Formación del Talento Humano
Actualícese con nuestros expertos de I+D, comprometidos con las problemáticas en seguridad digital y conviértase en un especialista.

SECURING DIGITAL TRANSFORMATION

#DigiwareSuAliado
#DigiwareSecurity
#JornadaDeSeguridadDigiware

Digiware | @Digiware | www.digiware.net

Centroamérica y El Caribe - Chile - Colombia - Ecuador - EE. UU. - Perú

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril - Junio 2017
Calle 93 No.13-32 Of. 102
Teléfonos 616 1407 – 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

Moodlemoot Colombia 2017

Bogotá, 31 de agosto y 01 de Septiembre

LLAMADO A CONFERENCISTAS Y TALLERISTAS

Talleres 31 de agosto

Queremos saber qué estás haciendo en Moodle.

Este año invitamos a los aspirantes a talleristas a participar con propuestas que se destaquen por su nivel de interactividad con el público.

Los talleres tendrán una duración de 4 horas.

Categorías: Algunas de las categorías propuestas son:

¿Cómo hacerlo en Moodle?

- Learning Analytics
- Diseño Instruccional
- Integración de herramientas y Plugins
- Investigaciones en Moodle

¿Qué hacer con Moodle?

Conferencias 01 de septiembre

Queremos saber qué estás haciendo en Moodle.

Este año invitamos a los aspirantes a conferencistas a aplicar en las siguientes modalidades y/o temáticas.

- **Pedagógico:** Prácticas pedagógicas emergentes, Gamificación y neuroeducación, Aprendizaje adaptativo, contenidos dinámicos y Aprendizaje móvil.
- **Técnico y Tecnológico:** Plugins, Analíticas de aprendizaje, Personalización de la interfaz y Sistema de reportes.
- **Tendencias y Casos de éxito:** Casos de éxito en el uso de la plataforma y Experiencias de éxito en las empresas.

Moodlerooms

2017 moodlemoot COLOMBIA

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Inscríbete en: http://bit.ly/2rFgak8

Más información del evento: http://bit.ly/2aBmkub

Cuarta revolución industrial: anticipo de un nuevo desarrollo de la humanidad

El evidente impacto de la cuarta revolución industrial en la sociedad completa, pone de manifiesto desafíos sociales, económicos, políticos y tecnológicos. En este sentido, los nuevos productos y servicios digitalmente modificados exigen un análisis de los retos y paradigmas de la seguridad y el control, como fundamento de la confianza requerida para que se haga realidad su promesa de valor.

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

No existe un espacio en el que la cuarta revolución industrial deje de ser protagonista. Figura en primera fila en mesas de debate, consejos académicos, conferencias, charlas informales y en los medios de comunicación especializados y los de interés general.

Esta nueva realidad digital y tecnológicamente modificada establece un cambio de paradigma en la sociedad actual que entra en tensión con las estrategias de negocio conocidas, con el fin de cambiar una percepción del cliente y crear una experiencia dife-

rente en el desarrollo de las actividades propias de las personas y sus retos.

Por esa razón, la revista Sistemas dedicó de lleno las páginas de su edición número 143, a hilvanar y deshilvanar los retos y paradigmas que la seguridad y el control afrontan en el marco de la cuarta revolución industrial. Un ejercicio que confronta los saberes previos de la práctica de seguridad de la información frente a las exigencias de los negocios, que demandan asumir riesgos retadores y calculados.

Cada una de las secciones se ocupa de una mirada al respecto. Con una visión holística, el ingeniero Eduardo Carozo Blumsztein aborda los beneficios, impactos y desafíos tecnológicos, como columnista invitado. El ingeniero Carozo, profundiza en las bondades de esta nueva revolución, con una mirada reposada sobre las condiciones de seguridad y control requeridas.

Por su parte, Rebecca Herold, reconocida y premiada consultora internacional, nos concedió una amplia entrevista, donde nos comparte sus puntos de vista sobre los asuntos más neurálgicos de la seguridad de la información y la protección de los datos. Desde su vista global, nos ilustra las exigencias y grandes desafíos que implica un flujo de datos continuo e inesperados entre los "objetos digitalmente modificados".

En la mesa de debate para la sección "Cara y Sello", nos preguntamos si la seguridad y el control son viables, también en el marco de la cuarta revolución industrial. Expertos analistas –por cierto de muy variados perfiles-, asistieron al encuentro para analizar aspectos tales como los riesgos, las amenazas, los cambios en los estándares, las prácticas de seguridad y de control, los cambios normativos sobre el tratamiento de la información, las empresas con infraestructura crítica, el analista de seguridad, además de las habilidades, competencias y conocimientos de los nuevos profesionales, entre los más destacados asuntos.

La encuesta nacional de seguridad informática 2017, capítulo Colombia, realizada por esta Asociación, a través de Internet, contó con la participación de 128 encuestados, quienes con sus respuestas permiten conocer la realidad del país. Este estudio cumple con varios propósitos. En primer lugar, muestra el panorama de las organizaciones colombianas frente a la seguridad de la información y/o ciberseguridad, y su respuesta a las demandas del entorno actual. En segunda instancia, es un instrumento referente para Colombia y Latinoamérica, en la medida en que llama la atención de todos los sectores interesados en los temas relacionados con la seguridad de la información.

El primero de los artículos, plantea un ejercicio de construcción conjunta en ciberseguridad y seguridad de la información que se denomina "*Juegos de guerra*". En un contexto geopolítico inestable, con amenazas digitales inciertas y nuevos competidores creando incertidumbres globales, las organizaciones deben avanzar rápidamente en espacios de construcción colectiva que permitan crear capacidades inexistentes frente a escenarios que aún no ocurren (Cano, 2017).

Bajo esta perspectiva los conceptos de ciberseguridad y seguridad de la información, comienzan a reconstruir

sus fronteras naturales y transitan hacia prácticas, algunas desconocidas, sobre contextos digitalmente modificados, en los que cualquier evento puede ocurrir y afectar las condiciones normales de la operación de una empresa. Posiblemente, esto implica desconectar y repensar conceptos sobre los cuales los estándares conocidos han sido planteados, para encontrar nuevas oportunidades que construyan un nuevo normal de "confianza" para las empresas en una sociedad tecnológicamente definidas.

Y para finalizar, el segundo artículo denominado "*IoT: interconexión digital, un reto mayor de seguridad*", describe el panorama de los cambios que los nuevos desarrollos tecnológicos introducen cuando las "cosas" son modificadas tecnológicamente. El autor establece un escenario de desafíos de seguridad y control que son relevantes para todos aquellos que quieren comprender las nuevas realidades emergentes propias del "internet de las cosas".

En resumen, esta edición de la revista nos permite explorar aspectos novedosos de una realidad que pronto nos abordará con todos sus desarrollos, por lo cual se hace necesario iniciar las reflexiones sobre las implicaciones de la seguridad y control como fundamento de la actualización de las prácticas de protección que la sociedad deberá asumir, para concretar las ventajas y logros que se esperan de esta nueva era, donde lo digital deberá converger con lo social, como anticipo de la transformación de las nuevas competencias cognitivas que lleven a un nuevo nivel de desarrollo a la humanidad.

Referencia

Cano, J. (2017) Juegos de guerra. Un ejercicio de construcción conjunta en ciberseguridad y seguridad de la información. *Revista Sistemas*. No. 143. Abril-Junio.

Jeimy J. Cano M., Ph. D., CFE. *Profesor Asociado, Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph. D. en Administración de Negocios de Newport University, CA. USA y Ph. D. (c) en Educación de la Universidad Santo Tomás. Obtuvo un Certificado Ejecutivo en Liderazgo y Administración del MIT Sloan School of Management y es egresado de los programas de formación ejecutiva de Harvard Kennedy School of Government: Liderazgo en el siglo XXI: Agentes globales de cambio y Ciberseguridad: Intersección entre política y tecnología, ambos en Boston, USA. Ha sido reconocido como "Cybersecurity Educator of the year 2016" para Latinoamérica, por Cybersecurity Excellence Awards. Es Examinador Certificado de Fraude – CFE por la ACFE y Cobit5 Foundation Certificate por ISACA. Cuenta con más de 20 años de experiencia como académico y profesional en seguridad de la información, auditoría de TI, forensia digital, delitos informáticos, privacidad y temas convergentes en Colombia y Latinoamérica y más de un centenar de publicaciones en diferentes eventos y revistas nacionales e internacionales.*

Programación Académica

Seminario Taller Virtual Sincrónico Indicadores para la Gestión de Proyectos

25 y 26 de Julio

Curso Contratación e Interventoria de Desarrollo de Software con Metodologías Ágiles

Del 25 de Julio al 01 de Agosto

Introducción al diseño de Bodegas de datos y Modelaje dimensional practicando con Pentaho

Del 11 al 19 de Julio

Curso Virtual Sincrónico Scrum Master con Certificación Oficial

Del 8 al 23 de Agosto

Curso: PMP-Online

Nota: Este curso se puede iniciar en la fecha que usted disponga y tiene tres (3) meses para realizarlo.

ACIS

ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

¡INSCRÍBETE YA!

Calle 93 No. 13 - 32 - Oficina 102
Teléfonos: 616 1407 / 09 - 301 553 0540
www.acis.org.co - cursos@acis.org.co - acis@acis.org.co

A Rebecca Herold hay que creerle

Reconocida y premiada consultora en el mundo, especialista en los asuntos más neurálgicos de la seguridad de la información, exitosa conferencista y profesora, entre otros calificativos no menos importantes, se refiere a los retos y paradigmas de la seguridad informática, en el marco de la cuarta revolución industrial.

Sara Gallardo M.

Si de los temas más neurálgicos sobre seguridad de la información se trata, Rebecca Herold no está por fuera del panorama mundial.

Sus más de veinte años trajinando en todas las aristas de ese ambiente, la ubican entre los tres líderes más influyentes como asesora, consultora con toda clase de certificaciones, profesora en prestigiosas universidades, además de proveedora de servicios desde su propia empresa (Rebecca Herold & Associates). Así lo registra, por ejemplo, la revista IT Security, entre otras publicaciones que hacen eco de su ejercicio profesional.

En la actualidad, lidera el comité de estándares de privacidad en el Instituto Nacional de Estándares y Tecnología (**NIST**) y provee servicios para la plataforma de gestión de la privacidad y seguridad de la información para distintas organizaciones, dentro de un marco normativo y de soporte de personal.

Ha publicado catorce libros y prepara el décimo quinto. Así mismo, la industria registra más de 200 artículos, columnas en periódicos y revistas de circulación mensual, sin contar los cientos de entrevistas publicadas en importantes medios de comunicación.

Sin más preámbulos y con la sencillez que la caracteriza respondió la entrevista.

El texto completo está en el siguiente link:
https://goo.gl/FuQRWp

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" 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 y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res); corresponsal de la revista IN de Lanchile. En la actualidad, es editora en Alfaomega Colombiana S.A., firma especializada en libros para la academia y editora de esta revista.*

La industria 4.0, tecnología de la información y ciberseguridad

Lo que nos interesa a los ingenieros.

Eduardo Carozo Blumsztein

Introducción

El presente artículo intenta enfocar los principales beneficios, impactos y desafíos tecnológicos del desarrollo de la Industria 4.0, en una visión holística evitando proponer soluciones puntuales.

Industria 4.0, un cambio real

La nueva transformación tecnológica, cambia los modelos de negocios, los liderazgos en múltiples sectores de la economía, los mercados de trabajo y los comportamientos de consumo de la sociedad moderna.

Se espera que su fuerza disruptiva sea la mayor que ha existido y los primeros vientos ya estén revolucionando los sectores financieros, logísticos y comerciales. Existen varios ejemplos ya operativos donde los ahorros generados por la optimización de los procesos o la eliminación de intermediarios superan ratios del 50% en industrias como la aviación, el transporte o la hotelería.

Como se puede visualizar en el gráfico 1, el ingreso de 50 millones de usuarios a *pokemon-go*, sólo tardó 19 días, frente a los exitosos cuatro años de la *world wide web*. Además, debe notarse que esa aplicación fue la primera que pudo implicar seriamente a muchos millones de usuarios en el manejo y gestión de una aplicación de realidad aumentada, logrando una clara interacción entre el mundo físico y el mundo digital.

Por otra parte, cada vez más estamos vinculando los aspectos de control de corte biológico en las nuevas aplicaciones y dispositivos, tanto en animales como en la interacción de lo electrónico, con las funciones biológicas del cuerpo humano. La profusión de dispositivos *wearables* e implantes para resolver problemas cerebrales, cardíacos o nerviosos es cuantiosa y todos ellos tienen su momento de conectividad e intercambio de información con diferentes sistemas y redes.

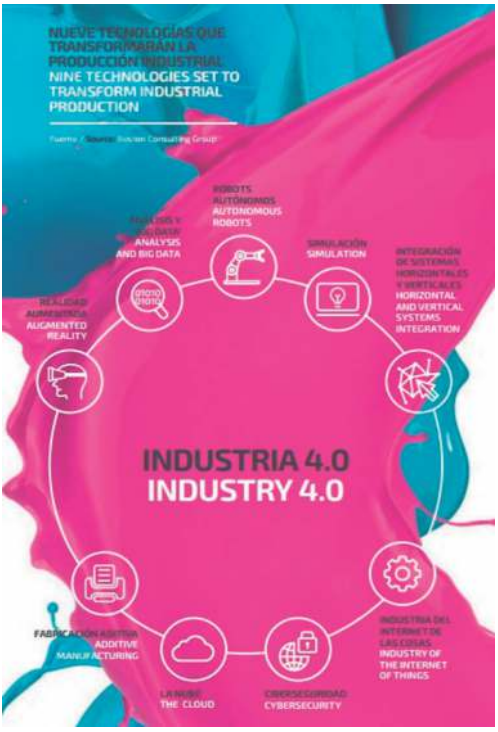
Imaginemos que necesitemos comprar una chaqueta. En no más de cinco años, podremos ordenar en forma verbal a algo que luce como un espejo (con realidad virtual sobrepuesta), en un probador de una tienda, qué estilo, tipo de paño y color, forma de cuello y bolsillos, tamaño y forma de botones, qué interiores y exteriores, etc., y luego superponer la prenda a mi cuerpo

Gráfico 1

con mi ropa actual, verlo en realidad virtual en tres dimensiones y en caso de que sea de mi agrado, darle aceptar al pseudo-espejo para que lo construya.

Al salir del probador las impresoras 3D y los robots de costura, estarán realizando esa prenda exclusiva y en los cinco minutos siguientes nos será entregada. Al salir de la tienda el sistema de reconocimiento facial nos identificará, y asociando el producto que he adquirido, realizará el cobro en forma directa a nuestra cuenta bancaria.

Esta es una escena que hace unos cinco años se consideraba futurista, pero ya es completamente posible y es parte de la nueva revolución industrial, llamada la cuarta revolución industrial.



Esta revolución no cambiará sólo lo que hacemos, sino en buena parte lo que somos. Como mostramos en los ejemplos anteriores, la misma se vivirá en tres espacios esenciales para la humanidad: la física, la digital y la biológica. Durante esta revolución, las industrias elevarán a un nuevo nivel el grado de digitalización de sus procesos y maquinarias.

Algunos países (como Uruguay) consideran estos cambios como una nueva oportunidad de re-industrialización, en la cual se pueda sostener el actual ritmo de crecimiento económico, a pesar del envejecimiento progresivo de su población. En los análisis prospectivos más relevantes se pronostica que se producirán en los próximos 20 años más bienes y servicios que en los últimos 50 años (Siemmens).

En el modelo propuesto por el BCG (*Global Management Consulting*), se observa que la ciberseguridad se considera con el mismo grado de importancia que otras dimensiones más conocidas en el mundo tecnológico como *IoT*, *Big Data Analysis*, Robótica, la nube, etc.

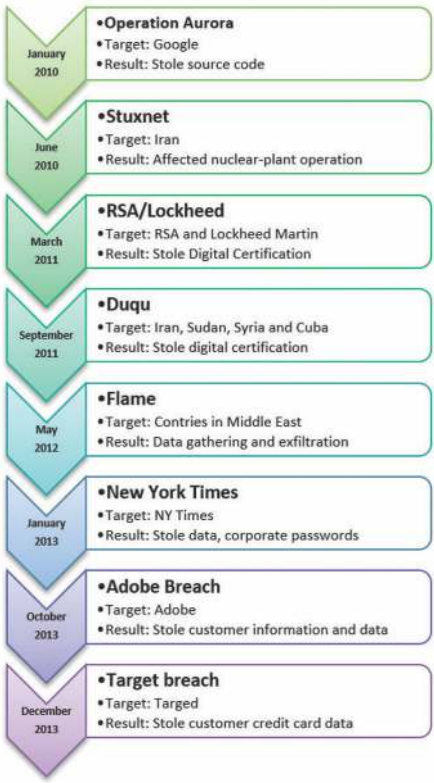
Ciberseguridad y la industria 4.0

¿Qué papel le toca en este escenario futuro a la seguridad de la información, seguridad informática, ciberseguridad y demás definiciones existentes?

En el momento de escribir estas líneas, hemos sufrido el ataque de WannaCry, han sido afectados en pocas

horas más de 300.000 equipos alrededor del mundo. Fue el ataque más visible a nivel global del que hay registro.

La prensa ha escrito ríos de tinta sobre dicho *malware* y la mayoría de las personas no conoce cómo se propaga, pero lo que todos entienden es que su información queda encriptada y que le aparece un aviso que le pide dinero para devolver su información, o la pierden… ¿Qué pasaría si en lugar de robar fotos familiares en PC's particulares, se pudiera robar información asociada a las configuraciones de los sistemas de control automático de las ciudades inteligentes? o ¿se ingresara al servidor de historias clínicas de una entidad médica y se capturara la información de sus pacientes?, ¿cuánto dinero se podría cobrar por esa información? o ¿se tomará el control sobre la nube transaccional financiera de un servicio de *home-banking* de un banco internacional? Estos ataques descritos o ya se dieron o están actualmente ocurriendo y son parte de la historia reciente.



Desde hace un tiempo equipos de investigadores de entidades con alto grado de capacidad financiera están desarrollando e instalando *malware* específico en los sistemas de información críticos alrededor del mundo, con la intención de efectuar ataques selectivos en el momento más adecuado, (o dicho de otra manera: cuando brinde máxima rentabilidad en términos de impacto). Dichas herramientas denominadas APT (*Advanced Persistent Treath*), en general, son utilizadas por agencias de seguridad de las diferentes potencias mundiales y otras entidades no gubernamentales, con finalidades no explícitas. Uno de los ejemplos que tomó notoriedad últimamente es la herramienta *eternalblue*, supuestamente desarrollada por la NSA (*National Security Agency*). La misma fue publicada por el grupo de *hackers* "Shadow Brokers" y en unas semanas la misma fue masivamente explotada para distribuir a nivel global el *ransomware WannaCry*, con el que comenzamos esta sección.

Estas herramientas se desarrollan con el objetivo de pasar inadvertidas y quedar instaladas ocasionalmente por años sin activarse en los diferentes sistemas objetivos. Dado que no se conoce su funcionamiento previo (por ser *zero day exploit*) se vuelve vital tener implementado en toda red que gestione sistemas de información críticos, seguridad en profundidad, gestionando los paquetes en diferentes segmentos de red e instalando inspección de paquetes en cada segmento especializado, no permitiendo la salida de paquetes de datos diferentes a lo esperado por diseño en la red. La implementación en algunos de estos segmentos de soluciones IPS (*Intrusion Prevention Systems*) es también una buena práctica requerida. Para aquellas soluciones basadas en comunicaciones *web* (la mayoría de las actuales), debería ser de uso obligatorio la implementación de un *Web Application Firewall* (WAF).

Las aplicaciones y anexos a los sistemas de información críticos deben ser tratados con el mismo nivel de exigencia que la implementación original, teniendo en cuenta aspectos de seguridad lógica, física y ambiental, debiendo ser testeados en forma detallada y explícita contra fraude, cumplimiento de *performance* y usabilidad, gestionando su ciclo de desarrollo, *testing*, producción y resguardo, en ambientes separados.

Por otra parte, resulta esencial la concientización permanente de las amenazas existentes en los usuarios de los mismos. Es definitivamente el punto más débil de la cadena y los usuarios son víctimas fáciles de múltiples engaños, tanto en la instalación de aplicaciones y utilización de código, (básicamente intentando ahorrar costos con código pirata, o creyendo que todo lo gratis se puede instalar sin validación, etc.), como también en la pérdida de sus credenciales de acceso. Para el acceso a información más sensible debería implementarse a los procesos de autenticación clásicos, algún componente de análisis biométrico adicional,

como reconocimiento facial, de huella digital o similares.

El proceso de migración a la nube, conlleva algunos cuidados extraordinarios en los procesos de control de acceso y gestión de interconexiones y es necesario incorporar además algunas barreras de criptografía avanzada, y en lo posible *firewall* de acceso a bases de datos.

Integridad y transparencia de los contratos en la Revolución 4.0

En el año 2016 nace *Ethereum*, basada en tecnología *Blockchain* que permite elaborar contratos inteligentes en forma autónoma y certificada ya sea persona-persona, persona-máquina, máquina-máquina. Estos contratos pueden ser predefinidos, pero se pueden firmar automáticamente y la figura del notario la realiza la *blockchain* en forma inmediata, con los requerimientos de integridad, disponibilidad y confidencialidad que se requieran en cada caso.

Este cambio, provocará un aumento sustantivo de la velocidad de desarrollo de las diferentes redes, porque será posible establecer *Smart-contracts* en tiempo real entre los diferentes dispositivos sin intervención humana. De esa manera, un dron podrá entregar paquetes a terminales de expendios de alimentos robóticas y autónomas, para alimento de humanos y definir en tiempo real las transacciones comerciales necesarias, sin peligro de robos, pérdidas de dinero o de información.

La gestión de los contratos por la *blockchain*, posibilita dos aspectos fundamentales desde la visión de ciberseguridad, además de la validación automática: la Integridad y Disponibilidad, de información clave. Una red basada en la tecnología *blockchain* en

la medida que va evolucionando ciclo a ciclo, permite que la información contenida en los contratos se vaya haciendo más estable e inmutable, convirtiéndose en un grupo de transacciones aseguradas y verificables por los distintos involucrados en tiempo real.

Esto permite integridad, transparencia y sobre todo la interactividad en tiempo real con dispositivos y personas para mejorar las redes comerciales en forma sustantiva. Esta tecnología está llamada a ser el futuro elemento que gestione la transaccionalidad y la vincule con la gestión comercial en forma definitiva.

Adicionalmente, resulta muy fácil generar sistemas de control de trazabilidad de procesos industriales de manera de poder asegurar la calidad de todos los proveedores de una cadena de valor compleja.

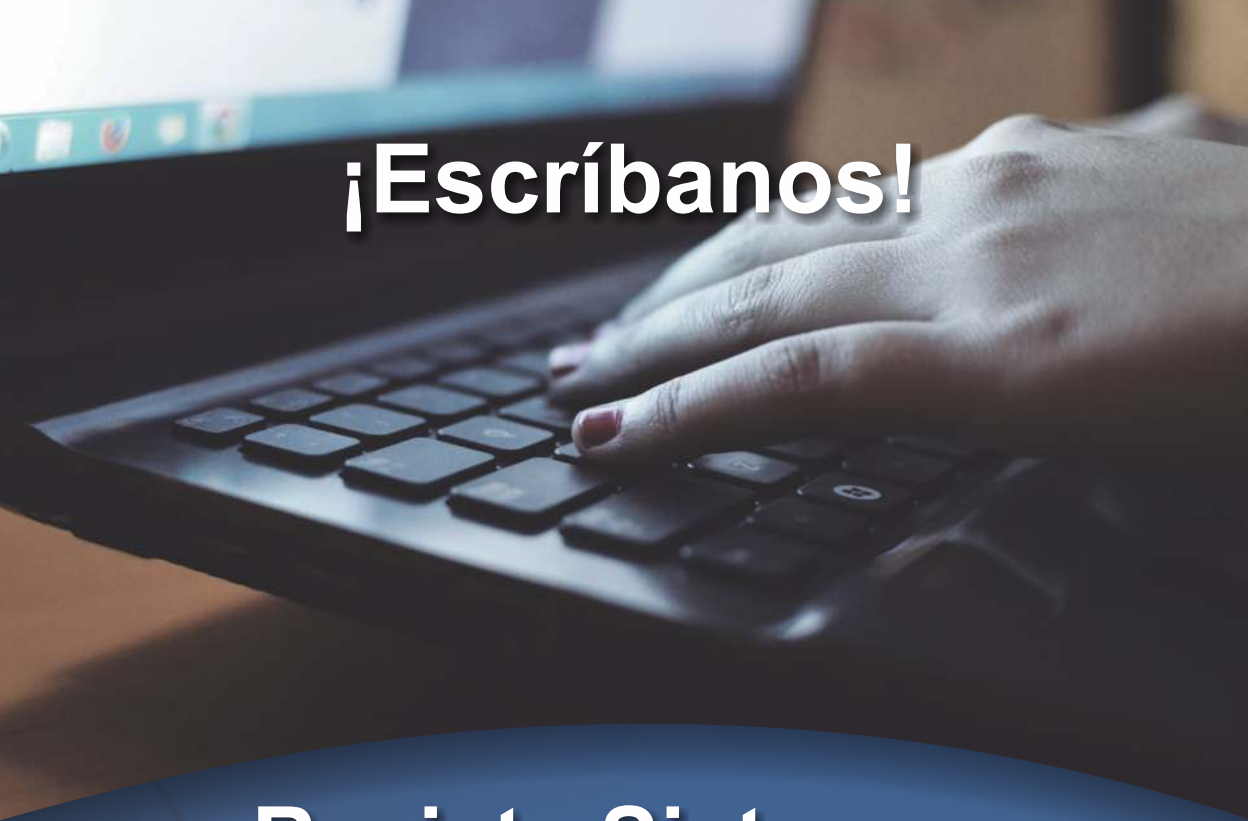
Debe considerarse muy seriamente este tipo de soluciones, tanto públicas como privadas, para la nueva Industria.

Conclusiones

Está todo listo para que las cadenas productivas mundiales migren a la Industria 4.0, solo deberán ajustarse las conductas asociadas a aseguramiento de la información (hacerlas más robustas) en todas las fases de desarrollo, producción, telecomunicaciones y desarrollar planes de contingencia y centros de respuesta, porque los problemas asociados a incidentes de seguridad del futuro tendrán un impacto mucho mayor si ocurren.

Es un mundo apasionante donde nuestros técnicos tienen un rol fundamental. Tendremos posibilidades casi infinitas, pero casi todas las nuevas implementaciones dependen tener un robusto sistema de seguridad de la información, nunca deberíamos olvidarlo.

Eduardo Carozo Blumsztein. *Ingeniero con Maestría en Telecomunicaciones. Es gerente de Comercialización de ITC SA. Ha dirigido proyectos en el área de ciberseguridad desde hace más de 12 años, en organizaciones como Antel, Agesic, OSE, en Uruguay, Carboclor, BA-Csirt en Argentina, Senatics y COPACO en Paraguay, EcuCERT en Ecuador, Cicte de OEA, Inteco de España, Proyecto AMPARO de Lacnic entre otros. Ha sido orador en varias universidades tales como UNAM y Politécnico Nacional de México, UPM de España, Universidad de Chile, Universidad de Buenos Aires. Es docente de posgrado del Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República (Udelar) y de grado en Seguridad Informática de la Universidad de Montevideo, integra el equipo de representantes académicos de Criptored de la Universidad Politécnica de Madrid.*



¡Escríbanos!

Revista Sistemas

Asociación Colombiana de Ingenieros de Sistemas (ACIS)

Diríjase a la editora de la revista:
Sara Gallardo M.
saragallardo@acis.org.co

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

Encuesta nacional de seguridad informática 2017

Desafíos de la cuarta revolución industrial

Realizada por la Asociación Colombiana de Ingenieros de Sistemas (Acis).

Andrés Ricardo Almanza Junco

La encuesta nacional de seguridad informática, capítulo Colombia, realizada por ACIS a través de Internet, contó con la participación de 128 encuestados, quienes con sus respuestas permiten conocer la realidad del país.

Este estudio cumple con varios propósitos. En primer lugar, muestra el panorama de las organizaciones colombianas frente a la seguridad de la información y/o ciberseguridad, y su respuesta a las demandas del entorno actual. En segunda instancia, es un instrumento referente para Colombia y Latinoamérica, en la medida en que llama la atención de todos los sectores interesados en los temas relacionados con la seguridad.

Metodología

El análisis presentado a continuación se desarrolló con base en una muestra aleatoria y de manera interactiva, a través de una página *web* dispuesta por Acis, para tal fin. Se han tenido en cuenta los aspectos más sobresalientes de los resultados obtenidos, en procura de mostrar a los lectores las tendencias identificadas.

Lo nuevo

En este 2017 el formato oficial de la encuesta cuenta con algunas modificaciones. Contempla unas nuevas preguntas, así como una revisión sobre lo evaluado año tras año, en la búsqueda de conocer mejor el ambiente que viven las organizaciones colombianas y latinoamericanas, en el marco de la seguridad de la información y/o ciberseguridad.

Lo nuevo está centrado en conocer más sobre la realidad del Chief Information Security Officer (CISO) o Director de Seguridad de la Información, frente a un escenario digital cada vez más complejo, dinámico, volátil e incierto, para que los encuestados analicen su entorno, así como el tipo de información que el CISO entrega a las organizaciones.

Datos generales

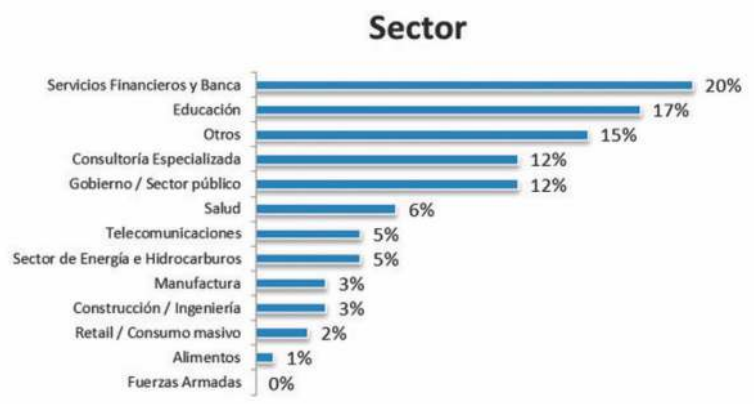
En esta sección están los datos más relevantes de la encuesta, relacionados con la demografía de los participantes y sus relaciones con la seguridad de la información.

Sectores

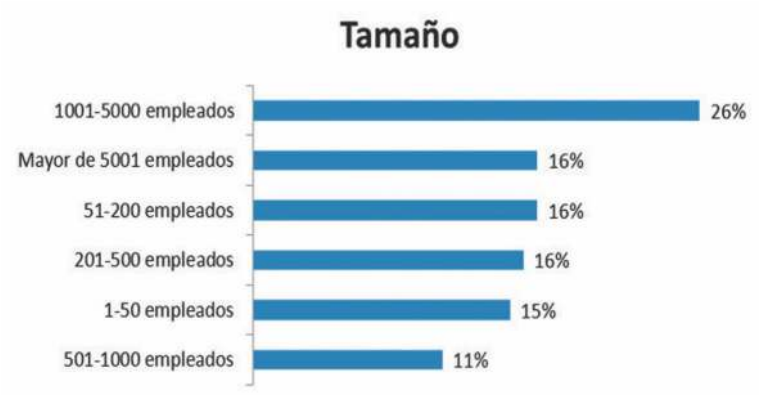
La gráfica 1, muestra la participación de los diferentes sectores de la realidad Colombiana. Se puede observar que la participación del sector financiero y el sector de educación fue la más nutrida; entre los dos suman el 37% de los participantes. El sector de Consultoría Especializada, y Gobierno comparten un nivel similar de participación, con el 12%. Entre otros sectores de la industria vinculados este año están Hotelería y Turismo, Medios de Comunicación y las industrias de entretenimiento. Resulta interesante el aumento en la participación de los distintos sectores, además de la penetración de la seguridad de la información como vector de trabajo para conocer y explorar.

Tamaños

Para este año, la distribución de las empresas es diversa. La mayor participación la tienen las empresas de 1001 a 5000 empleados (26%); le siguen las empresas de más de 5001 empleados (16%); luego las pequeñas empresas entre 51-200 empleados



Gráfica 1. Sectores participantes



Gráfica 2. Tamaños de las empresas

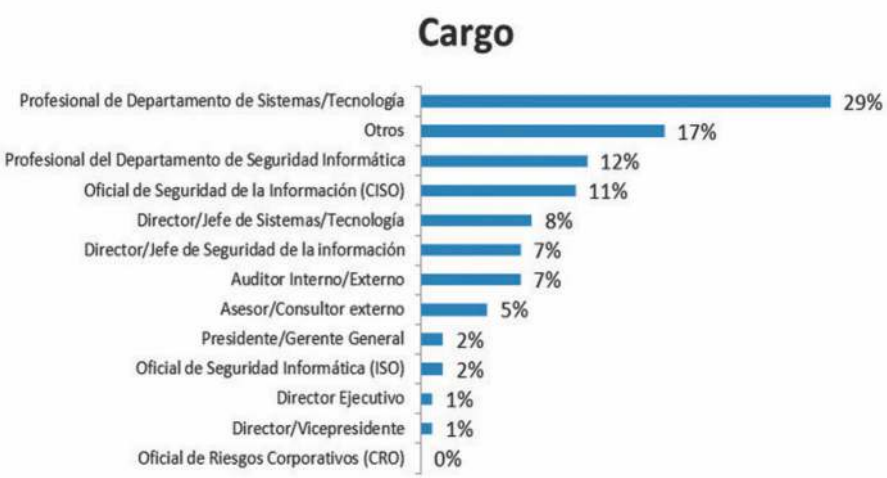
(16%); 201 a 500 empleados (16%); las mypimes de 1 a 50 empleados con un (15%) y, por último, las empresas entre 501-1000 empleados, con un 11%. Se observa que la seguridad de la información se está convirtiendo en una realidad, en medio de un interés por conocer lo que sucede en el contexto organizacional.

Quién responde la encuesta

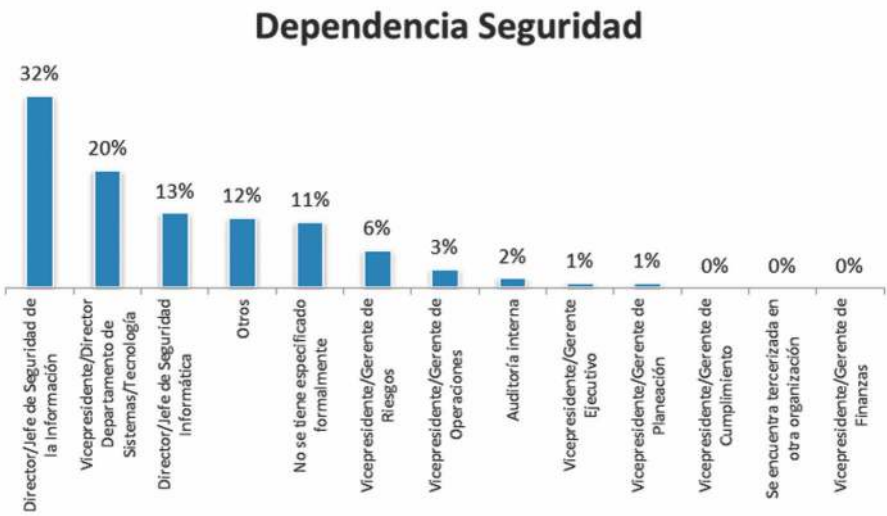
Un 37% de los encuestados pertenece a las áreas de tecnologías de la información con un (29%) y los directores de las mismas un 8%. Un 49% de los encuestados son de áreas de seguridad, a esta cifra se suma un 17% relacionado con cargos adicionales o nominaciones de los encuestados en sus empresas, muchos de ellos en áreas de seguridad y riesgos.

Dependencia de la responsabilidad en seguridad

Esta gráfica 4 refleja que el 43% de los encuestados dice que la dependencia de seguridad tiene área propia comprendida por la dirección de Seguridad de la Información y la de Seguridad Informática, en las que la seguridad de



Gráfica 3. Cargo de los encuestados

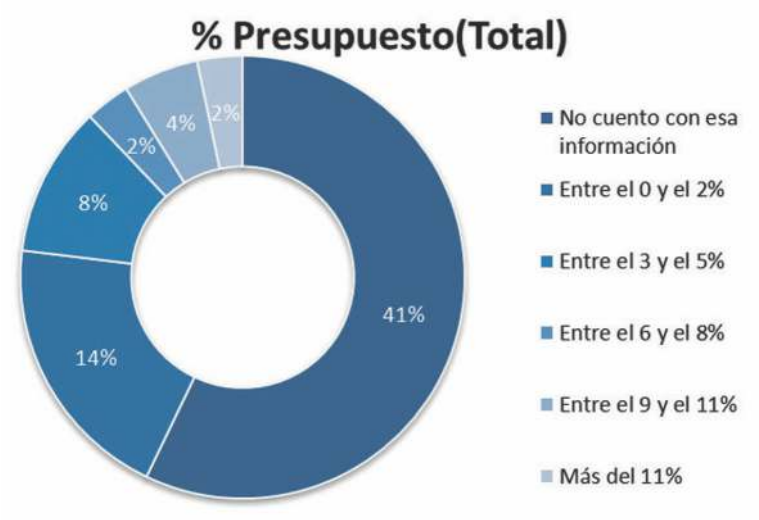


Gráfica 4. Dependencia de la seguridad

la información tiene su arraigo. Resulta interesante ver el cambio en la realidad del país, toda vez que en años anteriores, dichas áreas no reportaban área propia.

Según datos globales, las áreas de seguridad dependen en su mayoría de las áreas de TI. Según el informe de ESET LATAM 2017[1], el 54% de los encuestados dice depender del área de TI. En otro informe relacionado de Berkeley Research Group (BRG) [2], un 32% indica que el CISO le reporta al CIO, pero en el mismo informe resaltan que dichos reportes se vienen dando en áreas por fuera de las TI, con un 32% y el crecimiento sigue aumentando. Y la tendencia es que las áreas de seguridad seguirán encontrando su

Gráfica 5. Roles existentes



Gráfica 6. Distribución global del presupuesto

espacio en las organizaciones e irán aprendiendo la forma para interactuar.

Roles de Seguridad

La gráfica 5, representa los tipos de roles que las empresas colombianas poseen. En primera instancia, existe la tendencia de tener el rol del CISO en las organizaciones; y, sin importar la posición, este rol se consolida con un 49%. Así mismo, el analista de seguridad informática mantiene la segunda posición en la realidad nacional, con un 42%. Y con un 69% figuran las posiciones más técnicas como analistas de seguridad informática y los especialistas en pruebas de intrusión, como roles ya existentes dentro de la organización. Las tendencias internacionales confirman la posición del CISO como una ficha clave dentro de las empresas, así lo muestra el informe presentado por ESG-ISSA [3], en el que un 67% de las organizaciones cuenta con un CISO y, cerca de un 27%, planea incorporarlo en un futuro inmediato. El 53% de las empresas colombianas, dentro del rango de los sectores participantes con más de 500 empleados, manifiesta tener un CISO o un cargo similar, afianzando esta tendencia, con un impacto creciente en los últimos años.

Presupuestos en seguridad de la información

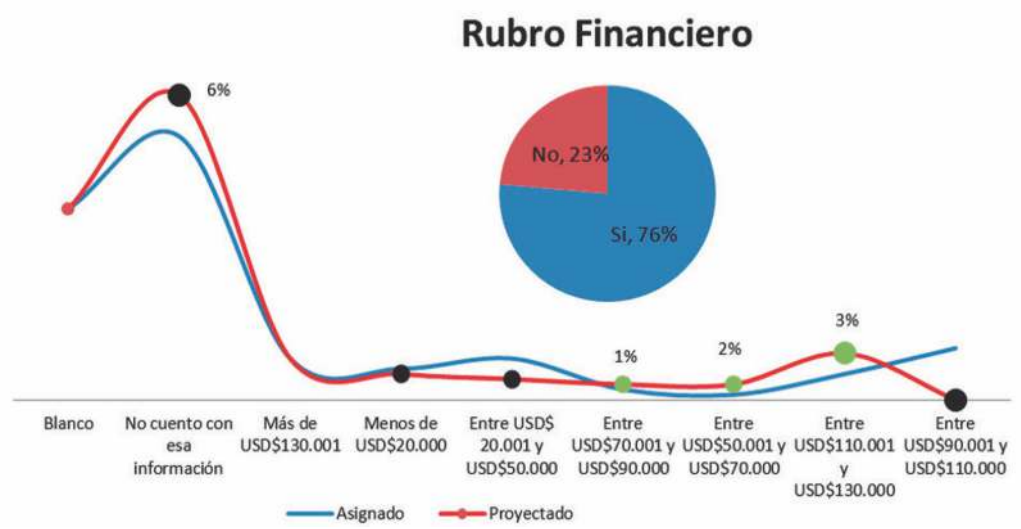
En la gráfica 6 se observa que un 30% de los encuestados manifiesta tener algún tipo de conocimiento relacionado con el presupuesto total de la organización, asignado en sus diferentes proporciones. El mayor valor se refiere a presupuestos, hasta en un 2% del total del presupuesto global de la organización; porcentaje al que le sigue un 8% correspondiente a los valores entre el 3% y 5% del presupuesto global. Y la pregunta también involucra un 23% sin presupuesto asignado para la seguridad de la información. Mientras solamente un 2% dice tener un presupuesto por encima y el 11% señala que las inversiones en seguridad son altas. Cabe anotar que las organizaciones están en un proceso de aprendizaje en los procesos de gestión de las inver-

siones en seguridad y que deben considerar en su interior. Este marco se refleja acorde con las tendencias internacionales en un 53% de la población, dentro del estudio de EY [4], en el que se considera que los presupuestos crecen, pero no son suficientes para enfrentar los nuevos desafíos de la ciberseguridad.

En la gráfica 7 se muestra la asignación de tales presupuestos. En la realidad nacional se comparan lo planeado con lo proyectado y para este año, los datos muestran que un 6% desconoce cuanto se proyecta del presupuesto de seguridad; en este sentido el 46% de los encuestados manifiesta no saber cómo se comportará la proyección del presupuesto. Mientras que el 40% señala no conocer cómo se dimensionó o definió el presupuesto de seguridad. Por otro lado, se observa un incremento de tres puntos en crecimiento en los presupuestos entre $US110 y $US130, lo que indica que sí hay inversiones claras en seguridad; son mínimas, si se compara con la realidad global que muestra un crecimiento de más del 20%, según los informes revisados. Esto puede estar sujeto a la realidad de Colombia y al contexto en el que se desenvuelve. Estudios como el de Deloite-NACSIO [5] muestra que los presupuestos de seguridad se han movido entre 1% y 5%, al revisar su apuesta 2014-2016 y su incremento se ha dado en cerca de un 6%. Hecho que ratifica la constante colombiana.

Incidentes de seguridad

Al revisar el escenario de incidentes en la realidad nacional, gráfica 8, encontramos datos interesantes. El 29% de los encuestados manifiesta no saber si la organización maneja sus incidentes o cómo los maneja. Y el porcentaje significativamente superior, 71%, está relacionado con la presencia de incidentes de seguridad dentro de las organizaciones. El 20% de la misma población manifiesta haber manejado entre 1 y 3 incidentes, y el 17%, más de 7.



Gráfica 7. Rangos de presupuestos

Gráfica 8. Cantidad de Incidentes

Al revisar cuáles son los tipos de incidentes más frecuentes o anomalías digitales atendidas en las organizaciones nacionales, la gráfica 9 muestra en detalle cada una. En primer lugar, un 43% de las respuestas refleja la presencia de Virus/Caballos de Troya como tendencia, frente a las anoma-

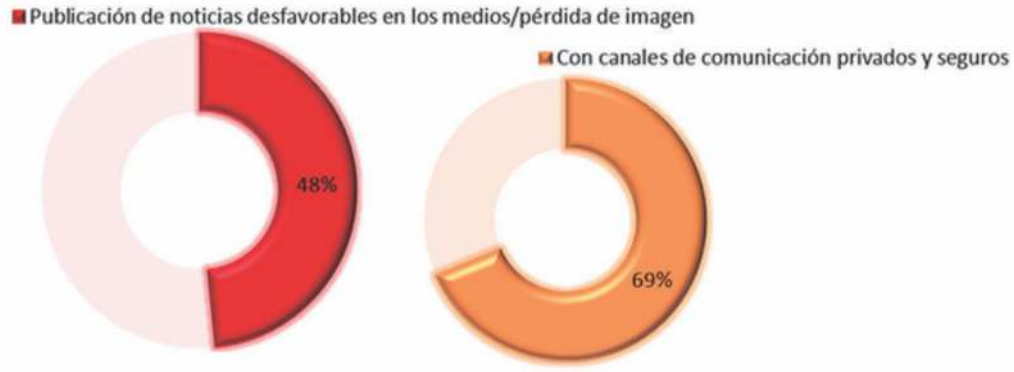
Gráfica 9. Tipos de incidentes

Gráfica 10. Enterado por vs Notificar a

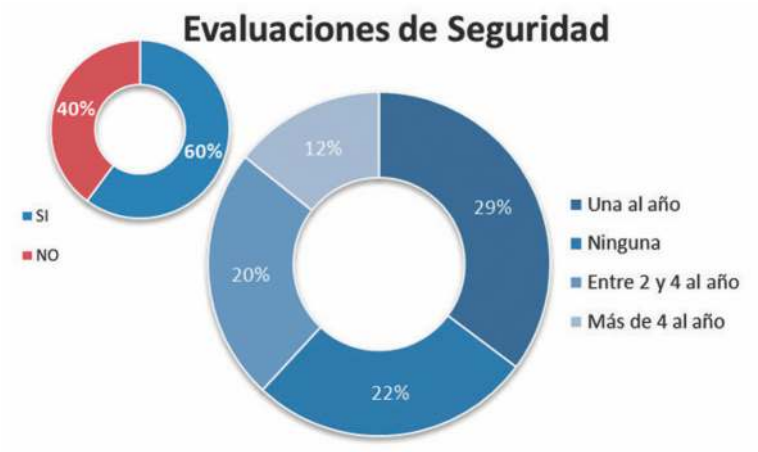
lías digitales. Le siguen el *phishing*, con un 34% y el *ransomware* con 20%, como anomalías en creciente presencia en las organizaciones. Al comparar estos porcentajes con las tendencias internacionales, se ratifica la constante, en un 39% de los encuestados, dentro del estudio de BRG [2]. Así mismo, el informe de ESET LATAM [1], muestra igual tendencia en un 49%.

La gráfica 10 refleja la notificación de las fallas de seguridad y la gráfica 11, a quién se reporta la situación. Según los encuestados, en el 54% de las organizaciones las anomalías son reportadas por sus propios empleados, lo que indica que los programas de sensibilización en seguridad, tienen algún efecto entre las personas. Así mismo, tales incidencias son notificadas a las directivas de la organización en un 57%. Estos porcentajes evidencian también los niveles de cultura, en materia de seguridad de la información en la realidad colombiana.

Un 48% de los encuestados manifiesta no denunciar las fallas por razones de imagen, mientras un 69% lo haría, pero a través de mecanismos de comunicación confiables (privados y seguros). En otras palabras, la disposición a denunciar está directamente ligada con la imagen de la organización. Así mismo, se refleja la confianza, como un factor significativo para crear mayores espacios de cooperación y trabajo común, orientados a estudiar entender y responder de una



Gráfica 11. No se denuncia vs Como hacerlo mejor



Gráfica 12. Evaluaciones de Seguridad

mejor manera los incidentes de seguridad en las empresas colombianas.

Herramientas de seguridad

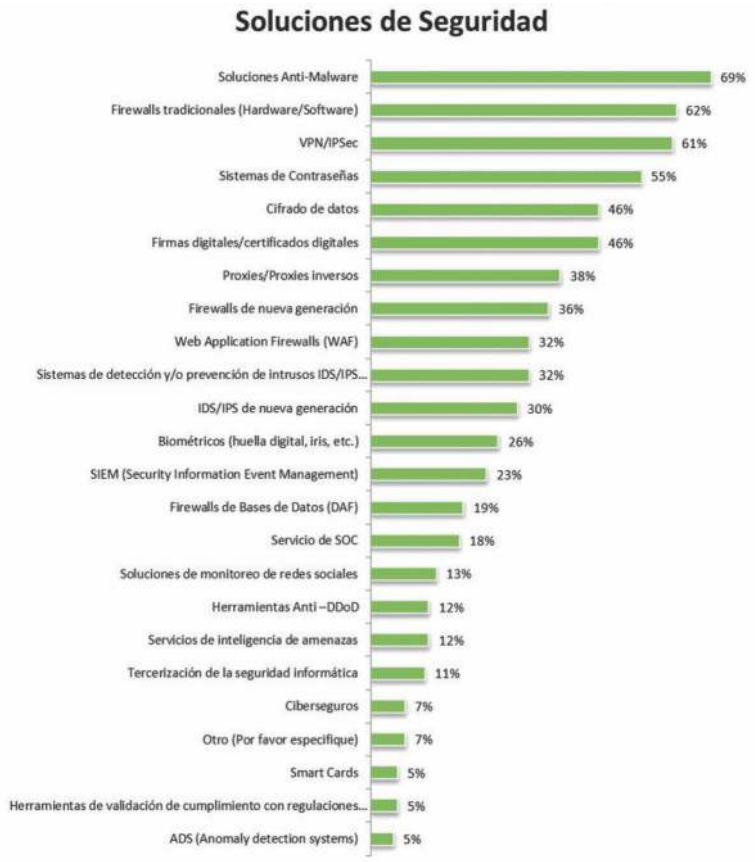
Al revisar qué están haciendo las organizaciones nacionales y cuáles son algunos de los instrumentos más usados como herramientas en torno a la protección de sus ambientes corporativos, la gráfica 12 muestra que el 60% de los encuestados realiza evaluaciones de seguridad en sus empresas, frente a un 40% que no lo considera pertinente o no lo ha contemplado como parte de los procesos en su organización. Mientras el 29% realiza una evaluación anual, como instrumento para revisar los procesos de seguridad.

Como herramientas o instrumentos para proteger información, se revisan los mecanismos tecnológicos y no tecnológicos de las organizaciones. En la gráfica 13 se ven las herramientas tecnológicas para proteger la información, como lo más usado.

Resultados similares son encontrados en informes como ESET LATAM [1], en donde el 83% de las compañías usan *software antimalware* y el 71% usa *firewalls* como segundo mecanismo de control. El informe de seguridad de CISCO [7], en torno a la realidad internacional, muestra que las soluciones *antimalware* son usadas en un 41%, mientras que los *firewalls* se utilizan en un 58%. Se observa una disminución en cuanto al uso. Este mismo informe está centrado en que las organizaciones han recurrido a la tercerización en este tipo de tecnologías y en cómo los mecanismos de seguridad de la nube han cobrado fuerza, a la hora de implementarlos en las organizaciones.

Políticas de seguridad

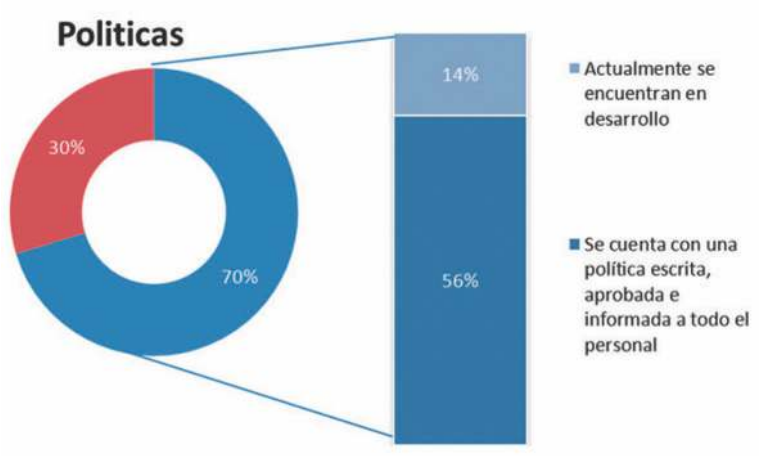
Muchas organizaciones ven en las políticas de seguridad un respaldo situacional frente a la seguridad de la información. La realidad nacional reflejada en la gráfica 14, señala que el 70% de los encuestados manifiesta que sí existe en su organización una política, frente a un 30% que dice no tener nada en su empresa. De esa población, un 56% advierte que la política está dispuesta de manera oficial en su organización. Estos resultados son intere-



Gráfica 13. Mecanismos de seguridad

santes, toda vez que el compararlos con el informe del Reino Unido [5], de 2016, sólo el 29% de toda la población tiene una política formalmente documentada. En la región, según el informe de ESET LATAM [1], el 74% usa como práctica de gestión las políticas y las tiene implementadas en las organizaciones. Por su parte, el informe de CISCO [7] indica que el 55% de las organizaciones tiene una política formal, de acuerdo con lo establecido en normas internacionales. Y las organizaciones colombianas entienden la necesidad de implementar un modelo de políticas de seguridad, además de su aporte en la construcción de un *framework* de seguridad organizacional.

Al revisar cuál es el *framework* de seguridad más usado en las organizaciones colombianas, la gráfica 15, indica que ISO/IEC 27001, es la referencia más usada, con un 57%, porcentaje que coincide con lo manifestado en el informe de CISCO [7], en el cual el 55% de las organizaciones usa como *framework* para definir sus políticas el estándar ISO/IEC 27001. Otros estándares usados son: ITIL, 35%, COBIT 5, 24% y las guías del NIST, 20%. Así mismo, el 46% de los encuestados manifiesta que las regulaciones nacionales también los llevan a usar un *framework* de seguridad dentro de las organizaciones.



Gráfica 14. Política de Seguridad

En términos de riesgos las empresas colombianas tienen una realidad interesante, como se observa en la gráfica 16. Al indagar si realizan evaluaciones de riesgos en materia de seguridad de la información, el 49% responde que sí y el 32% no. Sobre quienes las realizan, los resultados muestran que la frecuencia con que lo hacen está asociada con una valoración de riesgos de seguridad en un 22% y en torno al modelo para realizar dicho ejercicio, la tendencia es ISO/IEC 31000, con un 28% como principal modelo a seguir para el levantamiento de los riesgos. Y, sobre los riesgos identificados, el 51% de los encuestados manifiesta que son valorados como riesgos operacionales propios de la dinámica de las organizaciones. Las encuestas internacionales [5] ratifican la tendencia de realizar los procesos de riesgos de la seguridad y ciberseguridad (80%), como un instrumento de apoyo a la hora de enfrentar los desafíos de la realidad digitalmente modificada en la que se encuentran las organizaciones.

Implementar seguridad en las organizaciones siempre implica desafíos y

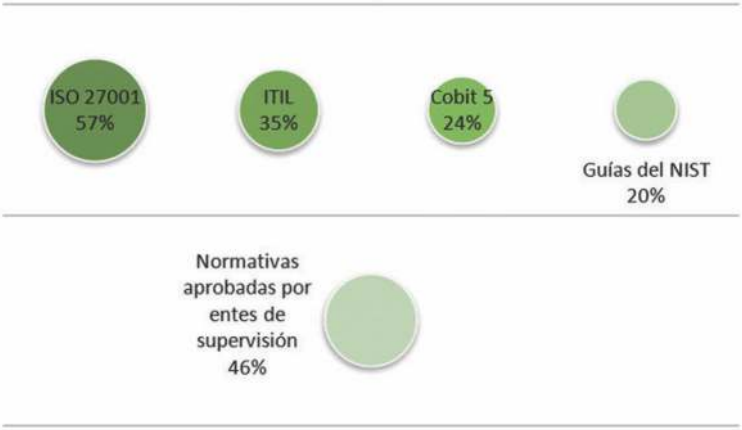
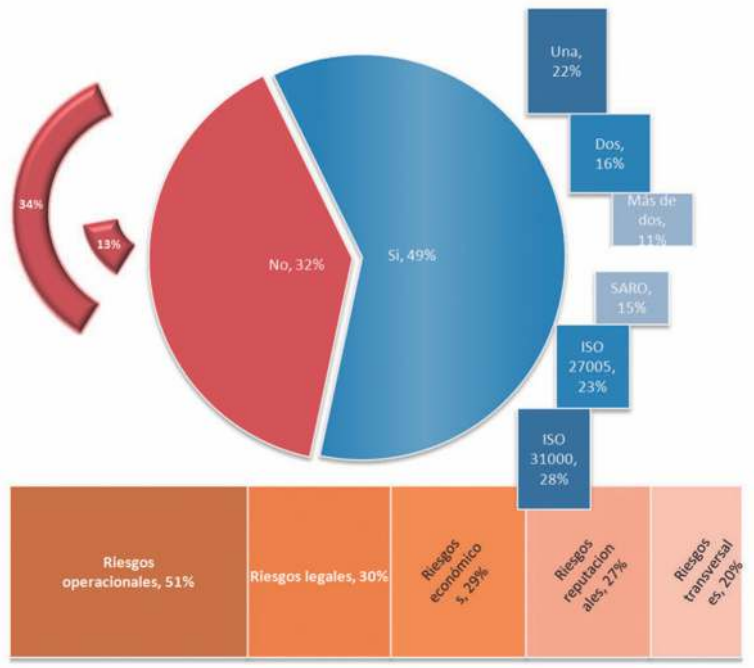


Gráfico 15. Frameworks de Seguridad vs Regulaciones



Gráfica 16. Gestión de Riesgos

retos que deben ser sorteados por el líder de seguridad de la información. Al indagar, gráfica 17, sobre cuáles son los obstáculos para una implementación de la seguridad en las organizaciones en la realidad nacional, un 61% de los encuestados manifiesta que la ausencia de cultura es uno de los mayores obstáculos a la hora de poder implementar la seguridad. A nivel internacional, el informe de CISCO [7], manifiesta que el principal motivo está relacionado con la disminución de presupuestos (35%); la ausencia de personal entrenado (25%), mientras que en Colombia solo el 14% considera que no hay recurso entrenado en materia de seguridad. El estudio de seguridad realizado por la firma Servicenow [6] señala que el 30% de los encuestados considera la ausencia de recursos, tanto en talento humano, como en tecnología, como uno de los factores claves para una adecuada implementación de la seguridad en las organizaciones. Aunque en Colombia no es considerado el principal motivo, sí coincide con las tendencias internacionales.

Capital intelectual

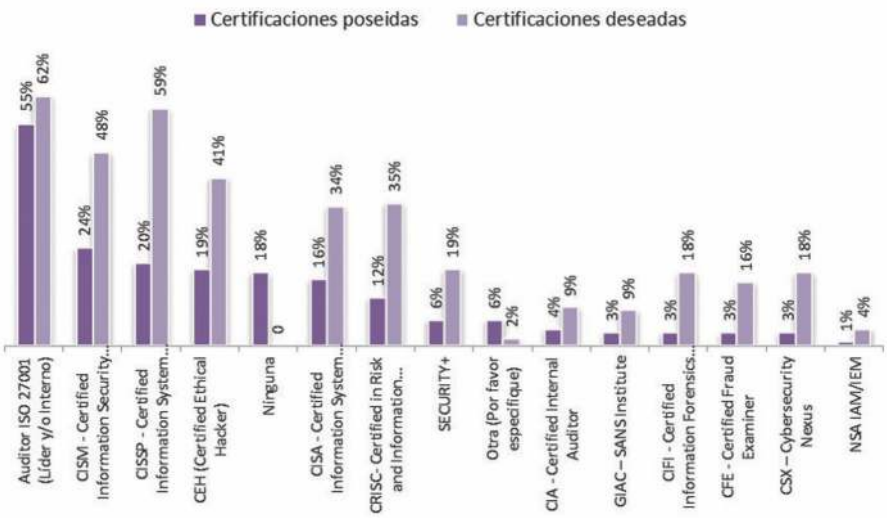
En seguridad de la información el talento humano es un recurso en demanda en las organizaciones y existe un déficit en su consecución. Así se observa en una de las conclusiones del informe de ESG-ISSA y Servicenow [3] [6]. La gráfica 18, muestra que en Colombia las áreas de seguridad están formadas principalmente por grupos de 1 a 5 personas, en un 45%; por otro lado, la experiencia mínima requerida para el talento de seguridad está especificada en dos años, como mínimo, con 51%. Según el informe de CISCO [7], el 15% de las personas contratan entre 1 y 9 recursos para la seguridad.

Gráfica 17. Obstáculos a la seguridad

En la misma medida se valoran las certificaciones (gráfica 19); las tendencias internacionales plantean un gran debate al respecto (ESG-ISSA [3]). Por una parte se ve cómo las certificaciones son importantes y el debate se centra en cuál de ellas es la más adecuada para mejorar las habilidades, conocimientos y uso de los recursos de seguridad. En Colombia las tres certificaciones más usadas, en su orden, son: Auditor Líder 27001, CISM y CISSP, CEH; y entre las más deseadas están loAuditor Líder 27001, CISSP, CISM y CEH, respectivamente. Esto confirma la tendencia internacional. Los datos internacionales y nacionales sugieren que la mejoría de habilidades se obtiene, en primer lugar, con la experiencia, y luego con las certificaciones de seguridad. En las tendencias internacionales es CISSP la certificación más valorada (56%), CompTIA (19%), CISM (17%) y CEH con un 12%. Así mismo, se ratifica la tendencia de ver a CISSP como la certificación que más aportes le puede hacer a los profesionales de la seguridad, a la hora de obtener un trabajo, seguido del mejoramiento de las habilidades del profesional.

En esta misma medida, la encuesta evalúa el papel de la academia, gráfica

Gráfica 18. Recursos y experiencia

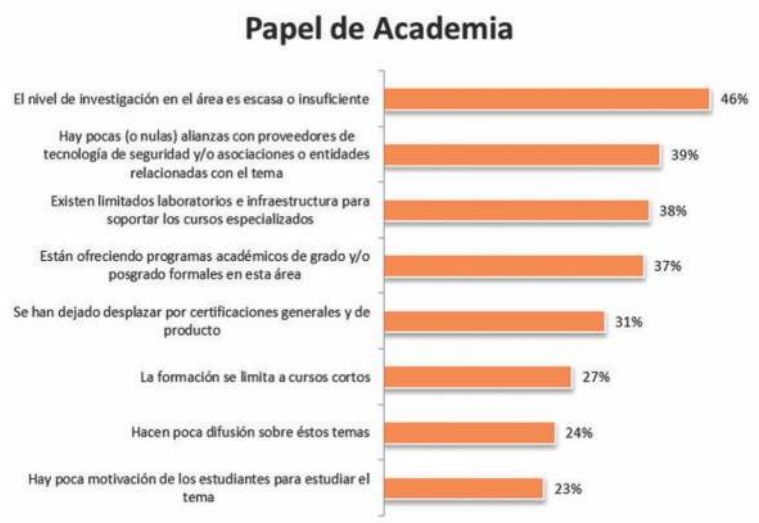


Gráfica 19. Certificaciones obtenidas vs deseadas

20, en la creación y formación de nuevos talentos en materia de seguridad y los resultados este año muestran tres puntos claves. No se está generando suficiente investigación en materia de seguridad en las universidades (46%); no hay alianzas entre la academia y los sectores de la industria (39%); y, si bien existe oferta de formación en materia de seguridad, sus laboratorios e infraestructuras son limitados a la hora de llevar a cabo dichos programas de formación (38%).

Los CISO

Esta sección busca saber qué ven los CISO o directores de seguridad de la información (Chief Information Security Officer) y cuáles son sus relaciones con la organización; así mismo, cuáles consideran ser los temas más relevan-



Gráfica 20. Papel de la Academia

Gráfica 21. Temas relevantes de un CISO

tes a tener en cuenta; qué creen que les falta por aprender y qué están entregando como información a las organizaciones.

En la gráfica 21, la pregunta sobre los temas más relevantes en materia de seguridad muestra que en la realidad colombiana, para el 60% de los responsables de seguridad, el desafío son las amenazas persistentes avanzadas, frente a las cuales deben estar muy preparados para enfrentarlas. Las tendencias internacionales ratifican la seguridad en la nube ESG-ISSA [3], BRG [2]. Estos temas figuran en la agenda del CISO, toda vez que replantear los modelos de controles fuera de la organización, implica encontrar equilibrio y balance en la ecuación de la protección, de manera de generar una confianza óptima para los servicios, los clientes y las operaciones de la organización. Por otro lado, EY [4], ratifica otro de los temas de las agendas de los CISO. Si bien en la realidad nacional no figura en las posiciones más críticas, sí aparecen su agenda. Internet de las cosas es una realidad que no se puede desconocer. Así mismo, *Big Data* y la analítica se encuentran como uno de los temas sobre la mesa de los CISO, particularmente, a la hora de utilizar todas las fuentes de información de anomalías, en procura de maximizar sus esfuerzos sistémicos por lograr una anticipación cada vez más confiable en la protección digital de las organizaciones.

La relación de la seguridad de la información con sus organizaciones pasa por toda la empresa, principalmente por sus dirigentes. En ese sentido, la encuesta evalúa cómo entienden los responsables de la seguridad la conciencia en materia de seguridad. La gráfica 22 muestra un panorama interesante para la realidad nacional. Encontramos que las altas direcciones tienen en cuenta la seguridad y atienden las recomendaciones de sus especialistas (21%).

En tal sentido, existe algo de conciencia y dentro de las organizaciones

entienden los riesgos en materia de seguridad. Esto no garantiza que ellos tomen una decisión y por tanto se pueden dar márgenes a exposición de riesgos. El ejercicio relacionado con lo que deben saber las altas direcciones en materia de seguridad de la información, está relacionado con la cantidad de información que estos reciben y la calidad de la misma. Por otro lado, vemos el extremo contrario como el segundo punto relevante de los hallazgos; el 21% manifiesta que tienen niveles directivos que poco o nada se involucran en la seguridad y la toma de decisiones frente a los riesgos. Esto invita a la reflexión de ¿cómo poder plantear la venta de la seguridad en las organizaciones?, ¿qué está haciendo el CISO para concienciar a sus directivos?, ¿cuáles podrían ser los puntos de encuentro entre el CISO y las juntas directivas? Las tendencias y reportes consultados en su totalidad muestran que la protección de la información ha venido siendo parte de las agendas de los consejos de dirección (Board) y de los niveles directivos de las entidades. Particularmente, esta afirmación se ve en el informe de BRG [2], en el que el 55% de los informes de un CISO llega a nivel directivo para participar activamente en las tomas de decisiones frente a la seguridad.

¿Qué es lo que puede mejorar un CISO? Es una de las preguntas que recurrentemente se encuentra en noticias y medios digitales, en la búsqueda de una respuesta clara para que su mensaje y la percepción que de ellos se tiene, puedan evolucionar. La gráfica 23 muestra la realidad nacional en términos de las brechas que pueden ser las oportunidades de mejora de los CISO; al respecto, el 58% ratifica la tendencia mundial: habilidades gerenciales; particularmente, la habilidad de comunicar el mensaje más allá de una simple vista del control. Le sigue interconectar negocios con oportunidades para mejorar los procesos, a través de los controles, como segundo elemento con un 41%. Los CISO deben cerrar, interconectar y balancear las necesidades de protección con las la forma de hacer más confiables los negocios en la vida digital. Esto lo ratifica el informe de ESG-ISSA [3], en el que se indica que la habilidad más valorada para el éxito de un CISO es la comunicación (47%); por encima está el lide-

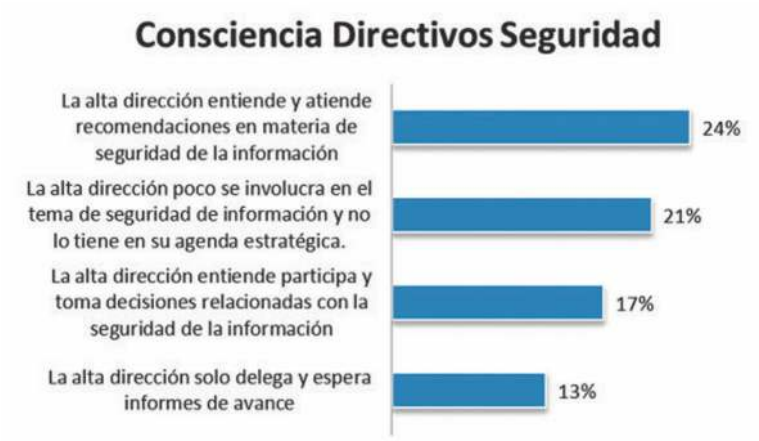


Gráfico 22. Consciencia de los Directivos

Gráfica 23. Oportunidades de mejora de un CISO

razgo (50%), nueva habilidad que debe ser involucrada en el portafolio de los CISO y su aplicabilidad en las organizaciones.

Este año, también se incluye el análisis de lo que entrega el CISO, versus la percepción que se tiene de ellos en las organizaciones. En la gráfica 24 se observa una relación de los dos elementos evaluados. Por un lado, los encuestados señalan la información técnica de la seguridad (38%), seguida de la información asociada a la gestión de la seguridad, con un 34%. En la otra parte de la gráfica 24 (percepción) vemos un 22% que percibe al CISO como un asesor; pero, al compararlo con las posiciones siguientes -implementador 20% y supervisor 19%-, aparece reflejado un asesor de nivel técnico en la supervisión e implantación de controles dentro de la gestión propia de la seguridad.

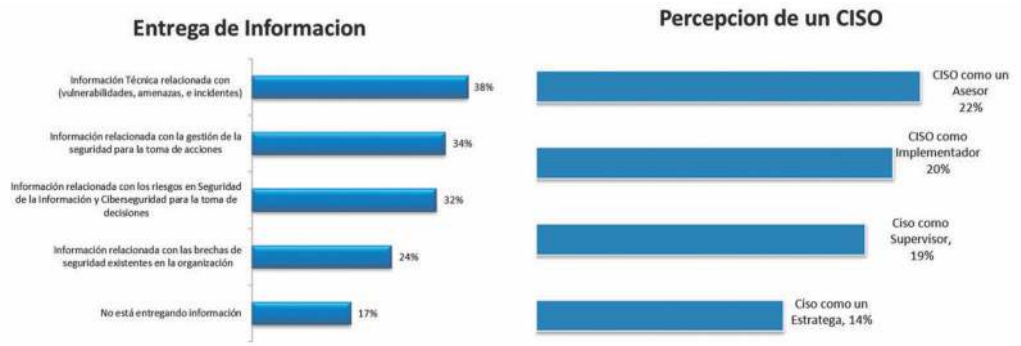
Conclusiones generales

Cada vez más, las organizaciones se enfrentan a una realidad digitalmente modificada, donde las nuevas tecnologías permean cada uno de los ambientes organizacionales y personales.

La creciente expansión digital genera nuevos riesgos y necesidades de protección, hecho que invita a la reflexión en aras de proteger la información en un mercado más competido y exigente.

En el entorno de la cuarta revolución industrial, los ejecutivos de seguridad se enfrentan a unos escenarios cambiantes y dinámicos que demandan reacciones rápidas, que contemplan la anticipación y la conciencia para proteger la información.

Año tras año, la encuesta ha venido mostrando la protección de la información como un elemento clave a la hora de enfrentar los retos en la realidad colombiana. No obstante, son necesarios pensamientos amplios que involucren a los actores y los lleven a hacer un replanteamiento de la protección de la información, sin perder de vista lo ya alcanzado, para enfrentar la realidad en el contexto actual.



Gráfica 24. Imagen vs Percepción de un CISO

En el marco de la cuarta revolución industrial, con ambientes cada vez más volátiles, inciertos, complejos y ambiguos, es necesario que los responsables de la seguridad de la información en las organizaciones tengan una atención plena y consciente, frente a los nuevos desafíos.

Dentro de la realidad nacional son varios los aspectos para destacar:

No distamos de la realidad internacional en términos de los ejercicios en la búsqueda de la protección de la información.

Se afianza la posición del CISO; de asesor técnico se espera que se convierta en un asesor que provee información estratégica para la toma de decisiones. En tal sentido, es de esperar que su comunicación mejore, se perfeccione y se fortalezcan las relaciones con los directivos de las organizaciones.

Se mantiene una sólida tendencia a usar mecanismos tecnológicos como las principales herramientas de protección. Así mismo, se abre el camino para ver más allá de las infraestructuras tecnológicas; es decir, ver en la protección una oportunidad para construir nuevos estándares alrededor de una cultura organizacional.

Se entiende en mayor proporción el poder de las anomalías digitales y de los adversarios digitales alrededor de las organizaciones colombianas. Se amplía la conciencia de que la seguridad requiere educación dentro de las organizaciones, en la búsqueda de la resiliencia digital.

Las nuevas tecnologías como *Big-Data*, *Cloud*, I*oT*, *IA* y *Machine Learning*, entre otras, están cambiando la concepción sobre cómo se ve el mundo, cómo se interactúa y se ponen en práctica mecanismos de protección.

A pesar de que en las organizaciones se observan mayores esfuerzos por implementar modelos de seguridad, las regulaciones ejercen una gran influencia a la hora de hacerlo, dejando de lado la intención de proteger o la responsabilidad por cumplir.

Las discusiones internacionales y nacionales generan el debate entre cumplimiento y seguridad. La seguridad usa el primero como un “disparador”, pero la meta de protección organizacional como valor sostenido, no está sujeta al mismo.

Referencias

[1] Eset Security Report Latinoamérica 2017. Consultado en mayo de 2017. https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

[2] Cybersecurity preparedness benchmarking study. Consultado en mayo de 2017. http://www.thinkbrg.com/newsroom-publications-cybersecurity-preparedness-benchmarking-study-report.html

[3] The State of Cyber Security Professional Careers (Part I and Part II). Consultado en mayor de 2017. http://www.esg-global.com/esg-issa-research-report

[4] Path to cyber resilience: Sense, resist, react. EY's 19th Global Information Security Survey 2016-17. Consultado en mayo de 2017. http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf

[5] 2016 Deloitte-NASCIO Cybersecurity Study. Consultado en mayo de 2017. https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress

[6] The Global CISO Study. Consultado en mayo de 2017. https://www.oxfordeconomics.com/recent-releases/the-global-ciso-study

[7] Cisco 2017 Annual Cybersecurity. Consultado en mayo 2017. http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017

[8] 2017 Data Breach Investigations Report. Consultado en mayo de 2017. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[9] Cyber Security Breaches Survey 2017. Consultado en mayo de 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Andrés Ricardo Almanza Junco, M.Sc. CISM, ITIL, ISO 27001, LPIC1.
Ingeniero de Sistemas, universidad Católica de Colombia. Especialista en Seguridad de Redes de la Universidad Católica de Colombia. Máster en Seguridad Informática de la Universidad Oberta de Cataluña, España. Líder facilitador profesional en Coaching de la ICL (International Coaching Leadership) and Future Achievement Internacional. Codirector de las Jornadas Internacionales de Seguridad Informática y Coordinador de las comunidades virtuales CISO's-COL y CISO's-LATAM y Segurinfo en Linkedin.

Seguridad y control ¿son viables?

La llamada cuarta revolución industrial trae 'bajo el brazo' tantos cambios, que el ser humano será otro, en su cotidianidad, en sus relaciones y hasta en su interior. Por supuesto, su entorno también será distinto y en ese ambiente que lo rodea la seguridad es protagonista. Asuntos que enmarcaron el Cara y Sello de esta edición.

Sara Gallardo M.

El salto de la máquina de vapor a los robots integrados en sistemas ciberfísicos, capaces de interactuar con seres humanos, es incalculable. Tales desarrollos tecnológicos han dado lugar a lo que los economistas optaron por definir como cuarta revolución industrial, un momento de la humanidad que quedará grabado en la historia universal, con un sello único.

Ese hecho sin precedentes, basado en Internet de las Cosas, impresión 3D, inteligencia artificial y nanotecnología producirá un hombre distinto, en un entorno también transformado por estas y otras tecnologías de la información y las comunicaciones (TIC). Y la seguridad, en todas sus acepciones, juega un papel muy importante.

En la mirada a ese panorama, hay de todo. Muchos pronostican beneficios para la sociedad y las economías, mientras otros más escépticos, lo contemplan con sigilo. “La hiper-conec-

tividad y las redes sociales nos están dividiendo en vez de unirnos. Existe más presión por actuar rápido, por lo que la democracia representativa se debilita y la toma de decisiones es cortoplacista. El 2016 nos mostró que las personas confunden opiniones con hechos, y rápidamente aceptan evidencia que confirma nociones preconcebidas o convicciones prejuiciosas", en opinión de Javier Arreola[1].

Este y otros asuntos como riesgos, amenazas, cambios en los estándares, prácticas de seguridad y control, cambios normativos sobre el tratamiento de la información, empresas con infraestructura crítica, el analista de seguridad, habilidades, competencias y conocimientos de los nuevos profesionales y la preparación de la Academia, fueron programados para el debate al que asistieron: María Del Pilar Sáenz Rodríguez, coordinadora de Proyectos de la Fundación Karisma; Jaime Eduardo Santos Mera, vicepresidente Legal de Gobierno Mercantil, de Colpatria S.A.; Juan Mario Posada Daza, gerente de Asesoría y Líder de servicios de Ciberseguridad en EY (antes Ernst & Young); Marcela García Caballero, head PR y Spokersperson de Rappi; Andrés Aguilera Castillo, profesor asociado, investigador de la Universidad EAN y Mauricio Guerrero Cabarcas, profesor asociado, investigador de la Universidad EAN.

"De cara al mundo digitalmente modificado -tal y como lo define en forma muy acertada el profesor Michael Porter-, los temas de seguridad adquieren una dimensión muy distinta y dirigen el pensamiento hacia nuevos horizontes que nos van a sorprender. De ahí que muchas consultoras adviertan sobre los 18 billones de dispositivos conectados que existirán en el futuro próximo y los riesgos a los que están expuestas todas las industrias", fue el preámbulo del director de la revista y

1 Javier Arreola, Executive, Investment Banking, GF Inbursa. *5 inquietudes que dejó el Foro de Davos*. 10 Febrero 2017. https://www.weforum.org/es/agenda/2017/02/5-inquietudes-que-dejo-el-foro-de-davos. Recuperado Junio 5 de 2017.


Pilar Sáenz


Marcela García


Jaime Eduardo Santos


Juan Mario Posada


Andrés Aguilera


Mauricio Guerrero

editor técnico en esta edición, Jeimy J. Cano M., quien, dio inicio al debate con la primera pregunta:

¿Cuáles son los nuevos riesgos y amenazas que pueden surgir como consecuencia de la cuarta revolución industrial?

Marcela García C.
Head PR y Spokersperson
Rappi
Que la seguridad vaya más despacio que la misma revolución, es decir, que no alcancemos a llevarle el ritmo y que, por ende, se abran unas brechas importantes y bastante delicadas que promuevan los ataques que estamos viendo hoy en día. Las interrupciones en la operación, que amenazan la continuidad de los negocios, los accidentes provocados por una amenaza cibernética, el acceso a este tipo de operaciones por amenaza humana, las características del mercado laboral, la automatización de las cosas y el descontento generalizado de carácter social, son algunos de los riesgos a los que se expone el mundo ante esta nueva consecuencia de la cuarta revolución industrial.

María Del Pilar Sáenz R.
Coordinadora de Proyectos
Fundación Karisma
Lo primero es hablar del rol de la sociedad civil, la cual está llamada a prender algunas alertas ligadas al tema de seguridad; particularmente, a los temas asociados con la privacidad, pero no son las únicas. Una de las cosas que hemos estado viendo de forma preocupante es que, en la primera política pública que hubo en Colombia sobre temas sobre ciberseguridad -el Conpes de 2011-, se perdió por completo la oportunidad de que la sociedad civil participara en forma activa en su elaboración; en 2016, para el nuevo Conpes de seguridad digital, sí nos invitaron. Lastimosamente, aun cuando en el nuevo Conpes se advierte que la sociedad civil es importante, que la seguridad digital tiene que ver muchísimo con el análisis de riesgos, que todos somos parte de las soluciones y

de los problemas que hay responsabilidad compartida, en el programa y el desglose del programa, se nombra el marco de derechos humanos, pero no se desarrolla. Entonces desde el punto de vista de sociedad civil, hace falta un montón de controles, primero para algunas de las instituciones que tienen en sus funciones seguridad, privacidad, defensa, inteligencia y demás. También adolecemos de datos; a diferencia de muchas de las partes que están en este debate, que saben cuántos son los afectados en empresas o en bancos por el último ataque, yo no puedo saber. Si vamos a ver cuántas personas fueron afectadas, ni idea; cuántos medios de comunicación, periodistas, cuántas universidades, otro tipo de información, no existe. Y pareciera que no hay nadie que esté encargado de recogerla. Entonces para mí eso es un riesgo y una amenaza y claramente la idea es poderlo debatir también.

Mauricio Guerrero C.
Profesor asociado, investigador
Universidad EAN

Hay tres puntos que me parecen importantes en términos de riesgos. El primero es cómo la diplomacia empieza a convertirse en un tema de diplomacia digital y cómo gracias a que muchas veces se borra la diferencia entre lo que hacen los países y lo que hacen *hackers* rusos o *hackers* de otros países. Esta diplomacia va a comenzar a tener unas implicaciones y unos riesgos en términos de seguridad del sistema internacional. El segundo punto, es cómo esto también va a llevar a que algunos países, si no siguen el ritmo o no implementan sistemas de ciberseguridad en sus fronteras, van a ser Estados en los cuales no solamente va a haber fallas físicas, sino fallas de seguridad. Y se van a convertir en sitios seguros para mafias internacionales o para potenciales personas que vayan a atentar contra la seguridad física, desde la seguridad virtual. Un tercer punto, que me parece un riesgo esencial, no solo en Colombia, sino a nivel mundial, es qué vamos a hacer con la educación. Cómo vamos a formar a esos 18 o 20 millones de personas que vamos a tener de brecha entre lo que requiere el mercado y lo que se está generando, no sólo en las carreras de ingeniería y otras disciplinas, sino en términos legales y económicos; cómo vamos a responder a esa masa crítica que necesitan las sociedades para poder enfrentar este reto de la ciberseguridad a mediano y largo plazo.

Andrés Aguilera C.
Profesor asociado, investigador
Universidad EAN

Frente a los nuevos riesgos de amenazas, me gustaría hablar de Internet de las cosas. El hecho de tener más dispositivos conectados, implica nuevos vectores de riesgo. Me parece oportuno recordar lo sucedido en octubre de 2016, cuando ocurrió un *Distributed Denial of Service Attack* (DDoS), a la empresa norteamericana Dyn. Este ataque fue bastante interesante, porque el método que utilizaron fue a través de la manipulación de cámaras conectadas a internet que habían sido fabricadas en Taiwan; este evento puede ser catalogado como uno de los mayores *DDoS* en los últimos 12 meses. A medida que agregamos más dispositivos, estos se convierten en nuevas avenidas o formas de atacar a los ciudadanos, a las corporaciones y al sector público, entre otros. Evidentemente, esa proliferación de dispositivos electrónicos es

una gran oportunidad de negocios, pero al mismo tiempo tales dispositivos conectados, nos pueden poner en riesgo a todos, tal y como se evidenció en el ejemplo del ataque mencionado.

Hay otro riesgo que hemos detectado desde la academia y lo hemos identificado como el *insider threat*. En algunas ocasiones hemos visto cómo los empleados de una corporación voluntariamente deciden vulnerar sus sistemas de seguridad y es muy poco lo que las compañías hacen para mitigar este riesgo, al menos en Colombia. Cuando hablamos de corporaciones grandes, esas buenas prácticas internacionales se empiezan a establecer acá. Pero, la mayoría de empresas medianas y pequeñas no tienen esa cultura de ciberseguridad.

Y otro aspecto es el cambio generacional que está ocurriendo con la fuerza laboral. En los próximos años la mayoría de la fuerza laboral va a ser ocupada por *millennials*, una generación que nació y creció con dispositivos electrónicos disponibles, pero lamentablemente, no tienen la suficiente conciencia para manejar la seguridad informática. Ellos que, son la mayoría de nuestros estudiantes de la universidad EAN, tienen dispositivos para todo, teléfonos inteligentes, televisores súper avanzados, están en todas las redes sociales posibles, pero son una generación descuidada en términos de seguridad. Son muy pocos quienes son conscientes de los riesgos a los que están expuestos a través de toda esta multiplicidad de aparatos y plataformas.

Juan Mario Posada D.
Gerente de Asesoría
EY (antes Ernst & Young)

Debido al escalamiento de la guerra cibernética que estamos viviendo se requiere un cambio cultural profundo. Los profesionales en temas de ciberseguridad, desde hace muchos años venimos advirtiendo la posibilidad que hoy se ha hecho una realidad. Hace mucho dejamos de enfrentar a jóvenes *hackers* más motivados por un reto, por un desafío académico y de habilidades, que por el dinero o el deseo de hacer daño. Ahora es evidente que nos enfrentamos a organizaciones dedicadas de lleno al cibercrimen, más sofisticadas, peligrosas y con autonomía financiera.

Teniendo claro este contexto, resulta importante mencionar que esta transformación digital empieza a tocar el corazón de los negocios. Estábamos acostumbrados a hablar, por ejemplo, de tecnologías de información asociadas a procesos de soporte; los sistemas que utilizamos cotidianamente como el correo electrónico, el sistema de información financiera, el sistema que gestiona la nómina, entre otros; hoy vemos cómo los riesgos de seguridad se materializan en el mundo de las tecnologías de operaciones (PLCs, SCADA, DCS, etc.).

Esta situación nos ha llevado a una convergencia entre dos mundos soportados por herramientas tecnológicas, pero con prioridades muy diferentes. El mundo de tecnologías de operaciones toca el corazón de los negocios, de las empresas y sus líneas de producción (gas, energía, petróleo, productos de consumo) y, en algunos casos, incluso la seguridad digital de las naciones, como sucedió en Ucrania en el 2016, interrupciones del suministro energético a causa de un ciberataque. Los ciberataques ya no se

quedan simplemente en el secuestro de información, sino que pueden causar desastres ambientales, pérdidas humanas, destrucción de equipos e instalaciones de alto costo en cualquier sector de la economía, lo cual conlleva altos costos de reparación, pues evidentemente reparar un computador portátil no se compara con reparar una planta energética y, tal vez lo más importante, el daño que se le causa a la reputación de las empresas afectadas, pues recuperar la confianza de la sociedad es tal vez lo más difícil de lograr después de un ciberataque.

Jaime Eduardo Santos M.
Vicepresidente legal de Gobierno Mercantil Colpatria
Colpatria S.A.
Desde del mundo del gobierno corporativo tengo una visión holística adicional. Si estamos viviendo la tercera guerra mundial, la ciberguerra es parte de ella. Si uno hace una suma de variables en este momento, encontramos situaciones como la de Siria, en la cual hay al menos 14 países que viajan a bombardear. En las guerras anteriores, se decía que si cinco países entraban en conflicto en dos continentes, teníamos una guerra mundial. Ahora eso está excedido en extremo, esa es una primera variable que me llama la atención. En Siria se usan drones *big data* y también armas biológicas, y eso tiene que ver con la cuarta revolución industrial: nanotecnologia biotecnología, información y cognición.

La segunda variable son las migraciones o desplazamientos como los llamamos en Colombia, las cuales son mayores que en toda la historia de la humanidad. Tenemos migraciones del África empujando duro a Europa Mediterránea y de Europa Mediterránea hacia arriba; encontramos un mesero español en Finlandia. Otra variable que me llama la atención es el crecimiento económico mundial, propio de la recesión de guerra. Esos crecimientos que tuvimos de 4, 5 en Perú o los de China de 8, no se van a volver a

ver en años, según dicen los economistas. Y eso implica otra variable propia de las guerras, el estancamiento o la recesión. Así mismo, los líderes globales que tenemos. En Colombia, con un problema tan serio de liderazgo, lo que estoy sintiendo es que estamos en las mismas que los líderes en resto del mundo. Entonces en conversaciones con mi hijo, le digo, no es que en Colombia hayamos mejorado, es que los demás han empeorado significativamente. Y todo eso me lleva a pensar que estamos viviendo una revolución social. Además, la brecha entre ricos y pobres también es enorme y viene indignando a muchos.

De manera que si uno hace esa combinación de variables o esa mirada sistémica obtiene un marco de actuación muy propicio para que en la cuarta revolución ocurran cosas que jamás nos hemos imaginado. Desde el mundo del gobierno de los ciudadanos creo que la democracia se acabó. Y en cualquiera de las elecciones que veamos, la democracia no existe, porque vota el 30% de la población o la población es obligada a votar, o vota el 70%, pero bajo engaños estadísticos. Y uno de los aspectos que más me preocupa hoy en día es la falsedad en la información estadística, unida a que nosotros tampoco sabemos leer estadística y nos dejamos engañar como mucha facilidad. Uno lee muchos artículos y textos sobre esto y hablan de tener democracia con la cuarta revolución industrial y yo creo que la democracia es la peor opción que se puede tener, cuando pasamos a un mundo en el cual se está cambiando a la propiedad común, al trabajo colaborativo. Así, la democracia está planteada con instituciones competitivas como el mercado y con derechos individuales como la propiedad intelectual y el *habeas data*, yo creo que eso ya debe evolucionar a intereses comunes.

Lo que está operando eficientemente en nuestra sociedad de la cuarta revolución es la anarquía para todo lo analógico y digital. Recordemos, para dar un ejemplo, la calle 72 con carrera 13 en Bogotá, durante una manifestación universitaria; todo es caos, pero todo el mundo pasa la calle. Esto lo explican las leyes de la física, a través de la entropía y en el espacio digital acontece lo mismo, la anarquía tecnológica, porque están ocurriendo cambios tan rápidos, que nos están llevando a ver el mundo de otra manera, como decimos los abogados, en otras circunstancias de modo, tiempo y lugar. ¿Será que el tiempo si existe? ¿O será que estamos todos en el mismo momento? Todo eso lo hace a uno pensar en aspectos que cambia la tecnología. En mi opinión, el siguiente modelo de gobierno que debíamos pensar es el modelo de la "sinarquía", o sea sin anarquía. En mi experiencia cuando se da una crisis tecnológica, lo único que se tiene garantizado es el caos. Y el éxito de la organización es salir lo más rápido posible y con los menores daños posibles de este. Si uno se pone a observar lo que sucede en Internet, ve que de ahí está saliendo la nueva forma de gobierno que es de cooperación descentralizada, en la que es más importante el acceso y el código abierto, que la propiedad privada del mundo analógico precedente y fuerte en las instituciones jurídicas globales. Incluso se puede ver que marcas como IBM, con su inteligencia cognitiva en Watson, permite que los científicos y médicos compartan su conocimiento en oncología. Para resumir, hay que mirar con atención la for-

ma de gobierno que vamos a tener por el impacto de la cuarta revolución industrial.

Jeimy J. Cano M.
Esta primera pregunta de los riesgos deja marcado un poco el terreno en el que nos vamos a mover. ¿Esos estándares y prácticas de seguridad y control van a cambiar? Nosotros veníamos de una tradición en seguridad de mucho tiempo. Si ustedes quieren mirar hay un documento recién desclasificado del Departamento de Defensa norteamericano, fechado el 11 de febrero de 1970[2], donde estaba el detalle completo de cómo se hacía seguridad y control en los sistemas de información del Estado norteamericano. Y si lo revisan a la luz de las prácticas de hoy, la pregunta que este servidor se hizo fue: -¿Será que no hemos evolucionado? Luego de revisarlo la reflexión fue: ¿Casi todo es lo mismo?

En este nuevo contexto la pregunta es ¿los estándares y las prácticas van a cambiar?

Mauricio Guerrero C.
Lo primero que tenemos que cambiar para aplicar estándares y prácticas nuevas es tener mentalidad siglo XXI. ¿En qué contexto? Soy un convencido de que nosotros todavía tenemos sistemas que están actuando para una sociedad estática, cuando estamos viviendo tendencias de dinamismo. Y para poder tener estándares de dinamismo, debemos pensar en lo que no están pensando nuestras Pymes; por ejemplo, cómo abordar mejores prácticas en tests de penetración, cómo incentivar la seguridad de sus bases de datos, no en el mismo lugar, sino mediante redundancias. Adicionalmente, las empresas deben ser capaces de identificar que se están presentando ataques desde adentro, porque siempre se está pensando en los ataques externos, pero no se protegen de los empleados insatisfechos. Para poder cambiar estas prácticas y estándares de seguridad, primero tenemos que cambiar culturalmente. No tenemos que pensar en silos de ingeniería de sistemas, de economía, de sociología, tenemos que comenzar a ser más holísticos en nuestro conocimiento y comprender que hasta que nosotros no identifiquemos cómo estamos educando y cuáles son esos puntos clave de control para empleados y sistemas, no vamos a tener estándares adecuados para nuestras sociedades.

Juan Mario Posada D.
Estudios de seguridad en Colombia muestran que los ciberataques han aumentado en una cifra cercana al 30%. Sin embargo, el más reciente informe global de ciberseguridad de EY, para el caso de Colombia en particular, indica que cerca del 50% de los encuestados declaran que se está disminuyendo el presupuesto en el fortalecimiento de la ciberseguridad y el deseo de protegerla. Lo que claramente va en contravía del cambio profundo de las prácticas, en materia de seguridad de la información. Definitivamente la interconexión es cada vez mayor, por ejemplo, se dice que el ser humano lee hoy cien veces más de lo que leía hace 20 años.¿Qué leemos? Y es importante responder esta pregunta, porque si tomamos las decisiones basados en lo que leemos y lo que leemos no tiene la calidad sufi-

2 Documento disponible en: https://www.rand.org/pubs/reports/R609-1/index2.html

ciente para soportar una buena decisión, estamos enfrentando un caos del que debemos tratar de salir y ese es el desafío interesante. La inseguridad está permeando la relación empresa-cliente, que se facilita por la necesidad de una mayor interacción entre los distintos segmentos de redes. En la industria vemos que hay más convergencia entre las tecnologías de operación y las tecnologías de información para obtener una mayor y más oportuna recopilación de datos que requieren análisis y que soportan la toma de decisiones. También es importante considerar la calidad de dicha información. Con esto quiero transmitir la necesidad de un cambio en los estándares de control. Ya no estamos enfrentados a los mismos riesgos, ni en las mismas condiciones y sí estamos ante un mundo mucho más indiferente y apático a las consecuencias de una guerra cibernética en curso.

Marcela García C.
Somos una empresa que existe gracias a la tecnología y genera flujo de caja gracias a la data que manejamos, pues, sin que entreguemos los datos, sí podemos analizar cómo están consumiendo los usuarios y, eventualmente, ayudar a los proveedores y aliados a entender a sus consumidores. Sin embargo, nunca debemos dejar de insistirle a nuestros empleados en la importancia de resguardar la infomarción y proteger la data. Es imprescindible que todas las empresas hagan lo mismo y que no se entienda esto como algo de las directivas. Mi edad me hace más positiva en el sentido de que tiene que haber un cambio de paradigma. Tiene que haber un cambio de mentalidad para que todas las empresas entiendan la importancia de la información. Sería interesante poner a funcionar métodos de educación para la gente que trabaja dentro de las empresas, y que esto venga como una directriz desde la dirección de la compañía, para lograr que los empleados entiendan la importancia de la información. Un empleado inconforme tiene un arma caliente en su mano que puede dañar la imagen de una organización.

Andrés Aguilera C.
Estandarizar implica cooperación. Y lo que nos ha demostrado la realidad, es que hay desconfianza. Desde la salida de Edward Snowden de su posición como contratista de los servicios de inteligencia norteamericanos, se empieza a filtrar información sobre el alcance de los programas y a generar una desconfianza entre varios gobiernos, por ejemplo Alemania o Brasil. Eso es un punto de partida, pero traigamos la discusión al día de hoy; se está diciendo que *WannaCry* es un subproducto o un rédito de una vulnerabilidad que había desarrollado el NSA, llamada Eternal Blue. Entonces, construir un estándar cuando hay este nivel de desconfianza es complicado. Yo soy un poco pesimista con esta situación. Uno ve cómo se empiezan a generar islas, feudos; vemos países menores como Corea del Norte tienen suficiente poder para desarrollar armas nucleares, o para poner a una empresa como Sony Pictures, bajo un ataque cibernético bastante fuerte, por una tontería. (La película "*The Interview"* no es mala, es pésima). Pero bueno, para discutir esto, está el dilema de estandarizar, porque para estandarizar en un mundo donde hay una desconfianza total, es muy complicado. Así mismo, la mayoría del tráfico de Internet pasa por Estados Unidos y este país tiene una de las legislaciones

más invasivas a la privacidad, esto en sí mismo se convierte en una disuasión a cooperar. Otro aspecto en cuanto a la cooperación, es el alcance que tienen los ataques cibernéticos de hoy. Y la forma de mitigar o de contrarrestar los ataques cibernéticos es a través de la legislación nacional. Pero, infortunadamente, la Ley 1273 del 2009 en Colombia se queda corta, es obsoleta y existen legislaciones en otras latitudes que la superan. Los cibercrímenes no están localizados en una sola jurisdicción, pueden estar enmascarados en un país de Medio Oriente o en una isla del Caribe. Bajo esa perspectiva no hay una estandarización del marco legal, aunque se hayan intentado cambios al respecto. Adicionalmente, hay una brecha muy grande entre los técnicos y la gerencia de la mayoría de las compañías, la dirección todavía no comprende la importancia ni el riesgo al que se están enfrentando.

Jeimy J. Cano M.

¿Necesitamos una alfabetización digital?

Algunas veces los ingenieros no logran que el mensaje llegue a la gerencia. La gerencia está pensando en términos del retorno de la inversión, de cuál es la ganancia o la pérdida del trimestre y estos elementos que son un poco más estratégicos, que son de más largo plazo, no permean el pensamiento estratégico de las compañías. La gerencia todavía ve con desconfianza la inversión en seguridad, porque lo define como un gasto adicional; la ciberseguridad implica costos que la gerencia no quiere asumir.

María Del Pilar Sáenz R.

Efectivamente, sí estamos ante un momento en el que ha cambiado la forma de tomar decisiones, y donde también los gobiernos se están quedando cortos, porque además tenemos un problema al considerar las fronteras. Pensando en un ciberataque, una compañía que tiene negocios en múltiples países.

Un concepto que viene desde la misma Internet, muy útil para esta discusión es el concepto de gobernanza y también el modelo de múltiples partes interesadas. Esas dos cosas que pueden tener todos los peros de este mundo, pero que es bueno traerlas a esta discusión. Porque si bien, estamos acostumbrados a un gobierno centralista, paternalista, que es el que toma las decisiones por sus ciudadanos, por sus empresas, por su institucionalidad. Ahora estamos cambiando a un modelo donde esta misma anarquía y el hecho de que haya más conocimiento repartido, hace también que haya ciudadanos y empresas que quieran participar en esa toma de decisiones y, claramente, todos tienen o todos deberían tener cabida en la mesa donde se discute, sin quitarle el papel al Estado, encargado de legislar o poner un marco de referencia; pero, los otros actores tienen que estar involucrados. Esa es la idea de modelo de múltiples partes interesadas.

Si tomamos eso y lo llevamos a la parte de estándares y prácticas, yo creo, que los hay muy buenos en el sistema financiero, por nombrar alguno. No serán los mejores, no serán perfectos, pero son mejores que los de otros sistemas y, sin embargo, son tan desconocidos para el resto, que es difícil llegar a ese mismo nivel por parte de la sociedad civil, la academia o cualquiera de los otros grupos, que deberían estar implementando sus medidas de seguridad para protegerse. Y es un

problema que no tengamos un estándar abierto, que no tengamos información, que no tengamos estadísticas, o que no las sepamos leer.

La educación juega un papel vital, pero va mucho más allá de la alfabetización. El grave problema que nosotros tenemos, es que hemos dedicado mucho tiempo a enseñarle a la gente a prender el computador, a abrir la hoja de cálculo o el procesador de palabras favorito, y creer que es suficiente y que el usuario ya sabe todo lo que debe saber. En mi concepto, la alfabetización debe apuntar a que los usuarios también conozcan asuntos básicos de seguridad digital, como saber identificar un sitio seguro para navegar en la *web*. Aunque en este tema hay otros problemas, como que el gobierno, por ejemplo, ni siquiera ofrece la mitad de sus servicios a través de páginas con https. Y, más allá de eso, coincido también en que estamos perdiendo interoperabilidad y aumentando la centralización, factores que son bastante nocivos. Las grandes compañías que manejan la comunicación de billones de personas, WhatsApp, por ejemplo, corren el riesgo de que el sistema se caiga y entonces, el mundo se detiene, aparecen los "memes" y la gente se ríe de lo sucedido. Pero, lo grave es la centralización de los canales de comunicación y la falta de interoperabilidad. Para citar un ejemplo concreto, quien usa Signal o Telegram no pueden comunicarse con los usuarios de WhatsApp. ¿Por qué? Porque se creó una barrera y ésta es completamente artificial. Deberíamos empezar a pensar en una estandarización que nos lleve a poder tener interoperabilidad y que el usuario diga, no voy a usar WhatsApp más, quiero usar Signal; pero que esto no impida que fluya la comunicación con los parientes y el experto en seguridad. Así mismo, en términos de las brechas del conocimiento, no es solamente que el técnico no le pueda hablar a la gerencia. Soy una convencida de que éste muchas veces le habla con sinceridad a la gerencia y la gerencia no sólo no lo entiende, sino que no tiene cómo entenderlo. Hay un problema de traducción del lenguaje técnico al lenguaje coloquial. Y si no miramos seriamente cómo logramos hacer puentes, seguiremos creando islas. En resumen se necesitan estándares y buenas prácticas, saber qué está haciendo el otro, mirarnos con un poco más de confianza y ver cómo podemos colaborar.

Sara Gallardo M.

Llevo 19 años como editora de esta revista y en todo ese tiempo no he dejado de escuchar el mismo planteamiento en torno a las carencias de la comunicación entre los técnicos y quienes no manejan el lenguaje de los bits y de los bytes.

Jaime Eduardo Santos M.

Tengo dos aproximaciones frente a la alfabetización digital. Una es que creo que sí van a cambiar todos los estándares, pero a partir de dos cosas. La fabricación de materiales por los humanos, entiéndase materiales como el grafeno y lo que son los seres humanos (biometría) y no de lo que saben o portan. Es decir, cuando uno va a un cajero, tiene una tarjeta y se sabe una clave, eso ya se murió. Pasamos a biometría, que es tomar una parte del ser y después vamos a pasar a partes más internas de ese ser. En este momento estamos en la parte externa del cuerpo, y la siguiente evolución va a la parte interna. Pero, esos estándares vienen por la industria, desde el mate-

rial y el diseño; nos va a gobernar la seguridad y eso va a ocasionar unos tipos de problemas, como los que está planteando la sociedad civil. En otras palabras, vamos a estar atrapados por alguna de las marcas globales.

Lo otro es el tema de confianza, relacionada con los empleados y tiene que ver con el hecho de compartir. En mi opinión, la tecnología está rompiendo la brecha de desconfianza; basta mirar cómo opera *blockchain*.

¿Por qué uno usa un abogado? Porque el abogado debe saber algo sobre normas y jurisprudencia que yo no sé. Es decir, el abogado es un intermediario. ¿Por qué utilizo un comisionista de bolsa? Porque él debe saber algo de mercado que yo no sé, y ahí estoy dispuesto a pagar un "peaje". En general, todo el que está atravesado en la mitad, lo que genera es confianza. Entonces por eso, las instituciones financieras tienen unas supervisiones especiales, unas normas especiales, porque el Estado tiene que cuidar la confianza en la banca central, la confianza en los bancos.

Mauricio Guerrero C.
Todavía tenemos problemas con el cambio en el modelo de negocios de las organizaciones; todavía pensamos en modelos de negocio del siglo XX, y hasta que no pensemos en cómo vamos a cambiar nuestra oferta y cadena de valor para tener en cuenta todos estos temas, muy probablemente va ser imposible que pensar en cómo vamos a sacarle beneficio a la ciberseguridad, a mediano plazo.

Jeimy J. Cano
¿Qué tipo de cambios normativos se advierten sobre el tratamiento de la información, en el marco de la cuarta revolución industrial?

Marcela García C.
El modelo de negocio nuestro gira alrededor de saber interpretar la información, pues aunque generamos rentabilidad con el porcentaje de utilidad que Rappi le genera a los restaurantes y mercados, nuestra labor es estar presente en los micromomentos de los usuarios y, por ende, poderles ofrecer lo que necesitan. Es por esto que es muy importante tener protegida la información, pues nosotros necesitamos tener protegida nuestra data que entiende a los usuarios. Para convertirnos en una aplicación disruptiva, debemos generar confianza y tener un control muy grande de la información que manejamos. Una empresa como Snapchat, que debía algo así como 500 millones de dólares, cuando entra a la Bolsa, se convierte en una empresa de 25 billones de dólares. Y eso se debe a la información que maneja, a que conecta a las personas y a que genera confianza. El poder hoy no lo da la tierra, como en la época de la agricultura. No es quien más tenga fábricas o propiedades, sino quien revoluciona a partir de la información que posee. Si la quinta guerra mundial va a ser por agua, la cuarta guerra mundial será por información. De ahí la importancia de generar una reglamentación básica que no interfiera en el derecho a la libertad de difundir, pero que maneje un control. Así mismo, educar a las personas desde los mismos colegios, sobre la importancia de compartir información y, sobretodo, cómo protegerla.

Juan Mario Posada D.
Aquí hay un tema interesante y es el desafío al que se enfrenta el modelo

legislativo actual de la mayoría de los países. La referencia que hacen a algunas de las aplicaciones móviles y redes sociales emergentes me lleva a pensar en el caso puntual del transporte, con aplicaciones que ya van a completar tres o cuatro años de funcionamiento en Colombia y la legislación aún no resuelve el conflicto, versus el modelo tradicional de transporte público. Es decir, la legislación va a un paso mucho más lento que la transformación digital. Estos problemas se están convirtiendo en problemas sociales de una magnitud importante.

Andrés Aguilera C.

Una de las cosas que ocurren en el sistema legal colombiano, es que lo que no está en la norma, no es delito. Nuestro sistema jurídico deja por fuera lo que no está tipificado en la norma o en el código penal; es decir, no es delito, y en nuestro país, durante muchísimo tiempo, ciertas conductas o actos delictivos que eran ilegales en otro lado, aquí no eran procesados. Precisamente, porque la legislación no había incluido esos nuevos delitos informáticos y como no estaban tipificados en el código penal, entonces no se perseguían.

De otra parte, nos damos cuenta cómo las innovaciones van a una velocidad que deja atrás todo accionar del Estado. Por ejemplo, cuestionamos la legalidad de Uber, a AirBnB porque pone en riesgo la legalidad de los hoteles, que pagan los impuestos, que hacen el registro nacional de turismo y un montón de cosas, estas nuevas aplicaciones empiezan a romper ese modelo tradicional. Sin embargo, las nuevas realidades nos llevan pensar que las jurisdicciones empiezan a borrarse.

Estados Unidos tiene una legislación bastante fuerte de protección al Estado. Uno de los aspectos más interesantes del escándalo de Snowden, es que todo lo que hizo el Estado norteamericano a través de sus agencias, era legal. Ellos nunca quebrantaron la ley. Por eso Snowden sigue siendo considerado un traidor, en lugar de ser un héroe; sigue siendo el "malo del paseo", porque las agencias gubernamentales actuaron dentro de lo que la ley les permitía. ¿A qué voy con esto? Los ciudadanos también necesitan ser protegidos, que se fortalezca el marco legal para protegerlos de la intervención estatal y de la intervención de esas empresas que empiezan a acumular grandes cantidades de datos que ponen en situación de vulnerabilidad la privacidad de las personas.

En Estados Unidos empezaron a implementar las leyes de divulgación. Cuando hay empresas que empiezan a manejar tantos datos sensibles de los usuarios y de los clientes, si llegan a tener algún tipo de vulnerabilidad, el Estado actúa. O sea, cada uno de los 47 estados que al día de hoy tienen leyes de divulgación, obligan a las empresas que han sido vulneradas a notificar a sus usuarios. Eso me parece que es una innovación legal que deberíamos considerar en nuestro país, porque seguramente muchos eventos informáticos ocurridos en Colombia, jamás se han divulgado, precisamente para mitigar el riesgo reputacional de un ciberataque.

Mauricio Guerrero C.

Lo que para nosotros es legal, seguramente para los rusos o para los chinos no lo es y al revés. Entonces, hasta que no sepamos qué es legal en el sistema internacional, los cambios

normativos van a estar relegados a un segundo plano. En este contexto, estamos bien atrasados en términos de comprender en el cómo vamos a combatir cierto tipo de delitos, porque todavía no sabemos cuáles son.

Un punto que me parece muy importante mencionar, con base en lo que han dicho es el tema de criptomonedas, porque no hemos sido capaces de cambiar la arquitectura financiera internacional durante los últimos 25 años, eso lleva un cambio de bastante tiempo y tenemos una nueva tecnología que ha sido disruptiva y está cambiando todo el sistema internacional. Parte del ciberdelito se está generando porque tenemos una moneda que es invisible, que no permite ver quién está detrás de estos delitos.

María Del Pilar Sáenz R.

Hace un año largo, para abril de 2016, Karisma participó dentro de la escuela de sur de gobernanza de Internet, organizada en las instalaciones de la OEA. Y, aprovechando que estaban varios de nuestros amigos y compañeros de la Sociedad Civil de América Latina, decidimos impulsar una declaración conjunta de la sociedad civil a la Organización de Estados Americanos, y a los gobiernos de los países miembros sobre temas de seguridad digital en América Latina. Y es realmente la declaración lo que quisiera traer a colación porque ya está por escrito. De lo que nosotros esperamos, no necesariamente todo se termina resolviendo en la regulación. En algunos casos son acuerdos o marcos generales sobre los cuales operar. Y, en tal sentido, nosotros sí creemos que fue un muy buen cambio, pasar de hablar de ciberseguridad a hablar de seguridad digital en el Conpes. Y es bueno porque el centro lo ponen en las personas y en las comunidades y no solamente en el Estado y la protección de las entidades del Estado. Eso no quita que sea importante la protección de las entidades del estado, pero el centro del asunto debe estar en la gente y en las comunidades. Es decir, debe estar alineado con el marco general de

los derechos humanos de cada uno de los países y del marco global que los cobija. Y ese marco aplica en los medios digitales, de cara a la privacidad, a la libertad de expresión como lo manifiestan los relatores de varios de los organismos internacionales, quienes manifiestan que si no hay una clara ley nacional, existe un marco de derechos humanos internacional que es garantista. En otras palabras, no es posible pasar por encima del derecho a la intimidad de los usuarios para ofrecer sus datos al mejor postor. Y en esa dirección, debe existir una institucionalidad que responda a esas expectativas. Es difícil, pero existe.

Adicionalmente, es necesario adoptar mecanismos de transparencia y rendición de cuentas. Y esto no rige solamente para las compañías que ya lo están haciendo avisándole a sus usuarios cuándo hicieron una petición de datos, sino también a las autoridades mismas cuando retienen información o la solicitan. Y en esta dirección venimos trabajando durante los últimos tres años, en lograr, por lo menos, que las Telcos en Colombia empiecen a generar informes de transparencia basados en la idea de rendición de cuentas. En esta rendición también hay que mirar qué pasa con los macrosistemas de vigilancia frente a los mecanismos de supervisión y control. En el caso colombiano es bastante grave.En nuestra ley de inteligencia y contrainteligencia, se exigió que las Telcos tienen que guardar la información de las conexiones de sus usuarios durante cinco años. En Europa, la Comisión Europea dice que seis meses, es demasiado. Nosotros tenemos cinco años y el acceso a esa información la tienen las autoridades competentes, que finalmente son muchas. Además tenemos cada vez más sistemas masivos de almacenamiento de la información, que pueden generar problemas.

El siguiente paso debería ser un fortalecimiento del cifrado. Nosotros desde la Sociedad Civil, creemos que el cifrado es algo importante y que cualquier tipo de acuerdo internacional para debilitarlo, como tener puertas traseras para burlar los sistemas de cifrado es algo nocivo porque el cifrado garantiza en algunos casos el anonimato, garantiza la posibilidad de ejercer la libertad de expresión y de tener intimidad. Es la batería de derechos humanos, otra vez.

Hay otra cosa que nosotros dijimos en su momento y era que se necesita tener un fortalecimiento y recoger e implementar experiencias y buenas prácticas de otras regiones en materia de políticas de seguridad digital. Y ahí por ejemplo, entra a jugar el tema de Budapest. Si bien no es la panacea y en su momento también tendremos objeciones sobre la forma en que se implementará, sí nos da un marco normativo general que se puede discutir internacionalmente y en el que todos podamos jugar en unas mismas condiciones.

Finalmente, agregaría que independientemente de la regulación que se vaya a plantear en el marco de la implementación del Conpes de seguridad digital, lo que se necesita garantizar es que todas las partes estén ahí en esa discusión, porque sin eso, no funciona.

Jaime Eduardo Santos M.
Abordaré la respuesta como abogado. El profesor italiano Mario Losano tiene un súper artículo denominado “El de-

recho turbulento", en el que señala que ya es hora de jubilar la teoría estructural de Kelsen. Debo anotar para los no abogados que Kelsen es el padre de la pirámide normativa que usábamos los abogados para interpretar el Derecho positivo. Claro que en Colombia no ha muerto la interpretación jerárquica, y las leyes se siguen haciendo pensando que Kelsen aplica en la era digital y al mercado de dos caras o de plataformas tipo Uber. De ahí que en mi blog señale que los abogados debemos cambiar la brújula y la escalera por el GPS. El deber ser es una estructura militar y cuando uno va a la realidad, así no funciona para muchos ciudadanos como los emprendedores del mundo digital. El Derecho es cómo funciona, cómo se vive, cómo lo aplican los jueces y no cómo se escribió en el siglo pasado o antes. Ilustra este punto la jurisprudencia de la Corte Constitucional sobre *habeas data*, que tiene más poder que la ley. También resoluciones de las comisiones de regulación que tienen más poder que una ley. Insisto que debemos seguir las decisiones de los jueces que pueden otorgar o negar derechos. En suma, el Derecho turbulento del profesor Losano exige aplicar el derecho como funciona y no en la jerarquía y la norma.

Además, Colombia no es líder en tecnología, no hacemos ciencia, esto puede sonar duro, pero no estamos en la frontera de ningún asunto de la cuarta revolución. Entonces no podemos estar en normas de frontera, sino en normas de copia, de seguidores. Es importante "darse cuenta" que la regulación en un mundo global viene de ONGs, como ocurre con las normas internacionales de información financiera, o las de gobierno corporativo y más aún, las de industrias como la aviación y la química.

El mensaje que les quiero dar es que los abogados estamos en un mundo turbulento, que empezamos a darnos cuenta que a nuestras facultades de derecho les está pasando lo mismo que a las facultades de contadores y a las de ingenieros; están formando personas para el siglo XXI con herramientas del siglo XX y estamos haciendo mal la tarea de educación, al punto que puede hoy ser más útil una certificación que un título universitario. Este es un debate para hacer.

Marcela García C.

No podemos tapar el Sol con un dedo. Esto es algo que está pasando; los negocios se hacen con información y por eso es importante dedicarnos a educar. Al educar a la gente, al enseñarles la importancia de proteger la información y de tener claridad de lo que implica hacer parte de la era digital. Por ejemplo, si educamos a las personas para que sepan lo que están firmando cada vez que entran a una nueva red social, tal vez, podamos evitar problemas en el futuro.

María Del Pilar Sáenz R.

Uno de los aspectos que considero vital es pensar, así como se planteaba aquí que la democracia ha muerto, uno también podía decir tranquilamente que el consentimiento informado no es suficiente y que eso es una falacia. En otras palabras, el hecho de firmar y marcar la casilla, no son aspectos suficientes para considerar que se entienden y aceptan los términos y las condiciones de servicio. Eso es 'carreta'. Nadie se lee la letra menuda, nadie. Y si tiene lupa tampoco le alcanza la vida para leerse los contratos de las cosas

que firmó cada vez que abrió una cuenta. Además, no lo va a entender porque está en unos términos espantosos. El consentimiento informado es una falacia. Si ese es el panorama, yo si quisiera traerlo acá, porque es un problema para la seguridad de los usuarios. Se les entrega unos poderes a unas empresas con las que se está firmando un acuerdo y al aceptar uno ya ha entregado el alma, esta vida y la otra. Entonces, eso claramente tiene que cambiar.

Hay un modelo canadiense, que es hablar de privacidad por diseño. ¿Qué pasa si ponemos al usuario en el centro? Pues si el usuario no va a ser el que lee el contrato hasta la última minucia ni va a cambiar todas sus opciones de seguridad a las más privadas, arranquemos al revés, que el estándar sea la privacidad. O sea que de entrada, una empresa no le pueda enviar todos los correos de este mundo, y que si usted quiere un correo, tenga que marcar la casilla.

Tuvimos una discusión álgida con el gobierno cuando estaban empezando a plantear todo el proyecto de carpeta ciudadana, -un proyecto de MinTIC que después cambió de nombre a servicios digitales básicos y ahora a servicios digitales ciudadanos-. La implementación de este proyecto implicará que ciertas empresas puedan tener en sus manos la información que resulta de la interacción entre el Estado y los ciudadanos, en la carpeta de cada ciudadano estará almacenada toda esta información. Per se. Yo quiero que esa carpeta y todo el sistema que la soporta tengan las mejores medidas de seguridad y que tengan las mejores opciones de privacidad por diseño. Ese fue el planteamiento que hicimos a ese proyecto. Desde Sociedad Civil no podemos renunciar a eso.

Jeimy J. Cano M.
Se han referido a la confianza como marco general de la discusión y un poco sobre el tema normativo. Éste señala que la confianza, cuando existe, acelera las cosas, y cuando no, genera limitaciones. Más adelante conversaremos que en seguridad lo que hacemos es un ejercicio de confianza imperfecta, todo el tiempo. Todos nos equivocamos. Así que la idea es ponerse de acuerdo en el umbral de riesgo acordado.

Vamos ahora a pasar al tema que es realmente del Estado. Las infraestructuras críticas o los elementos de la gobernabilidad de una nación. Un escenario que, por ejemplo Rappi, lo debe tener en el mapa de riesgos. ¿Qué sucederá cuando eso pase? Y en otros espacios como los aeropuertos, operadores, los servicios de energía, petróleo, gas y otros similares. Se empieza a pensar en la dimensión de lo que implica estar conectados y funcionando, dependiendo de una infraestructura crítica. Así que la siguiente pregunta es:

¿Qué pueden hacer las empresas con infraestructura crítica de un país, frente a esta realidad? ¿Se debilita el cargo de analista de seguridad en el contexto de la cuarta revolución industrial?

Juan Mario Posada D.
Este tema de las infraestructuras críticas es muy vigente, porque el país está trabajando desde hace bastante tiempo en la identificación de la infraestructura crítica cibernética. Y lo que

requieren, pueden y deben hacer las empresas que operan o que son dueñas de los componentes críticos es, en primera instancia, conocer cuáles son esos elementos de la operación del negocio que forman parte de la infraestructura crítica de la nación. Y, a partir de allí, hacer análisis de los riesgos a los que están enfrentados esos activos de infraestructura crítica cibernética, que dejan de ser un riesgo circunscrito y trascienden a lo que es el riesgo o el efecto adverso que puede causar en la nación, en la sociedad civil, en el medio ambiente, en las personas y en los distintos componentes. Habiendo pasado por ese análisis de riesgos, también será importante esa autoevaluación del control, o de los controles orientados a la mitigación de tales riesgos. Un aspecto fundamental cuando hablamos de infraestructura crítica cibernética, es la cooperación. Porque una empresa como *Rappi* depende de los proveedores del servicio de Internet y éste depende del servicio de energía; y el proveedor de energía, a su vez, depende de la empresa de petróleo y gas, por los combustibles que utilizan para mantener sus plantas-; y, así sucesivamente. Se trata de una cadena interminable en la que todos los actores se convierten en un punto único de falla. Y frente a esta situación se requiere una cooperación muy fuerte, para que los esfuerzos sean coordinados en pro de mantener la continuidad. En Colombia no es una obligación reportar los incidentes cibernéticos a los que se ve expuesta una empresa. De manera que la cooperación es el elemento central de la protección de la infraestructura crítica cibernética.

Sobre la pregunta ¿se debilita el cargo de analista de seguridad? Yo no creo que se debilite, se enfrenta a un gran reto. De ahí que sea necesario entender mucho más del entorno en el que opera y construir empatía con los interlocutores del negocio. Porque el analista de seguridad debe verse desafiado a comunicarse en un lenguaje mucho más claro con la alta dirección de la organización, con el Gobierno, con la sociedad, de manera de lograr la alfabetización digital y la alfabetización en seguridad. Porque la sociedad entiende muy bien los riesgos de seguridad física. Por ejemplo, salgo de mi casa, debo dejar cerradas la puerta y las ventanas; salgo de mi casa y debo apagar la estufa de gas; salgo de mi casa y debo tomar una serie de precauciones. Apliquemos estos conceptos a nuestro comportamiento y a nuestra disciplina en el entorno digital.

Jaime Eduardo Santos M.

La infraestructura no es exclusiva del Estado, no es pública, nuestros gobiernos en Latinoamérica han tenido una ola de privatización de los servicios estratégicos, lo hemos visto en nuestro país en los servicios públicos domiciliarios; las telecomunicaciones, la energía, el agua, la recolección de basuras,etc. También es importante se-ñalar que la infraestructura crítica no es una responsabilidad solamente del sector público, sino de las empresas que están operando como concesionarias.

Sobre el analista de seguridad hay un déficit de talento cibernético a nivel global. No hay los suficientes analistas. No obstante, en el evento de CEBIT, de abril de este año en Alemania, vi utilizar sistemas de inteligencia artificial y realidad aumentada, precisamente para gestionar y mitigar los riesgos inherentes a la estructura críti-

ca. En consecuencia, vemos cómo la misma tecnología está proporcionando nuevas herramientas para mitigar esas nuevas amenazas.

Mauricio Guerrero C.
¿Qué pueden hacer las empresas? Pensar en resiliencia y no en continuidad de negocios ni en gestión de riesgos, sino en algo más integrado. Sistemas resilientes, es un tema que todavía no estamos desarrollando en el país y que deberíamos trabajar muy seriamente, de cara a la infraestructura crítica. Si las empresas son resilientes, el país es resiliente, en eso todavía no estamos trabajando muy seriamente, creo que ahí hay una oportunidad para los consultores y para muchas personas. Considero que esto fortalece al analista de seguridad, en el sentido en que el modelo de negocios, le está exigiendo a las empresas tener a alguien interno, y eso hará que esa brecha de talento siga creciendo, debido a que muchas más empresas van a necesitar a estos analistas; a través de tercerización o teniendo a alguien *in house*, pero el analista de seguridad, por todo lo que hemos hablado, es indispensable en el actual modelo de negocios, y una pieza indispensable para poder enfrentar los retos del futuro.

María Del Pilar Sáenz R.
Siguiendo la conversación, la micro conversación, que fue mirarnos a los ojos y decir: "la infraestructura no está o está acá, pero no nos pertenece como país". Además de la resiliencia, también es importante pensar en la transparencia, en todos los escenarios. Para poder tomar buenas decisiones se necesita información y en cualquier caso, la información tiene que ser lo más veraz, completa y actualizada, lo más cercana a lo que está pasando, como para que uno pueda decidir algo. Si se tiene acceso a esa información, probablemente se podrían tomar mejores decisiones, en un marco de transparencia. Si supiera cuántas empresas tienen problemas de seguridad, no estoy diciendo que me digan exactamente qué empresa, porque entiendo el problema de reputación, pero si supiera cómo está el sector, quizá pudiera tomar mejores decisiones sobre si necesitamos más y mejores regulaciones.

Y frente a la figura del analista de seguridad, también creo que se debe fortalecer. Este perfil empezará a cambiar y se le van a exigir otras cosas. En mi caso, yo no solamente le exigiría que hable en un lenguaje un poco más humano con el resto de la jerarquía con la que tiene que interactuar, sino que le exigiría, que fueran un poco más sensibles con las necesidades del usuario y que se pusieran en los zapatos del otro. ¿A qué va esto? En muchas de las decisiones de política pública se consideran las necesidades e intereses de las empresas o del mismo gobierno pero no las de los ciudadanos.

Tomemos como ejemplo los teléfonos celulares y la cantidad de datos que estos dispositivos generan y la información sobre sus usuarios que se puede derivar de su análisis. Un teléfono móvil cada tres segundos se comunica con las torres de telefonía más cercanas, para encontrar la que le da mejor señal en el eventual caso de necesitar establecer una llamada. Por esta razón, cada tres segundos la red de telefonía celular sabe con bastante precisión, donde está mi móvil y por tanto dónde estoy yo. Más allá de eso,

al usar el GPS mi dispositivo puede saber dónde está localizado el equipo y si uso aplicación para tomar un taxi o plantear la mejor ruta hacia mi destino, también sabría hacia donde voy. Yo no siempre quiero que mi teléfono sepa para dónde voy. Y aún más, si mi teléfono sabe para dónde voy, yo no sé si quiero que la compañía que me provee el plan de datos lo sepa.

En este entorno surge la discusión sobre los algoritmos. Los algoritmos nos están definiendo ahora a nosotros como personas, frente a unos intermediarios, que son esas grandes compañías que tienen un consumo masivo de información de la gente. Uno termina siendo perfilado y caracterizado por un algoritmo. ¿Quién controla eso? Nadie. ¿De qué forma podemos tratar que las personas que diseñan y generan esos algoritmos también sean conscientes de otros problemas como la transparencia, la intimidad, la libertad de expresión, relacionadas con otra cantidad de asuntos? Es necesaria una mirada de derechos humanos porque hay un montón de vacíos que no se están considerando cuando se plantean este tipo de preguntas.

Jaime Eduardo Santos M.
Hay bienes que son públicos, bienes que son privados y bienes que son comunes, como el aire. Entonces lo primero que tienen que hacer las empresas con infraestructura crítica es ser conscientes de que manejan un bien común, no un bien privado. Cada vez que hay un debate, que si unas antenas se tienen que devolver, que si unos camiones de basura se tienen que devolver, se arma un debate, que si eso es público, que si es mío o si es de quien dio la concesión. Entonces, me encamino porque tenemos que proteger el concepto del bien común, que es además una institución real, en el mundo irreal del derecho. Y el que está llamado a que eso funcione así, es nuevamente el ciudadano a través de la democracia participativa. Si bien, atrás mencioné que la democracia murió, es porque la participación ciudadana la está ayudando a que muera, la está ayudando a enterrar. Hay que pasar a la democracia participativa.

En segundo lugar, además de saber que es un bien común, es necesario aprender de la industria de los juguetes para hacer las cosas bien desde el diseño y probarlas en laboratorios que les permitan responder con eficiencia durante una crisis, quizás originada en un error humano o en un ataque cibernético a la energía o las comunicaciones.

Soy un convencido de que en las cosas básicas están las soluciones a las más complejas.

Jeimy J. Cano M.
¿Cuáles son las habilidades, competencias y conocimientos que requerirán los nuevos profesionales frente a la seguridad y control en la cuarta revolución industrial? ¿Se están preparando las universidades para formar a los estudiantes en dichas competencias/habilidades?

Marcela García C.
De la misma manera que se instauró como requisito hablar inglés, se debería exigir a los empleados saber cómo reconocer la importancia de proteger la información y entender un poco acerca del mundo digital. Debemos aprovechar que en el país está llegando Internet a los municipios más apartados, para poder educar a todas las

personas a que administren mejor la información, a saber a qué están expuestos y a aprender sobre cómo manejar la información en el momento en que se vinculen laboralmente a una empresa.

Juan Mario Posada D.

Las dos habilidades fundamentales de los nuevos profesionales deben ser el buen uso de la tecnología y el buen uso de la información, desde el punto de vista de la ética, de la responsabilidad social y, en general, de la profesión de la cual hacen parte. Así mismo, es necesario que los profesionales se preparen en seguridad, frente a esta cuarta revolución industrial. Y puede parecer muy gracioso, pero los profesionales de seguridad tendrán que aprender de mercadeo, de cadenas de suministro, de estrategias, de servicio al cliente, de líneas de producción, de finanzas en una medida suficiente para entender los retos de los negocios digitales, para lograr ofrecer valor a través de la gestión de la seguridad.

Andrés Aguilera C.

Este es un tema que nos toca a nosotros como profesores de la universidad y es una de las líneas de investigación que estamos adelantando. La cuarta revolución industrial implica la desaparición de muchos empleos; implica que muchas funciones se pueden automatizar y se pueden dejar a algoritmos a programas, a un montón de cosas. Y, en tal sentido, el reto de universidad es que seguimos operando bajo un modelo de negocio obsoleto. La misma tecnología nos está retando, porque el salón de clase es una limitación física, cuando vemos que el nuevo modelo negocios contempla el uso de MOOC (Massive Open Online Course), cursos de miles de estudiantes y la pregunta que nos debemos es ¿qué están haciendo nuestras universidades para entrar en ese juego? Entonces el modelo actual, que es el que seguimos, es el profesor, quien prepara su clase, tiene una infraestructura limitada, el número de sillas, el número de estudiantes. Pero cuando el modelo de negocio cambia y se convierte en un MOOC obviamente las posibilidades son mucho más grandes. Y la cuarta revolución industrial también está poniendo presión sobre los profesionales de otras disciplinas.

Estamos viendo tecnologías como *high-frequency trading*, en la que el analista financiero sólo tiene que determinar ciertos parámetros de rendimiento. Tecnologías como la inteligencia artificial o la impresión de 3D van a cambiar el panorama laboral. Todos los pronósticos que se hacen es que nuestros profesionales están aprendiendo al día de hoy cosas, que van a ser obsoletas muy pronto.

La apuesta que estamos haciendo es que nuestros estudiantes empiecen a aplicar algo que se llama *Life-Long Learning*, para que las herramientas que reciben en la universidad les sirvan, no sólo para obtener un grado y un título, sino para que puedan seguir aprendiendo a lo largo de su vida. Todo está cambiando muy rápido. Nuestros profesionales de la próxima promoción, seguramente en muy poco tiempo, tendrán que volver a las aulas o tendrán que volver a formarse en las últimas tendencias, en el más reciente *software*, o en cualquier asunto que sea necesario. La cuarta revolución industrial está cambiando toda la dinámica del trabajo, se está contemplando el desempleo tecnológico y la universidad, de cierta forma, debe lle-

nar esos vacíos, también innovándose.

Mauricio Guerrero C.

En mi opinión, se trata de habilidades. En el informe del Foro Económico Mundial, del año pasado se decía que ocho de cada 10 habilidades necesarias a 2020 serán habilidades suaves, un aspecto muy importante para cualquier profesional. Así mismo, se referían al problema de comunicación que tenemos. Es necesario revisar cómo nos comunicamos todos para tener modelos de negocio más exitosos. Hacia el futuro serán las certificaciones las que funcionen, en especial porque los análisis que estamos realizando lo hacemos bajo el paradigma de la computación clásica, pero una vez la computación cuántica sea comercializable, nos va a cambiar todo.

María Del Pilar Sáenz R.

La pregunta me puso a reflexionar, porque debe orientarse a si hay que formarse para la vida y no para el trabajo. Parece obvio decirlo, pero hay que decirlo. Y lo planteo desde mi propia experiencia. Soy física de formación y todo lo que he hecho durante los últimos años está relacionado con una rama totalmente diferente. Es decir, mi trabajo en la política pública es más de abogados que de cualquier otra disciplina. Y terminé involucrada porque me interesaba. El pensamiento en la "caja" es lo peor que uno puede poner en práctica. Un aspecto clave es la flexibilidad, la posibilidad de iniciar con un tema y terminar en otro, experimentando la formación por el camino. Más allá de tener una serie de habilidades esenciales es importante entrenarse para hacer algo específico. En ese sentido, el aprendizaje sobre tecnología también debe enfocarse no hacia saber hacer, sino hacia entender cómo funciona. Es paradójico que la mayor parte de los equipos utilizados son cajas negras para casi todos los usuarios. Tan es así, que somos incapaces como país de generar una nueva tecnología, porque no la entendemos y no estamos en esa punta. La solidaridad se suma también; puede parecer un valor extraño cuando uno lo piensa en educación, pero es muy importante ponerse en el 'zapato del otro' y ser capaz de bajarse del nivel de lenguaje especializado cuando se le habla a una persona que no habla sobre lo mismo, en los mismos términos. El principio que me enseñaron en la universidad, es que realmente podría demostrar que entendía un tema, cuando fuera capaz de explicárselo a una persona sin conocimiento sobre el área. En pocas palabras, falta mucha pedagogía sobre tecnología.

Jaime Eduardo Santos M.

La formación universitaria daría para un único debate. No obstante, en mi opinión la academia está atravesando por una crisis enorme y opto por las certificaciones. Y a estas sumaría la curiosidad y una visión transversal. Infortunadamente, nuestro sistema educativo es de silos de conocimientos. Si usted es abogado, no sabe sumar; si es físico no sabe leer. Y todas las universidades están construidas desde esa perspectiva. Así que el primer cambio en las personas sería lograr salirse de esas cajas para tomar diferentes asignaturas en diferentes disciplinas. Las universidades no son flexibles, aunque los jóvenes estén optando por hacer dobles programas. Basta contemplar la dificultad para el cambio de una carrera a otra, aunque sea similar en disciplina.

Y además, cuando pasamos a la inteligencia cognitiva de la cuarta revolución industrial, la situación se vuelve más compleja para los métodos de enseñanza tradicionales. La máquina aprende como el humano para ayudarle, pero podría ser para sustituirlo en muchas funciones, como algunas legales. (Abogado Ross basado en Watson). Luego lo que tenemos que legarle a las nuevas generaciones es que sean curiosos y holísticos para construir su historia de vida. Aquí en el foro estoy oyendo dos ejemplos que me llaman mucho la atención: una física en políticas públicas y un politólogo en sistemas. Eso son historias de vida, eso no son hojas de vida.

Jeimy J. Cano

Después de observar los caminos disciplinares, hoy estamos en otro escenario que es el transdisciplinar: comenzar en Comunicación, conectar con Derecho y terminar en computación. Esto significa construcción y conexión. En esa dirección creo que la cuarta revolución nos invita a mirar una postura de tales dimensiones.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" 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 y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res); corresponsal de la revista IN de Lanchile. En la actualidad, es editora en Alfaomega Colombiana S.A., firma especializada en libros para la academia y editora de esta revista.*

Juegos de guerra

Un ejercicio de construcción conjunta en ciberseguridad y seguridad de la información.

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

Introducción

En un contexto geopolítico inestable, con amenazas digitales inciertas y nuevos competidores creando incertidumbres globales, las organizaciones deben avanzar rápidamente en espacios de construcción colectiva que permitan crear capacidades inexistentes frente a escenarios que aún no ocurren (Cano, 2017).

Bajo esta perspectiva los conceptos de ciberseguridad y seguridad de la información, comienzan a reconstruir sus fronteras naturales y transitan hacia prácticas, algunas desconocidas, sobre contextos digitalmente modificados, en los que cualquier evento puede ocurrir y afectar las condiciones normales de la operación de una empresa. Posiblemente, esto implica desconectar y repensar conceptos sobre los cuales los estándares conocidos han sido planteados, para encontrar nuevas oportunidades que construyan un nuevo normal de "confianza" para las empresas en una sociedad tecnológicamente moldeada.

Para lograr lo anterior, tanto la ciberseguridad como la seguridad de la información, temáticas complementarias en sí mismas, deben crear un mercado propio, que haga nuevos trazados sobre un territorio de volatilidades digitales, con el fin de encontrar distinciones que permitan a las organizaciones y a las personas establecer sus propios fundamentos de la lectura de la protección, en el conjunto de expectativas y logros que se pretenden lograr, anticipar y desarrollar para conquistar un nuevo lugar en la dinámica de los negocios actuales.

Esto supone que la ciberseguridad y la seguridad de la información dejen de ser aspectos solitarios de las empresas, dominios controlados por un conocimiento especializado, para convocar la sabiduría del negocio y de sus participantes, habida cuenta que su visión en el terreno ofrece aspectos de

la realidad que, por lo general, superan la percepción particular de un analista de seguridad o ciberseguridad.

En este sentido, la práctica de los "juegos de guerra" (en inglés *war games*) establece una oportunidad para encontrar los diferentes puntos de vista de la dinámica de la organización con la lectura de los analistas de seguridad y ciberseguridad, orientados a comprender y construir en conjunto, las acciones requeridas para responder táctica y estratégicamente a la experiencia de un ciberataque, o mejor, a un escenario de negocio donde se compromete la promesa de valor de la compañía en un entorno digitalmente modificado.

Aunque esta práctica no es nueva en el escenario global, como quiera que ha sido utilizada en entornos de defensa nacional por algunas fuerzas militares del mundo (Perla, 1990), sí es una nueva apuesta que marca un estado de madurez en la comprensión de los escenarios tecnológicamente modificados de las empresas, en las que tanto los directivos como las personas de la línea de operación, además de los especialistas en seguridad y ciberseguridad, participan para crear una visión simulada de un ciberataque con información incompleta, que pruebe las capacidades de la organización para enfrentar este tipo de situaciones digitales adversas.

Juegos de guerra: una apuesta de construcción conjunta

En el contexto militar los juegos de guerra suponen un reconocimiento de los actores en conflicto, una perfilación de las capacidades del oponente, un territorio que se debe dominar y una conquista que se debe concretar. Por lo general, en este escenario las partes entre sí se reconocen y saben qué tiene cada una para concretar golpes certeros sobre los activos estratégico de la otra, por lo cual el combate se convierte en un juego de estrategias para saber usar lo que se tiene, con el fin de tomar ventaja frente a las limitaciones de los otros (Perla, 1990).

En este juego de estrategia, quien logre la mayor ventaja, es decir, logre descifrar la dinámica de su inteligencia, las tácticas de operación de las tropas, inhabilite las posibles armas claves de mayor destrucción y daño e infiltre las mismas operaciones de su oponente, sin que este lo note, tendrá una superioridad militar que doblega y compromete los planes de su enemigo, no solamente en el terreno operativo, sino en la conceptualización y estrategia de guerra.

Esta lectura militar de los juegos de guerra, si bien suena amenazante y clásica frente al reto de la defensa nacional, plantea un desafío de interés para las organizaciones con el fin de concretar estrategias de defensa frente a un entorno asimétrico e incierto, donde existen múltiples intereses comprometidos, actores conocidos y desconocidos, que en cualquier momento pueden crear el escenario específico en el que pueden comprometer las operaciones claves de una empresa.

Por tanto, los "juegos de guerra" en el contexto empresarial establecen momentos de preparación, reflexión y desafío permanente para habilitar la construcción de una capacidad colectiva de comprensión y desaprendizaje organizacional, sobre la realidad de

las amenazas digitales actuales, orientada a establecer y anticipar estrategias y acciones claves que permitan actuar frente a ataques digitales o campañas planeadas por terceros en contra de la dinámica de la empresa, de manera de aumentar la capacidad de resiliencia empresarial necesaria para continuar avanzando sobre mercados inexplorados y crear oportunidades en medio de situaciones inciertas (Bailey, Kaplan y Weinberg, 2012).

Los "juegos de guerra" en las organizaciones establecen un nivel de compromiso mayor en sus ejecutivos, como quiera que la comprensión de la dinámica de los negocios y sus implicaciones, dejan de estar en los niveles tradicionales de riesgo empresarial y se enriquecen desde la perspectiva de los ecosistemas digitales donde opera la empresa. Esto es, los directivos comienzan a incorporar la distinción de los productos y servicios digitalmente modificados y sus impactos en los diferentes grupos de interés.

Cuando los "juegos de guerra" se constituyen en una práctica permanente de la empresa, la organización permanece en "modo radar" (Prize, 2015); es decir, explorando e identificando aspectos de su entorno digital para capitalizar como oportunidad o reconociendo posibles amenazas para actuar de manera anticipada y aumentar su capacidad de respuesta ágil y efectiva, según se materialicen los impactos de un riesgo desconocido o no identificado.

Juegos de guerra: una aproximación metodológica

Desarrollar un ejercicio de "juegos de guerra" demanda una serie de pasos preliminares, semejantes a la construcción de un escenario, pero diferenciada, en la medida en que se priorizan las acciones contrarias, desde los diferentes puntos de vista de los actores invitados al ejercicio y las capacidades requeridas, para dar cuenta de la situación adversa.

De acuerdo con Bailey, Kaplan y Weinberg (2012) es importante considerar las siguientes preguntas con el fin de contextualizar el ejercicio de "juegos de guerra":

- ¿Puede la organización identificar y valorar rápidamente una brecha de seguridad?
- ¿Puede la organización tomar decisiones efectivas para contener la brecha identificada?
- ¿Puede comunicar efectivamente la brecha identificada a todos sus grupos de interés?
- ¿Puede ajustar rápidamente las estrategias y tácticas de negocio con ocasión de la brecha identificada?
- ¿Puede la organización actuar en conjunto con aliados estratégicos de forma efectiva frente a la brecha identificada?

Basado en estas primeras consideraciones, se plantean, siguiendo las indicaciones metodológicas de la práctica de Intel (Casey y Willis, 2008), dos escenarios, el "más probable" y el de "mayor impacto o daño". Cada escenario planteado contiene al menos los siguientes elementos:

- Un agente que provoca el impacto o daño (por ejemplo, hacktivista pa-

trocinado por un estado, crimen organizado, actor no identificado, empleado interno).

- Habilidades requeridas (por ejemplo, ingeniería social, *malware*, espionaje, vulnerabilidad conocida o desconocida).

- Objeto del ataque (por ejemplo, cuenta de correo electrónico, cuentas de redes sociales, cuentas financieras, datos personales).

- Objetivo del ataque (por ejemplo, robo de información personal, robo de propiedad intelectual, daño en los datos, daño en la imagen, pérdida financiera, interrupción del servicio).

- Indicadores del entorno (por ejemplo, noticias sobre ataques similares, casos semejantes procesados por las autoridades, recientes hallazgos académicos o de la industria sobre nuevas vulnerabilidades).

Con esta información se procede a escribir una historia que conjugue todos los elementos planteados previamente, con el fin de crear un contexto de reflexión base que permita a los participantes imaginar posibilidades, desde cada uno de sus puntos de vista. En este ejercicio no se desecha ninguna perspectiva ni se restringen posturas de los participantes, como quiera que es de esta forma como se enriquece la historia planteada y los elementos de riesgo o amenaza identificados hasta ese momento (Casey y Willis, 2008).

Luego un facilitador, preferiblemente del área de seguridad o ciberseguridad de la información, compila las diferentes visiones identificadas sobre la historia, establece los enlaces frente a las capacidades claves de la organización y aquellos elementos que no puedan relacionarse con las capacidades actuales, para resaltarlos como fuentes de vulnerabilidad que deben ser estudiados y revisados por la organización, en conjunto con el área de seguridad y ciberseguridad y los ejecutivos de la empresa.

Considerando los dos escenarios planteados, este ejercicio deberá tomar por lo menos dos días de trabajo dedicado (Casey y Willis, 2008), con el fin de documentar y establecer los elementos suficientes para fundamentar el escenario de amenazas emergentes planteados, las vulnerabilidades conocidas o no documentadas, las brechas de capacidad que tiene la empresa frente a los escenarios conocidos y finalmente las acciones de mitigación, preparación o defensa requeridas para actuar y superar las posibles inestabilidades que puedan generar la materialización de dichos escenarios.

Juegos de guerra: cambios de perspectiva

La aplicación de los "juegos de guerra" en el contexto de las prácticas de seguridad de la información y ciberseguridad, establecen un planteamiento disruptivo que supera la visión de controles generales y sobre todo, la de riesgos particulares sobre el tratamiento de la información en la empresa. Este nuevo ejercicio de exploración y respuesta a la incertidumbre del entorno permite a la organización como a la seguridad de la información y a la ciberseguridad:

- Tener el tiempo para pensar y facilitar reflexiones de manera creativa

en torno de los desafíos de un contexto digitalmente modificado.

- Superar los límites de los estándares conocidos, con el fin de desafiar continuamente sus prácticas.

- Dialogar constantemente con el exterior, desconectando lo conocido para enriquecerlo con lo volátil, incierto, complejo y ambiguo.

- Aprender a generar valor más allá de los productos o servicios propios de la organización.

- Mejorar la capacidad de resiliencia de la organización frente a entornos inciertos y volátiles (Adaptado de: Ponti y Ferrer, 2011).

Por tanto, los "juegos de guerra" motivan de forma inteligente el uso de las habilidades emocionales y sociales de los participantes alrededor de los retos de la seguridad y ciberseguridad en entornos digitalmente modificados. Es en palabras de Bailey, Kaplan y Weinberg (2012) un "*mecanismo para establecer la prioridad de los activos a proteger, identificar, superar y cerrar las vulnerabilidades claves, identificar las fallas propias en la capacidad de respuesta ante un evento adverso y construir un tipo de 'memoria con músculo' necesaria para tomar decisiones apropiadas en tiempo real con información limitada*".

Así las cosas, esta práctica establece una forma de cambiar el imaginario de la seguridad de la información y la ciberseguridad que sugiere un espacio de construcción conjunta, donde los participantes se divierten trabajando en un ambiente de motivación, curiosidad y pasión que releva los matices propios de las prácticas de seguridad y control de la organización, no solo en su interior, sino como parte de la dinámica exterior empresarial que forma parte del ecosistema digital del cual es partícipe.

Los "juegos de guerra" no solo revelan problemáticas particulares de las amenazas digitales o impactos en los activos digitales críticos de las empresas, sino que dejan ver otros riesgos propios de los procesos de negocio, impactos no dimensionados sobre grupos de interés y aspectos inexplorados de las relaciones entre los procesos de negocio, que comunican vulnerabilidades o fallas existentes en las áreas corporativas que no se habían identificado (Casey, 2007).

Reflexiones finales

En el contexto empresarial, los "juegos de guerra" establecen una lectura proactiva y de construcción conjunta de las capacidades corporativas para anticipar y responder de la mejor forma a las inestabilidades del entorno de los negocios actuales.

A diferencia del ejercicio que se esboza en el escenario militar, el enemigo en un ambiente volátil, incierto, complejo y ambiguo ya no es conocido y mucho menos sus capacidades o armamento disponibles para comprometer los activos digitales estratégicos de la empresa. En este sentido, la práctica de gestión de riesgos tradicional se debilita, para darle paso a una nueva forma de aumentar la capacidad de visualización y entendimiento de los nuevos patrones de amenazas existentes que pueden afectar las promesas de valor de la empresa para con sus clientes.

En consecuencia, los "juegos de guerra" plantean un ejercicio diferente para motivar estrategias de protección del valor de los activos digitales empresariales, y provocar acciones creativas, orientadas a atender la incertidumbre natural de los entornos de negocios actuales, para concretar puntos de desconexión de los conceptos conocidos, con el fin de incorporar tendencias y rarezas del exterior, que permitan nuevas ganancias teóricas y prácticas en el entendimiento de los retos empresariales al interior.

Los "juegos de guerra" permiten validar concretamente los supuestos propios sobre las prácticas de seguridad y control vigentes en la empresa, con el propósito de hacer una declaración sincera sobre el nivel de exposición de sus activos críticos.

Se trata de comprender y declarar desde la inevitabilidad de la falla, la oportunidad para construir de forma colaborativa una nueva realidad de la protección del valor de la corporación, frente al reto de una acelerada digitalización de productos y servicios.

Los "juegos de guerra" permiten una democratización de la lectura de la protección de los activos digitales, que conjuga las perspectivas de las personas a cargo de los mismos, con la visión especializada de los analistas de seguridad de la información y ciberseguridad. En este ejercicio, no solamente se retan los supuestos de base de la seguridad y control actuales, sino que se habilitan espacios para compartir lecciones aprendidas en otras temáticas, que nutren el ejercicio como una estrategia para recolectar información y motivar analíticas de datos hacia el futuro.

Considerando la acelerada transición hacia la nueva revolución industrial, mediada por la digitalización de productos y servicios (Kane, 2017), para crear nuevas experiencias motivadas en los datos e información recolectada de los diferentes grupos de interés, los ejercicios de "juegos de guerra" igualmente deberán avanzar en sus desarrollos incorporando las posibilidades de simulaciones con el uso de inteligencia artificial, desarrollo de prototipos y juegos de roles que permitan entrenar a los participantes en las decisiones que deben tomar frente a momentos de incertidumbre y confusión total.

Este documento no pretende agotar las reflexiones sobre las nuevas formas de reconocer patrones emergentes en el entorno, pero sí es una excusa académica para pensar de forma diferente sobre el entendimiento de los nuevos desafíos del entorno y cultivar un diálogo creativo hacia el surgimiento de pensamientos no convencionales en seguridad de la información y ciberseguridad, que obliguen una mirada de la realidad a través de una óptica totalmente distinta, superando el temor a lo desconocido y rompiendo las barreras y supuestos de los estándares conocidos.

Referencias

[1] Bailey, T., Kaplan, J. y Weinberg, A. (2012) Playing war games to prepare for a cyberattack. *Mckinsey Quarterly*. July. Recuperado de: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/playing-war-games-to-prepare-for-a-cyberattack

[2] Cano, J. (2017) El riesgo geopolítico en clave de la seguridad y la ciberseguridad de las empresas modernas. Recuperado

de: https://www.linkedin.com/pulse/el-riesgo-geopol%C3%ADtico-en-clave-de-la-seguridad-y-las-cano-ph-d-cfe

[3] Casey, T. (2007) Threat Agent Library Helps Identify Information Security Risks. *Intel White Paper*. Recuperado de: https://communities.intel.com/servlet/JiveServlet/previewBody/1151-102-1-1111/Threat%20Agent%20Library_07-2202w.pdf

[4] Casey, T. y Willis, B. (2008) Wargames: Serious play that test enterprise security assumptions. *Intel White Paper*. Recuperado de: https://communities.intel.com/docs/DOC-1519

[5] Kane, G. (2017) Digital Maturity, Not Digital Transformation. *Sloan Management Review*. Blog. Recuperado de: http://sloanreview.mit.edu/article/digital-maturity-not-digital-transformation/

[6] Perla, P. (1990) *The art of wargaming: A guide for professionals and hobbyist*. USA: US Naval Institute Press

[7] Ponti, F. y Ferrer, J. M. (2011) *Si funciona, cámbielo. Cómo innovar sin morir en el intento*. Bogotá, D.C, Colombia: Grupo Editorial Norma.

[8] Prize, W. (2015) *1000 ideas para atraer lo que quieras a tu vida*. Madrid, España: Mestas Ediciones.

Jeimy J. Cano M., Ph. D., CFE. *Profesor Asociado, Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph. D. en Administración de Negocios de Newport University, CA. USA y Ph. D. (c) en Educación de la Universidad Santo Tomás. Obtuvo un Certificado Ejecutivo en Liderazgo y Administración del MIT Sloan School of Management y es egresado de los programas de formación ejecutiva de Harvard Kennedy School of Government: Liderazgo en el siglo XXI: Agentes globales de cambio y Ciberseguridad: Intersección entre política y tecnología, ambos en Boston, USA. Ha sido reconocido como "Cybersecurity Educator of the year 2016" para Latinoamérica, por Cybersecurity Excellence Awards. Es Examinador Certificado de Fraude – CFE por la ACFE y Cobit5 Foundation Certificate por ISACA. Cuenta con más de 20 años de experiencia como académico y profesional en seguridad de la información, auditoría de TI, forensia digital, delitos informáticos, privacidad y temas convergentes en Colombia y Latinoamérica y más de un centenar de publicaciones en diferentes eventos y revistas nacionales e internacionales.*

IoT: interconexión digital, un reto mayor de seguridad

Los cambios en los diferentes estilos de vida que conllevan los avances tecnológicos son abrumadores y las generaciones llegan a verlos reflejados en su diario vivir.

Joshsua J. González Díaz, MSc.

Introducción

En tiempos de cambio, quienes estén abiertos al aprendizaje se adueñarán del futuro, mientras que aquellos que creen saberlo todo estarán bien equipados para un mundo que ya no existe. Eric Hoffer.

La próxima era de Internet de las Cosas (IoT) borrará la línea entre nuestras vidas, en cuanto a la perspectiva del mundo físico y aquel al cual estamos conectados “en línea”. Los ataques dirigidos a nuestros espacios en la red, donde somos moradores ciberpespaciales, pondrán en peligro nuestra seguridad física, cosa que puede llegar a sonar como historia de ciencia ficción. Tradicionalmente, los vectores de ataque a nuestros lujos fundamentales tecnológicos han requerido manipulación física, sobre todo porque el acceso a la infraestructura se ha llega-

do a limitar desde Internet. Esto está a punto de cambiar con la participación causada por un futuro con miles de millones de "cosas" conectadas a Internet, y de cómo un ataque simple puede causar un apagón perpetuo de bombillas LED en una autopista, o de cómo las decisiones de seguridad mal tomadas pueden llegar a violar groseramente la seguridad física y la privacidad de las familias, o cómo la inseguridad de los vehículos eléctricos poderosos pueden poner su vida en riesgo y la sustracción de información mediante electrodomésticos altera su privacidad.

Existe un riesgo tangible en los dispositivos IoT y, cada vez, vamos a depender en mayor grado de la tecnología, a medida que avanza el tiempo. Una vez que comencemos a comprender la causa de las actuales vulnerabilidades de seguridad en los dispositivos de hoy, comenzaremos a establecer el camino para un futuro que nos ayudará a habilitar estos dispositivos para mejorar y aumentar de forma segura nuestras vidas.

Los atacantes maliciosos ya están trabajando en ello, descubriendo y explotando estos defectos de seguridad y seguirán encontrando formas astutas e inimaginables de abusar de sus conocimientos de todas las maneras posibles. Estos atacantes contemplan desde estudiantes universitarios curiosos a grupos delictivos y patrocinados por gobiernos u organizaciones al margen de la ley –y no propiamente nos referimos a grupos de *hacktivismo*–, interesados en aterrorizar a los individuos y/o poblaciones. El impacto de las vulnerabilidades de seguridad en los dispositivos IoT puede conducir a un compromiso masivo de privacidad y causar daño físico. Las apuestas son altas.

IoT es el futuro, el futuro de la industria, el futuro de las organizaciones y pro-

Ilustración 1. Se descubre un envío de electrodomésticos espía procedente de China. Disponible en: https://es.rbth.com/cultura/technologias/2013/10/30/se_descubre_un_envio_de_electrodomesticos_espia_proceden_33821

bablemente su futuro personal. Bienvenido al futuro. Se deletrea I-o-T. Todo esto puede parecer un 'bombo' ahora, pero al final resultará ser bastante discreto; IoT es muy, muy real.

Dispositivos *Wearables y Healthcare,* es más que estar a la moda

En muchos casos de historias de ciencia ficción, donde Hollywood mostraba cosas que llegaban a considerarse fantasiosas, como el hecho de que por medio de un reloj se pudiese uno comunicar, como era el caso de Dick Tracy, o la posibilidad que en este mismo dispositivo un agente espía extrajera herramientas para la consulta y robo de información, como era el caso del agente 007. Los dispositivos *wearables* (aquellos dispositivos electrónicos que pueden ser usados como parte de su vestimenta) es un tema que ha recibido la atención de muchos pioneros en tecnología, tal como lo llega a mostrar el nuevo desafío de "Make it Wearable"[1] de $ 5,000 publicado por Intel. Este desafío recompensa tanto a visionarios como a los constructores que conciben o construyen aplicaciones portátiles que pueden cambiar la computación personal en nuevas direcciones innovadoras. Los dispositivos *wearables* ahora están en el centro de casi todas las discusiones relacionadas con Internet de las cosas (IoT), y la gama completa de nuevas capacidades que la conectividad generalizada puede traer.

A menudo, algunas de estas discusiones crean más preguntas que respuestas. Tal vez eso es algo común, dado que todavía estamos en las primeras etapas de su ciclo de vida, pero algunas preguntas tienen que ser respondidas antes de un verdadero "despliegue" de dichos dispositivos. Por ejemplo, "¿Estos dispositivos van a ser sólo periféricos para un teléfono inteligente, o hay un papel más importante para ellos como parte de la Internet de las cosas?"

Una de las primeras funciones de los dispositivos, ya están relacionadas con la identificación y aún más sorprendente, con la seguridad. Quizás no considere que usted use en el trabajo un dispositivo *wearable*, pero estos pueden llegar a proporcionar características para su identificación y manejo de la seguridad dentro del ambiente laboral. Algunas configuraciones avanzadas incluyen algunas capacidades biométricas (como la activación mediante huellas dactilares, por lo que sólo el propietario del dispositivo pueden realizar acciones sobre este).

Existen implementaciones de estos dispositivos orientados a la salud y muchas veces a la actividad física, y ofrecen mediciones biométricas tales como frecuencia cardíaca, niveles de transpiración e incluso mediciones complejas como los niveles de oxígeno en el torrente sanguíneo. Los avances tecnológicos pueden permitir que los niveles de alcohol u otras similares se realicen a través de un dispositivo *wearable*. La capacidad de detectar, almacenar y rastrear mediciones biométricas a lo largo del tiempo y luego analizar los resultados, es sólo una posibilidad interesante. Y, más allá de un tipo de entretenimiento en actividad física, se encuentra esa línea

[1] Iniciativa dada por Intel, concurso que entregaba US$5.000ºº. Extraído de: https://newsroom.intel.com/chip-shots/chip-shot-nixie-wins-500000-grand-prize-in-intel-make-it-wearable-challenge/

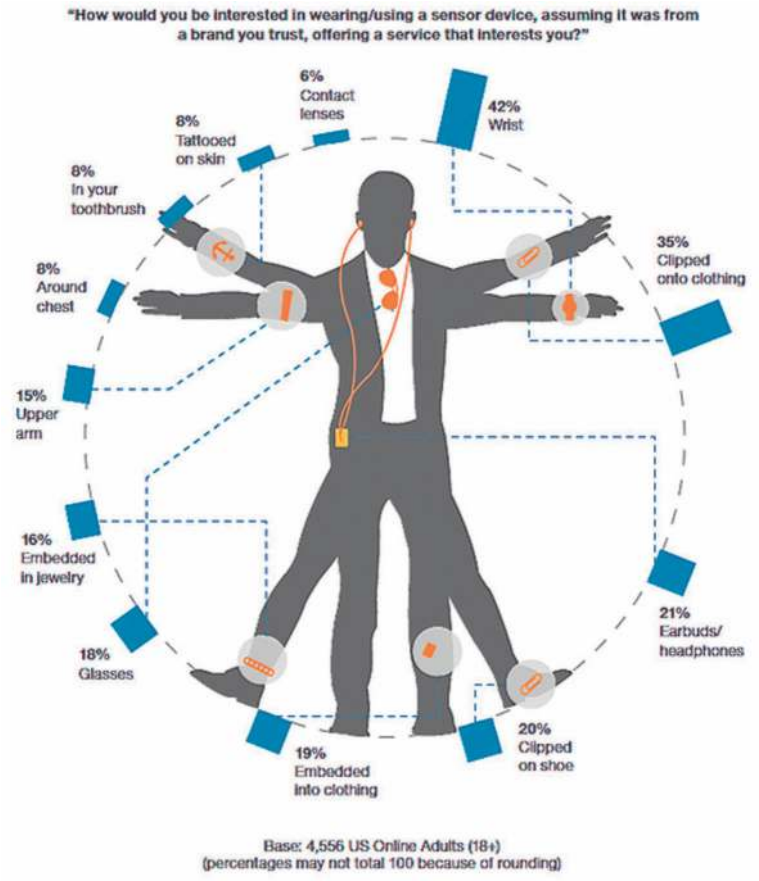


Ilustración 2. Extraído de North American Consumer Technographics Consumer Technology Survey 2014

de los dispositivos de *health-care* que llegan a basarse en un mismo principio de un dispositivo *wearable*, pero con fines de cuidado de la salud. Claro ejemplo de ello podría ser el seguimiento de la temperatura corporal, que al ser analizada podría proporcionar una indicación temprana de un resfriado.

Otras capacidades adicionales de los dispositivos usables son más mundanas, pero también pueden proporcionar información que podría ser útil para ajustar los controles ambientales. Los ejemplos anteriores podrían contemplar un teléfono inteligente como el control central para la entrega de estas capacidades, pero ¿es realmente el enfoque más eficiente? ¿Sería mejor si los dispositivos de Internet de Cosas (IoT) pudieran comunicarse directamente? Ciertamente, nadie quiere ser obligado a usar su teléfono inteligente para cada transferencia de información de sus dispositivos *wearable*. Tal vez un modelo mejor es que el teléfono inteligente puede ayudar a configurar los modos de operación, así como el nivel de privacidad que desea aplicar. Una vez que la comunicación "estratégica" está en su lugar, todos los dis-

positivos pueden comunicarse de la manera que se les ha permitido.

Veamos un ejemplo sencillo. Digamos que el reloj inteligente está captando sus lecturas biométricas para que pueda obtener una alerta temprana de una posible enfermedad (tal vez porque estaba en un avión). Supongamos además, que tomó el viaje de avión para una entrevista de trabajo y que está en su camino hacia su primera reunión. ¿Desea que sus lecturas biométricas estén disponibles para la persona que realiza la entrevista? Probablemente no. ¿Sería posible utilizar el teléfono inteligente para proteger las lecturas biométricas en tiempo real (y cualquier historial de lecturas) del acceso del entrevistador? Alternativamente, si su reunión no fue para una entrevista de trabajo, sino un chequeo anual de su médico, usted querrá permitir el acceso a todos sus datos biométricos.

Los dispositivos *wearables* le podrían permitir conectarse automáticamente a dispositivos alrededor de la casa también. Un posible escenario sería la preferencia de iluminación preferida cuando se use la televisión según la ubicación dentro de la sala. Usted podría encender el televisor y su dispositivo portátil podría ayudar a ajustar el nivel de iluminación de las luces LED conectadas dentro de la habitación. Una casa inteligente podría incluso soportar el bloqueo automático de la luz de las ventanas que creaban reflejos en el televisor. Incluso la retroiluminación en la pantalla del televisor LCD se puede ajustar y todos los ajustes optimizados para ahorrar energía, así como la creación de la experiencia de visualización más favorable. Todas estas interacciones podrían hacerse de forma automática, directamente entre dispositivos, una vez que la estrategia global se ha establecido a través de una interfaz de teléfono inteligente.

Una tecnología que abusa de su iniciativa

El apagón del año 2003 fue generalizado y afectó a las personas a lo largo de partes del noreste y medio oeste de los Estados Unidos y Ontario. Aproximadamente, 45 millones de personas fueron afectadas durante dos días. Sólo en Nueva York, fueron reportadas 3.000 llamadas de incendios, debido a incidentes relacionados con individuos que usaban velas. Hubo 60 casos de incendios de alarma que fueron causados por el uso de velas y dos casos de muerte. En Michigan, las velas encendidas que fueron olvidadas causaron un fuego fatal que destruyó una casa.

La cuestión sorprendente no es que se produjera el apagón del noreste, sino cómo el mundo desarrollado depende de la electricidad. De la misma manera, giramos un interruptor y esperamos el resplandor instantáneo de la 'llama eléctrica'. Abrimos la nevera y esperamos que nuestra comida y bebidas nos esperen a la temperatura adecuada. Caminar hacia nuestras casas y esperar que el aire acondicionado mantenga de forma continua y automática un equilibrio cómodo entre las temperaturas fría y caliente. Han pasado aproximadamente 100 años desde que descubrimos cómo generar electricidad. Antes de eso, las casas estaban encendidas con lámparas de queroseno y calentadas con estufas. Nuestro nivel actual de dependencia de la electricidad es fenomenal; las ciudades y negocios se detienen en segundos por un apagón.

Ahora con el uso de tecnologías de IoT para la automatización de este tipo de servicio, los dispositivos IoT que controlan la iluminación deben incluir la seguridad como parte de su arquitectura y diseño. El sistema de iluminación de tonos de Philips es uno de los dispositivos IoT más populares del mercado actual y ha presentado varios problemas de seguridad, incluyendo cuestiones fundamentales como la seguridad con contraseña y la posibilidad de que el *malware* abuse de los mecanismos de autorización débiles para causar apagones sostenidos. Por otro lado, la complejidad de interconexión con nuestro espacio ciberespacial (Facebook) con dispositivos IoT que utilizan servicios como IFTTT son servicios útiles y permitirán nuestro futuro automatizado, pero es necesario pensar en las implicaciones de las cuestiones de seguridad y privacidad.

Se ha descubierto que una partida de aparatos eléctricos enviados a San Petersburgo desde China servían también como terminales de espionaje. Se colocaron chips especiales en planchas y hervidores de agua, que se pueden conectar a la red y son capaces de expandir virus y spam. Los equipamientos se conectan vía wifi a cualquier ordenador no protegido en un radio de 200 metros[2].

Los empresarios recibieron ayuda de miembros de la aduana para descubrir los productos “espía”. Antes de ser enviados desde China a los rusos les extrañó el peso de los aparatos, que difería ligeramente con lo apuntado en los documentos. La partida se detuvo en la frontera y fue examinada por expertos en electrónica. Se descubrió que tenían incorporados chips diseñados para distribuir spam y virus informáticos.

Sin embargo, alrededor de 30 planchas, hervidores de agua, teléfonos y cámaras de vídeo del lote inspeccionado han sido distribuidas en tiendas de San Petersburgo. No está claro si esta tecnología ha llegado también a otras regiones de Rusia[3].

[2] Jamy Tostadora: N Brunstein diseñó un concepto de tostadora llamada "Jamy Toaster", que utiliza el Wi-Fi al centro meteorológico para averiguar el pronóstico del tiempo. Y cuando tuesta un pedazo de pan para el desayuno 'imprime' el pronóstico del día sobre el mismo.

[3] Extraído de: https://es.rbth.com/cultura/technologias/2013/10/30/se_descubre_un_envio_de_electrodomesticos_espia_proceden_33821

Ilustración 3. JAMY TOASTER, Tostador inteligente predicción estado del tiempo.

El poder de IoT radica en parte, en su capacidad de operar no sólo en el mundo físico de las cosas reales, sino también en el mundo virtual, donde las cosas se digitalizan y sólo existen como información digital. Debido a que atraviesa ambos mundos, IoT puede enviar datos digitales a través de la red a un controlador distante conectado a un dispositivo físico, por ejemplo una máquina de producción importante.

Dichos datos entonces indican a la máquina que se apague o encienda, dependiendo de lo que usted quiera que haga.

Pensemos un momento en esto: se tiene un sistema virtual que controla remotamente una máquina física. ¿Puede ver por qué la seguridad es tan importante para IoT? Sin un enfoque de seguridad eficaz, un *hacker* podría apagar una pieza importante de un equipo de producción y mantenerlo apagado, tal vez en algún momento crítico de producción.

Es posible que ni siquiera sepa que el problema existe e intente volver a conectar la máquina hasta que descubra que la producción se ha detenido y envía físicamente a alguien a la máquina para reiniciarla en forma manual.

El ataque de Stuxnet, donde el gusano penetró inicialmente en una instalación nuclear iraní, llevó a las máquinas a un sobrecalentamiento más allá del punto de ruptura, cerrando la producción durante meses. Se extendió a través de las operaciones industriales en muchos países, lo que llevó a las personas de sistemas a implementar medidas para prevenir incidentes de tipo Stuxnet.

A falta de detalles sobre cómo el ataque realmente funcionó, se apresuraron a soluciones rápidas como el despliegue de *Firewalls* frente a los equipos en el taller. Desde entonces, la industria ha aprendido que los *Firewalls* tradicionales son un sobrante de la era de la defensa perimetral de TI, que nunca detendría un ataque de este tipo.

La seguridad como un desafío más para la gestión de riesgos

El proceso para gestionar los riesgos de seguridad de IoT es el mismo que para cualquier otro riesgo:

- Identificar las posibles amenazas individuales.
- Evaluar cada amenaza en términos de su probabilidad de ocurrir y el daño que puede causar.
- Identificar y desplegar medidas defensivas adecuadas a la probabilidad de cada riesgo y posibles daños.

Diferentes tipos de vulnerabilidad producen diferentes amenazas con el potencial de diferentes daños. Una amenaza que potencialmente puede apagar una línea de montaje de fábrica o una plataforma petrolera es de una magnitud diferente a la de una amenaza que puede interferir con un proceso de almacenamiento del inventario. Mediante la evaluación del valor en riesgo, es posible tomar decisiones informadas sobre cuánto invertir en medidas defensivas. De esta manera, invertir en seguridad IoT no es diferente de comprar cualquiera de los diferentes tipos de seguros que la organización necesita. En todos los casos, la inversión debe ser proporcional a la probabilidad del riesgo y al valor potencial de la pérdida o daño.

Las compañías han estado desplegando con éxito IoT bajo diversos nombres por años. Sí, hay riesgos serios, sin embargo la industria ha estado ocupada desarrollando estrategias defensivas y participando en esfuerzos colaborativos para contrarrestar varios riesgos con métodos defensivos, productos y mejores prácticas. Todo comienza con una sólida identificación, evaluación y gestión del riesgo.

Sin embargo, es importante entender que IoT no tiene una estrategia mágica de seguridad. El alcance y la variedad de soluciones IoT evitan eficazmente la aparición de una defensa de seguridad sin fallos. La tecnología IoT está cambiando en forma constante, las soluciones están evolucionando continuamente, y también las amenazas y los vectores de ataque. Usted está tratando con adversarios activos que trabajan en forma permanente para ser más astutos que usted y sus defensas. No es una solución única, y tampoco es su defensa. La gestión de riesgos, como he dicho, es un proceso continuo que debe revisarse al menos una vez al año –quizás con mayor frecuencia–, a medida que cambian las soluciones y surgen nuevas amenazas. La clave para todos nosotros es ser inteligentes y conscientes de los riesgos de TI, y no tener miedo.

Hay muchas razones por las que alguien 'hackearía' una solución IoT. Para algunos, es un acto de exploración de nuevas tecnologías y para unos pocos un acto de guerra o terror. La mayoría –sospecho–, está esperando ganancias financieras al robar datos o secretos comerciales para obtener ventaja competitiva, las razones son tan numerosas y variadas como las tramas de la televisión de muchos programas policiales y del crimen. Una conclusión particular de años de estudios de seguridad es clara: la mayoría de las brechas de seguridad se aprovechan de vulnerabilidades bien conocidas que no se han resuelto a pesar de las amplias alertas, y la mayoría de los atacantes son conocidos por usted, empleados, contratistas o socios de un tipo u otro. En general, los ataques no son ni esotéricos ni exóticos.

La seguridad se ha convertido en uno de los principales inhibidores de la adopción de IoT [4]. Un modelo de separación física de dispositivos es algo inaudito de aplicar, todo debe estar conectado. ¿Cuánto tiempo podría funcionar una organización si el correo electrónico e Internet no estuvieran disponibles? Todo, prácticamente todos los procesos de negocio, dependen de la capacidad de conectarse. Hoy en día, la idea de desconectar una organización de la red global es simplemente absurda.

La verdad es que no todas las amenazas son las mismas y no todas las amenazas tienen el mismo valor para una organización. Su respuesta a diferentes tipos de amenazas y objetivos de amenazas diferentes debe ser medida y proporcional. Por eso –aunque suene a algo que muchas personas en seguridad llegan a predicar y no aplicar– esto requiere la gestión de riesgos.

Desafíos de la seguridad de IoT

El desafío número uno en la gestión de riesgos y la evaluación de amenazas es la gran escala esperada de IoT. Hablamos de los miles de millones de dispositivos conectados. Por supues-

to, muchas organizaciones no tendrán miles de millones de dispositivos conectados. Sin embargo, no tiene que ser un negocio muy grande para encontrarse con un millón de dispositivos conectados, especialmente si se incluyen todos los de sus empleados y otros. Incluso si usted tiene sólo unos miles de dispositivos conectados, representa mucho más, para tratar de manejar el desafío de seguridad sin herramientas automatizadas de análisis, monitoreo y mucho más. Sólo un millar de dispositivos conectados pueden generar corrientes masivas de datos de 24 × 7, así como un gran número de alertas que afectarán cualquier cosa, excepto herramientas automatizadas e inteligentes (basadas en reglas o basadas en políticas) y tecnología [3].

Además, la seguridad encuentra la amplia variedad de dispositivos, incluyendo diferentes tipos de controladores, monitores, medidores y aparatos. Muchos de estos dispositivos pertenecerán a sus empleados, por lo que probablemente tendrán un conocimiento limitado de lo que son y lo que hacen, sin mencionar cómo entender y comunicarse entre ellos.

Mejores prácticas de seguridad

Las prácticas de seguridad de IoT siguen evolucionando. El diseño (arquitectura) y la construcción de una estrategia integrada (holística), debe incluir seguridad desde el principio. No deje la seguridad como un cerrojo al final. Debe ser inherente en su proceso de IoT desde el principio.

Adopte estándares apoyados por la industria, los enfoques patentados minimizaran sus esfuerzos de seguridad en el futuro. Consultar cuando sea necesario los organismos de normalización, así sean asociaciones comerciales, para obtener orientación.

Implemente la seguridad en todas partes: desde el centro de datos central detrás y fuera del *firewall* corporativo y hasta los dispositivos de borde, que en este caso serían aquellos que hemos discutido. Esto significa insistir en que sus empleados y proveedores participen y colaboren en su estrategia de seguridad.

Automatice y monitoree la seguridad de IoT de extremo a extremo. Construir modelos que incluyan análisis predictivo, especialmente analítica basada en la nube. Alertar a la gente para que tome medidas, tan pronto como los problemas se vuelvan evidentes. Los esfuerzos manuales serán rápidamente inundados y rebasados por el volumen de la actividad de IoT, incluso en una pequeña organización.

Segmente el tráfico IoT y el tráfico regular de la red de TI y utilice una infraestructura de red *multitenant* para aislar los problemas. Use segmentación y otros procesos bien conocidos, pero al mismo tiempo trabaje con los proveedores de TI para expandir su *software* y herramientas existentes para manejar vulnerabilidades de seguridad IoT. No se trata de difamar a los diferentes fabricantes y proveedores, pero resista la tentación de implementar herramientas específicas de IoT.

Para finalizar quisiera proponer como un primer paso para afrontar el tema de seguridad frente a IoT: evaluación y monitoreo de riesgos informados, acompañado de una respuesta de seguridad apropiada y proporcional, que

explique el nivel de amenaza específico y la cantidad de valor en riesgo. Los riesgos tenderán a ser similares, solo que utilizan un tipo de tecnología diferente.

Una vez que determine esto, puede elegir la mejor opción de proveedor entre las soluciones de seguridad IoT más apropiadas y construirlo en su ecosistema de IoT desde el principio de manera segura. Otra opción emergente que vale la pena considerar es una póliza de seguro cibernético que algunas compañías de seguros están comenzando a ofrecer. Después de eso, sólo hay un paso final, pero importante: involucrar a sus altos ejecutivos y obtener su apoyo, porque ninguno de ellos querría que su empresa aparezca como una víctima de ciberataque de IoT en la portada de un periódico.

Referencias

[1] Irvine, Cynthia (2014) *Security Education and Critical Infrastructures*.

[2] Ventre, Daniel (2015) *Chinese Cybersecurity and Defense*. Wiley 1st Edition,

[3] Maciej, Kranz (2017) *Building the Internet of Things*. Wiley 1st Edition,

[4] Dhanjani, Nitesh (Early Release – 2017) *Abusing the Internet of Things*. O'Reilly 1st Edition

[5] Pfister, Cuno (2011) *Getting Started with the Internet of Things* O'Reilly

[6] Gragido, Will & Pirc, John (2011) *Cybercrime and Espionage*. Syngress

[7] Andress, Jason & Winterfeld Steve (2011) *Cyber Warfare*. Syngress

Joshsua J. González Díaz, MSc. *Ingeniero de Sistemas de la Pontificia Universidad Javeriana, especialista en seguridad de la información de la Universidad de los Andes, Especialista en Derecho Informático de la Universidad Externado de Colombia y Magíster en Seguridad de la Información de la Universidad de los Andes. Actualmente, se desempeña como profesor instructor de la maestría en Seguridad de la Información en la Universidad de Los Andes y CEO de la empresa de consultoría Stark Industries SAS.*

Electronic Game Developers Congress

VI Versión del EGDC

Electronic Game Developers Congress

¿Qué es el EGDC ?

Es una iniciativa de la revista La revista Gamers-on, creado en el 2010 (antes llamado Anigames-expo) con el objetivo de promover y fomentar el desarrollo económico de la industria del entretenimiento digital, aplicaciones y videojuegos en Colombia y América Latina, creando un espacio académico de integración y de negocio.

En el EGDC se reunirán los principales exponentes de la industria del entretenimiento digital y videojuegos, para tocar temas como: Inteligencia Artificial, Big Data, Realidad virtual y aumentada, tecnología, e-sport, innovación, novedades en marketing, negocios entre otros.

Este año en asocio con la Universidad Central, Universidad Jorge Tadeo Lozano y la universidad Militar son los organizadores de la VI versión del EGDC Electronic Game Developers Congress.

El congreso ha traído al país a los principales exponentes de la industria del entretenimiento digital y los videojuegos; y nos han apoyado importantes empresas privadas y gubernamentales: que han permitido su desarrollo y ejecución en la capital del país de forma exitosa, convirtiéndose en el evento académico y de negocios de TI, más importante del país En la promoción y desarrollo de videojuegos.

Durante 3 días será el escenario más importante para conocer y comprender la visión del futuro de estas industrias así, como sus novedades en marketing, negocios, tecnología e innovación.

¿Cuándo? Bogotá Agosto 10-12 2017. EGDC reúne a los principales exponentes de la industria del entretenimiento digital y video juegos en un solo Lugar

Compra tu entrada en: https://goo.gl/GkaPte

Más información en: http://bit.ly/2rmTfKT

GAMERSON

AREA51 TRAINING CENTER

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

UNIVERSIDAD CENTRAL

UNIVERSIDAD MILITAR NUEVA GRANADA

UTADEO
UNIVERSIDAD DE BOGOTÁ JORGE TADEO LOZANO

BOGOTÁ MEJOR PARA TODOS
ALTA CONSEJERÍA TIC

globaltek
SECURITY

1995 - 2017

Cumplimos 22 años de experiencia en la ejecución de proyectos de Seguridad de la Información y protección de activos digitales

Usted ya nos conoce

Numerosas organizaciones del sector público y privado en Colombia y en Latinoamérica, han confiado en la experiencia que GLOBALTEK SECURITY ha demostrado a través de los años, que la cataloga como una compañía estructurada y bien preparada para el desarrollo de proyectos e implementación de servicios tendientes a la protección de los activos digitales y los datos sensibles.

Contáctenos, somos su aliado en soluciones y proyectos de Seguridad de la Información.

FORCEPOINT Platinum Partner

SOPHOS Platinum Partner

ALIEN VAULT Certified Partner

Sede Administrativa: Calle 23 G No. 81-76 Bogotá - Colombia PBX: (571) 410 80 04

Oficina USA: 1901 Cedar Ct - Weston, FL 33327, Phone: (1) 954-302 2785

www.globalteksecurity.com