Unidad 4 / Escenario 8

Lectura fundamental

Innovación en Seguridad de la información: un reto para las nuevas tendencias de TI

Contenido

Palabras clave: seguridad, nuevas tendencias, espionaje digital, vigilancia digital, innovación en seguridad.

Nos encontramos en la Era Digital, la cual se encuentra altamente influenciada por las tecnologías de la información. Temas como *big data*, IoT y ciberseguridad no son del todo ajenos a la cotidianidad. Sin embargo, su exponencial evolución también ha generado inquietud en asuntos como la seguridad, puesto que los desarrollos de las tendencias en relación con esta no han ido al mismo ritmo y, hoy en día, la seguridad para nuevas tendencias es un reto.

Como se anuncia en diferentes estudios, la transformación digital se está convirtiendo en una estrategia empresarial fundamental. Hace un par de años, este tema generaba proyectos algo aislados en las organizaciones. Hoy en día, podemos identificar que las empresas desde su creación son "digitales".

En este Escenario se exponen algunas de las tendencias de TI, los retos en seguridad para estas tendencias y el papel de la innovación para acelerar el proceso de protección de la información que inevitablemente utilizarán dichas tendencias.

1. Nuevas tendencias: *cloud*, *big data*, IoT

Las nuevas tendencias de TI se encuentran relacionadas entre sí, lo cual genera un ambiente interesante para los temas de seguridad, puesto que se ha identificado que se requerirá de una plataforma *cloud* para su desarrollo y contar con el respaldo de la ciberseguridad.

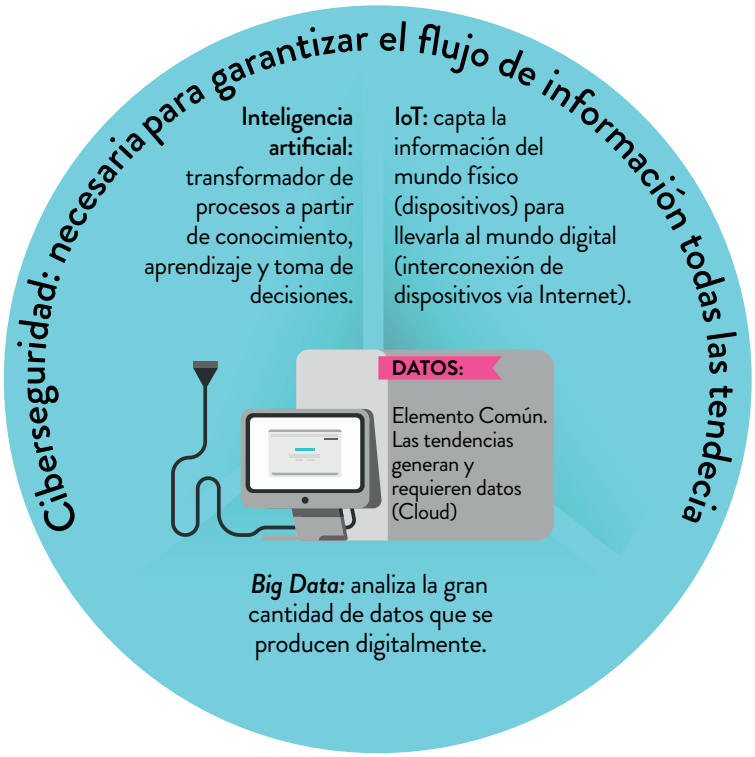

Figura 1. Relación nuevas tendencias de TI

Fuente: elaboración propia

Como todos sabemos, los servicios de *cloud computing* permiten almacenar, modificar y acceder a recursos tales como datos, programas y aplicaciones a través de Internet. Cuentan con grandes beneficios como mayor flexibilidad (permite el acceso al recurso en todo momento) y accesibilidad (se puede acceder al recurso desde diferentes dispositivos en cualquier lugar, facilita la expansión de una empresa a otro país o región y facilita el análisis de datos que provienen de diferentes orígenes en tiempo real).

Según la encuesta sobre el uso de TIC y comercio electrónico en las empresas de INE, Instituto Nacional de Estadística de España, en el año 2016 se produjo un aumento importante en el porcentaje de empresas que adquirieron algún servicio *cloud computing*. Según la encuesta, en el año 2014 un 15 % de las empresas utilizaban el servicio, mientras que para el año 2016 el 19,3 % lo usaron. Adicionalmente, se encontró que las empresas que más demandan estos servicios son empresas grandes de más de 249 empleados. Sin embargo, empresas de menos de 10 empleados también han empezado a utilizar los servicios cloud, especialmente para el correo electrónico, repositorio de datos y aplicaciones propias para las empresas, como la facturación ERP y CRM, entre otros (Ametic - Madison Market Research, 2016).

El principal reto que presenta la tendencia es el tema de seguridad. Aunque los servicios cloud mejoran la percepción de disponibilidad, principio esencial de seguridad de la información, temas como la confidencialidad se ven altamente comprometidos, especialmente en el robo y uso de información personal (Ametic - Madison Market Research, 2016).

1.1. Big data

Se denomina *big data* a la gestión y análisis de grandes volúmenes de datos provenientes de diferentes fuentes, canales y sistemas digitales mediante tecnologías escalables de computación y almacenamiento de nueva generación (Ametic - Madison Market Research, 2016).

Según el informe anual la sociedad en red del Gobierno de España, para el año 2016, aproximadamente el 2.7 % de las microempresas analizadas utilizaban *big data* para el desarrollo de sus actividades. Aunque la cifra no es significativamente alta, es interesante que empresas de menos de 10 empleados mencionen el uso del *big data* para el desarrollo de sus negocios (Ametic - Madison Market Research, 2016).

Adicionalmente, hoy en día se habla de la cadena de valor digital centrada en el análisis y uso de datos. En la Figura 2 se presenta el resumen de este concepto:

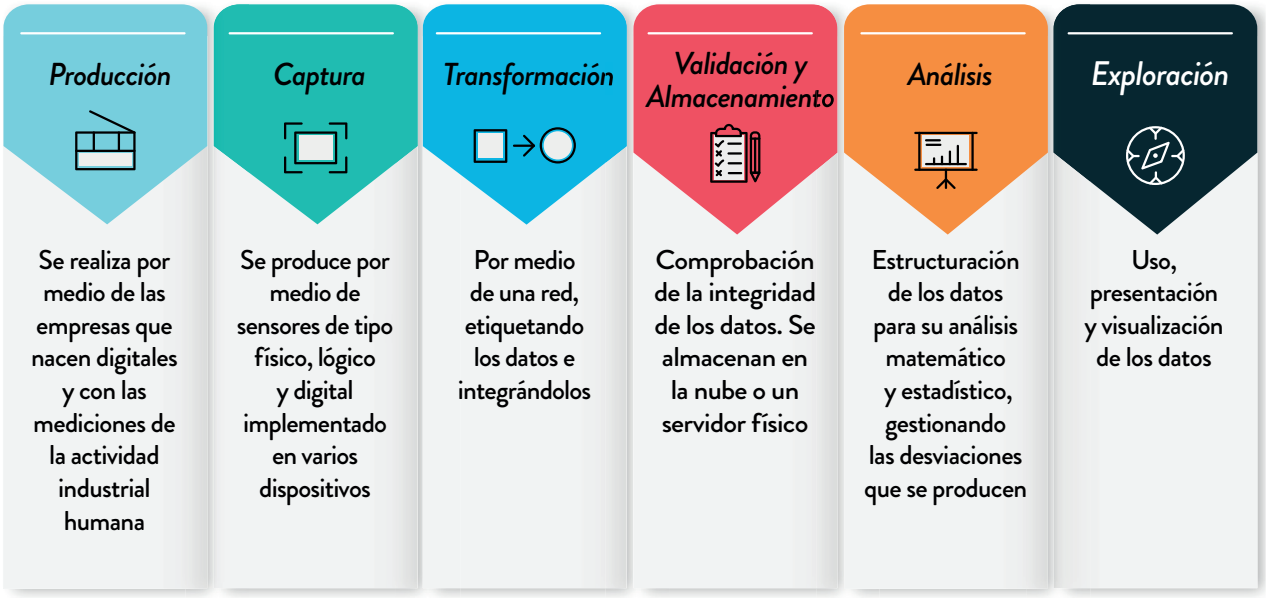

Figura 2 Cadena de valor digital (datos)

Fuente: elaboración propia

Al igual que la tendencia *cloud*, el principal reto es ciberseguridad, de la cual se espera avance a la misma velocidad que está creciendo *big data* en los diferentes sectores.

1.2. IoT

Internet de las cosas (IoT por sus silgas en inglés *Internet of the things*) hace referencia a la conexión y comunicación de objetos de todo tipo a través de Internet.

Las ventajas que reporta el IoT para generar acciones preventivas son numerosas; entre ellas están la conexión de múltiples dispositivos, mejorar la calidad de vida del mundo entero, tomar decisiones que faciliten la gestión empresarial, entre otros (Ametic - Madison Market Research, 2016).

El valor del IoT radica en la información recolectada. Esta información, con uso de *big data*, por ejemplo, que la depura y la entrega en formatos más asequibles para la toma de decisiones, puede ser utilizada también en el desarrollo de nuevos proyectos y de modelos de negocio con procesos automatizados, por ejemplo (Ametic - Madison Market Research, 2016).

El principal reto al que se enfrenta IoT es garantizar la seguridad, especialmente la confidencialidad de los datos. Lo anterior, por las aplicaciones en sectores como la salud, en la cual se espera brindar mejor calidad de vida a pacientes mayores de edad, crónicos etc.

1.3. Inteligencia artificial

La inteligencia artificial tiene como objetivo emular el comportamiento humano (aprendizaje, capacidad para concluir, comprensión, desarrollo del lenguaje y la comunicación con personas) y mejorarlo (computación cognitiva).

Las tecnologías basadas en la inteligencia artificial se están aplicando a la predicción de comportamientos en contextos conocidos. Estos análisis predictivos se utilizan en una gran variedad de áreas como *marketing*, operaciones, TI, ventas, finanzas y recursos humanos.

El principal reto de la inteligencia artificial es tomar decisiones a partir de datos no estructurados que generan conocimiento y aprendizaje para la máquina (Ametic - Madison Market Research, 2016).

1.4. Ciberseguridad

Como se analizó en el Escenario anterior, la ciberseguridad es importante para la economía digital. En las tendencias en el sector de las TI anteriormente mencionadas (*cloud*, *big data*, IoT e inteligencia artificial), existen vulnerabilidades y amenazas que la ciberseguridad debe atender.

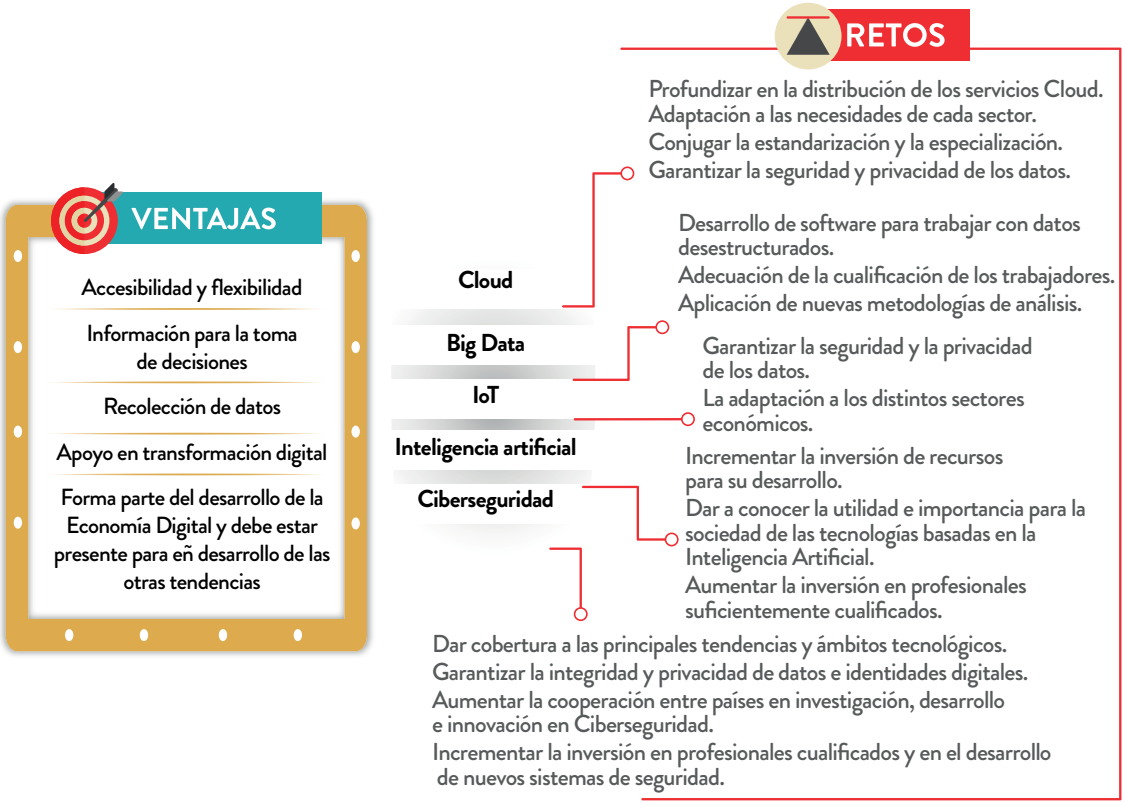

Figura 3. Resumen de ventajas y retos tendencias de TI

Fuente: elaboración propia

Los datos producidos por el IoT almacenados en la *cloud* y analizados por el *big data* son objetivos de ciberamenazas, principalmente por la conexión a internet que demandan.

2. Seguridad de nuevas tendencias de tecnología (*cloud*, *big data*, IoT)

Son evidentes las ventajas de la tecnología en la era digital. Sin embargo, el tema de seguridad es una gran preocupación para el buen uso de las tendencias mencionadas anteriormente, puesto que su evolución y su correspondiente seguridad no han sido paralelas.

En este sentido, es importante conocer los aspectos que cada tendencia TI debe considerar para mejorar la sensación de seguridad.

2.1. Cloud computing

Los principales riesgos relacionados con la computación en la nube surgen de la dependencia de internet, la concentración de datos y los contratos mal ejecutados. Esto desde el punto de vista de usuarios del servicio de la nube.

La dependencia de internet es un riesgo que parece inevitable en el mundo de los negocios digitales de hoy. Una interrupción de Internet puede prevenir y retrasar funciones comerciales, y causar problemas importantes para los clientes. Una organización que depende de los proveedores de la nube también confía en un tercero para salvaguardar sus datos centralizados. Si la red del proveedor de la nube se ve comprometida, esto podría provocar la pérdida de acceso del cliente a los datos, lo que daría lugar a una reputación dañada. Usar un proveedor de la nube que no proteja adecuadamente los datos puede tener consecuencias negativas para las organizaciones, los empleados y los clientes. Un riesgo adicional puede surgir de contratos de servicio débiles con un proveedor de la nube (Antonucci, 2017).

Por esta razón, antes de contratar un servicio en nube, es importante validar la reputación del proveedor, confirmar, si es posible, qué elementos de seguridad ha utilizado para el *hardware* y *software* que utiliza, es decir, los elementos de seguridad física, lógica y de aplicaciones.

2.2. Consideraciones para seguridad física

- Las principales consideraciones para temas de seguridad física hacen referencia a planeación, protección de la vida humana e identificación de zonas seguras que permitan crear perímetros de seguridad para el acceso.
- En temas de planeación, la recomendación principal es realizar programas de seguridad física con temas referentes a prevención de delitos, utilizando herramientas como CPTED, por sus siglas en inglés.

Esta metodología se ha utilizado con éxito en la planeación de ciudades y combina el entorno físico y los problemas de sociología que lo rodean para reducir las tasas de delincuencia y el miedo al delito. En términos de empresa, se debe garantizar que una solución IoT haya identificado zonas seguras que preferiblemente se construyan bajo las buenas prácticas CPTED.

- Se debe determinar el valor de la solución y el costo de la instalación física que la alberga con el fin de identificar la relación costo beneficio de la seguridad. Es decir, si es conveniente aplicar un control de seguridad porque resulta más económico que el potencial robo.
- Los controles ambientales automatizados contribuyen en el tratamiento del riesgo, en la medida en que pueden reducir el daño efectuado. Por el contrario, los controles de tipo manual pueden consumir más tiempo, son propensos a generar más errores y requieren atención constante.
- Cierto tipo de controles utilizados para la seguridad física pueden afectar la integridad de las personas. Estos problemas deben ser tratados, puesto que la principal premisa de la seguridad física es que la vida humana está por encima de la protección de una instalación o los activos que contiene.
- La ubicación de una empresa debe considerar aspectos tales como el delito local, las posibilidades de desastres naturales y la distancia a hospitales, a estaciones de policía y bomberos y aeropuertos, entre otros (Harris, 2013).

2.3. Consideraciones para seguridad lógica

- Es importante contar con personal capacitado y con pleno conocimiento en temas de redes, sistemas operativos, bases de datos y aplicaciones.
- Se deben aplicar defensas a nivel lógico como lo son *firewall*, *proxy* e IPS que facilitan el control de acceso a Internet.
- Se debe garantizar VPN con un alto nivel de seguridad en temas de encriptación de datos y de canales.
- Comprender las nuevas tendencias de ataques como los son lo APT (amenaza persistente avanzada).

2.4. Consideraciones para seguridad en las aplicaciones

- La seguridad debe abordarse en cada fase del desarrollo del sistema y no solo al final de este, ya que esto último implicaría costo, tiempo y esfuerzo adicionales, y no sería funcional.
- Los sistemas y aplicaciones pueden usar diversos modelos de desarrollo que emplean diferentes ciclos de vida; no obstante, todos los modelos contienen iniciación de proyectos, análisis y planificación de diseños funcionales, especificaciones de diseño de sistemas, desarrollo de *software*, instalación, operaciones y mantenimiento, y eliminación de alguna forma o manera.

- El control de cambios debe establecerse al comienzo de un proyecto y debe hacerse cumplir a través de cada fase. Los cambios deben ser autorizados, probados, y grabados; estos no deben afectar el nivel de seguridad del sistema o su capacidad para hacer cumplir la política de seguridad.
- El marco del ciclo de vida de desarrollo del sistema (SDLC) proporciona una secuencia de actividades para que la sigan los diseñadores y desarrolladores de sistemas. Consiste en un conjunto de fases en las que cada una usa los resultados de la anterior, con el objetivo de crear resultados de calidad.
- ISO/IEC 27002 tiene una sección específica que trata sobre los sistemas de información, específicamente sobre su adquisición, desarrollo y mantenimiento. Proporciona orientación sobre cómo construir seguridad en las aplicaciones.
- El estándar ISO/IEC 27034 cubre los siguientes conceptos: descripción y conceptos de seguridad de aplicaciones, marco normativo de organización, proceso de gestión de seguridad de aplicaciones, validación de seguridad de aplicaciones, estructura de datos de control de seguridad de aplicaciones de protocolos y orientación de seguridad para aplicaciones específicas.
- Web Application Security Consortium (WASC) y Open Web Application Security Project (OWASP) son organizaciones dedicadas a ayudar a la industria a desarrollar *software* más seguro.
- CMMI (Capability Maturity Model Integration) es un modelo que proporciona a las organizaciones los elementos esenciales para los procesos, no solo operacionales, que mejoran su rendimiento. El modelo CMMI usa cinco niveles de madurez designados por los números 1 hasta 5. Cada nivel representa el nivel de madurez de la calidad y optimización del proceso. Los niveles están organizados de la siguiente manera: 1 = Inicial, 2 = Administrado, 3 = Definido, 4 = Gestionado cuantitativamente, 5 = Optimización (Harris, 2013).

2.5. IoT

Una empresa que desarrolle y/o implemente IoT para su propio negocio debe garantizar a sus usuarios internos y externos la privacidad de los datos y el transporte seguro de los dispositivos conectados.

Para ello se recomienda diseñar una política especial de IoT que esté amparada por el sistema de gestión de seguridad de la empresa:

- Identificar a todos los interesados (reguladores, individuos, aquellos que usan los dispositivos, miembros del público, propietarios de datos).
- Identificar los peores escenarios posibles.
- Cifrar datos del centro de datos al punto final.
- Segregar la red de IoT de los datos corporativos críticos.

- Identificar y asignar (lo mejor que se pueda) todos los dispositivos que están conectados al dispositivo o dispositivos que se venden, por ejemplo, a clientes; en particular, cómo recopilan datos, cómo se comunican entre sí y cómo estos enlaces están protegidos.
- Diseñar políticas enfocadas en la recolección, el uso y la protección apropiados de los datos del consumidor.
- Documentar los usos permitidos. Asegurarse de que otras organizaciones que tienen redes que se conectan con los dispositivos de una empresa tengan un conjunto claro de pautas para el uso de estos.
- Restringir el uso en las aplicaciones y definir la responsabilidad dentro de los contratos.
- Instalar el mejor *software* para *firewall* y antivirus, y auditar a fondo las políticas y prácticas de seguridad de los proveedores (Antonucci, 2017).

2.6. Big data

Al utilizar Cloud como plataforma para su desarrollo, la tendencia *big data* debe seguir las recomendaciones brindadas anteriormente.

Adicionalmente, se deben tener en cuenta las siguientes consideraciones:

- Redundancia de datos: eliminar datos redundantes, es decir, datos que ya no son relevantes para fines analíticos.
- Antivirus: adoptar la mejor protección contra virus, asegurando la aplicación de actualizaciones de manera manual o automática.
- Cifrado: cifrar datos tanto en reposo como en tránsito. Los datos en reposo suelen ser aquellos que no se mueven y, generalmente, son datos que se almacenan en una copia de seguridad. Los datos en tránsito, por el contrario, son datos que se mueven entre redes y se aplican fuertemente en el uso de análisis de *big data*. Esta práctica a menudo se denomina "cifrado de extremo a extremo". También se recomienda habilitar la gestión cuidadosa de las claves de descifrado.
- Almacenamiento de datos separados: el almacenamiento de datos en múltiples ubicaciones minimiza el impacto de una violación de estos en una de esas ubicaciones.
- Cumplimiento legal: promover el cumplimiento del reglamento garantiza que la recopilación sea necesaria y que se haya obtenido el consentimiento explícito y a través del movimiento de redes entre países, si corresponde.
- Cumplimiento de PCI: PCI-DSS es un estándar de la industria para organizaciones que recopilan datos de pago. Su objetivo es garantizar que los datos de la tarjeta, emitidos por el principal proveedor de ella, se almacenen y procesen de manera adecuada.

Una violación de datos puede resultar en evaluaciones costosas por parte de representantes de las principales organizaciones de tarjetas de crédito, junto con multas.

- Proveedores: si la organización utiliza proveedores en la nube para procesar o almacenar datos, se deben documentar los procedimientos de seguridad y protección de la privacidad. Los contratos también deben redactarse de forma estricta para minimizar la responsabilidad en nombre de la organización, en caso de que se produzca una infracción (Antonucci, 2017).

3. Espionaje digital

El espionaje digital es una forma de piratería que se realiza por razones comerciales o políticas. Por ejemplo, un atacante puede robar información sobre el diseño de tecnología de una compañía porque no cuenta con el conocimiento para producirla por sí mismo. Esto se hace con el fin de obtener ventaja competitiva o desarrollar y, luego, lanzar un producto al mismo tiempo que su fabricante original. El espionaje digital es una amenaza directa para la seguridad nacional en todo el mundo, así como para las empresas.

Los *hackers* que se dedican al espionaje digital a veces llevan a cabo estas actividades por patriotismo provocado por amenazas reales o percibidas, o por la falta de respeto de otros países. La inteligencia del gobierno se ve comprometida cuando los *hackers* realizan con éxito el espionaje digital porque la información en los documentos clasificados puede contener tecnología avanzada o información de defensa nacional. El espionaje digital a menudo ocurre sin dejar rastro, por lo que es difícil saber con cuánta frecuencia tiene lugar. A veces, incluso cuando se ha descubierto el espionaje digital es imposible rastrear a las partes responsables debido a las sofisticadas técnicas que los *hackers* utilizan.

4. Vigilancia digital

La vigilancia digital es la supervisión de la actividad informática, de los datos almacenados en un disco duro o la transferencia a través de redes informáticas. La vigilancia digital generalmente se realiza de manera supersticiosa y puede ser realizada por cualquier persona, gobierno, corporaciones e incluso personas.

La vigilancia digital tiene diferentes formas. Todos los formularios de internet, por ejemplo, vigilan lo que se está haciendo en un computador, especialmente lo que se está buscando en Internet. Una forma de esta vigilancia es la vigilancia de red. También hay vigilancia corporativa, *software* malicioso y software policial y de gobierno. Algunas de las formas de vigilancia digital son para proteger y otras son para robar información y venderla.

La vigilancia de red es el monitoreo de datos y tráfico en Internet que puede incluir llamadas telefónicas monitoreadas por el gobierno.

La vigilancia corporativa es muy común y es información recopilada para propósitos de mercadeo y/o para venderla a otras corporaciones, o también para compartirla con agencias gubernamentales. El *software* malicioso se usa para ver datos almacenados en el disco duro de un computador y también para monitorear las actividades de una persona.

5. Innovación en seguridad de la información

La visibilidad y la automatización son áreas clave de la innovación en ciberseguridad, contando con elementos básicos para gestionar riesgos y sin descuidar el elemento humano. Esto quiere decir que regularmente las empresas no cumplen con los principios fundamentales para protegerse, como la gestión de configuración de equipos, procesos y demás elementos, control de acceso, segmentación de redes, monitoreo de eventos y, lo primordial, no saben identificar dónde se encuentran los activos de información más importantes.

Hoy en día hay una preocupación mayor por las llamadas técnicas avanzadas, generando más complejidad en la gestión de seguridad sin haber hecho lo básico correctamente. Utilizar herramientas modernas para redes obsoletas en temas de gestión no es garantía de protección porque los atacantes siempre usan el método más sencillo para lograr sus objetivos maliciosos y por lo general se basa en vulnerabilidades comunes y bien conocidas, empleando únicamente herramientas más sofisticadas como último recurso.

Aspectos en la ciberseguridad que resultan de gran interés para temas de innovación, como es la aplicación de inteligencia artificial, por ejemplo, son la visibilidad y la comprensión de los activos de información clave que posea una empresa y lo que sucede en las redes que interactúan con esos activos; no se trata del tradicional monitoreo de red que se preocupa más por temas de disponibilidad, por ejemplo.

Lo que se requiere es una visibilidad mejorada e inteligente, que le permita a las empresas eliminar privilegios de acceso y red innecesarios, rastrear movimientos de datos, limitar qué aplicaciones se pueden ejecutar en determinados recursos informáticos y reducir la cantidad de control que los usuarios tienen sobre sus sistemas y su capacidad para instalar *software* malicioso inadvertidamente. Puede que se diga que estas acciones las realizan dispositivos de seguridad lógica, pero esto genera puntos de latencia, complejidad y muchas veces incapacidad del personal de TI para administrarlos correctamente, lo que impide que los dispositivos operen como se debe. La visibilidad inteligente debe hacer uso de la inteligencia artificial para aprender cómo opera la red de un usuario y logre tomar decisiones que son difíciles de rastrear, como el reducir accesos de un usuario y, en dado caso, volverlos a otorgar de manera autónoma.

Otros puntos importantes son la automatización, la orquestación y el enriquecimiento. Esto se encuentra muy relacionado con lo anterior, pues implica que es necesario para las empresas correlacionar la información que reciben de los diferentes dispositivos de seguridad (orquestación). Esta correlación debe generar valor para la organización en temas de seguridad (enriquecimiento) para que de manera autónoma se tomen decisiones (automatización), y así el personal de TI se encargue de gestionar efectivamente los riesgos y atienda cosas realmente orientadas al negocio.

Ser capaces de hacer cosas como bloquear sitios web, cerrar procesos y restablecer las credenciales de los usuarios de forma automática u orquestada es el reto en innovación para la ciberseguridad hoy en día, lo cual implica hacer uso de las nuevas tendencias para protegerlas por sí mismas.

La innovación en torno al concepto de orquestación también tiene como objetivo permitir a las organizaciones implementar acciones de remediación en todos los componentes relevantes de seguridad. En este sentido, la automatización se considera un área clave de innovación para contrarrestar los ataques cada vez más automatizados que pueden abrumar a los equipos de seguridad y a las defensas tradicionales.

Pero aparte de la tecnología, es primordial que las organizaciones no pasen por alto la importancia del trabajo en equipo y de la sensibilización de los usuarios para generar cultura en seguridad.

Todos en una organización deben comprender que, en última instancia, la seguridad se trata de seres humanos. Son ellos los que descubren infracciones, los que hacen defensa, los que reciben alertas y necesitan decidir cómo responder.

Entender el elemento humano de la seguridad complementa el uso de las nuevas tendencias para la protección de una organización que requiere estar a la vanguardia de la tecnología, cumplir sus objetivos estratégicos y mantener sus activos protegidos para lograr el cumplimiento de sus metas (Ashford, 2015).

Referencias

Ametic-Madison Market Research. (2016). *Informe de Tendencias TI* . Madrid, España: Ametic - Madison Market Research.

Antonucci, D. (2017). *The Cyber Risk Handbook*. USA, Canadá: John Wiley & Sons.

Ashford, W. (13 de octubre de 2015). Cyber security innovation is crucial, says security evangelist. *ComputerWeekly.com*. Recuperado de http://www.computerweekly.com/news/4500255332/Cyber-security-innovation-is-crucial-says-security-evangelist

Harris, S. (2013). *All in One CISSP*. Exam Guide. New York, USA: McGraw-Hill.

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Teoría de la Seguridad

Unidad 4: Seguridad en la nuevas tendencias de TI

Escenario 8: Seguridad en la nuevas tendencias de TI

Autor: Alexandra Peña Daza

Asesor Pedagógico: Angie Viviana Laitón Fandiño

Diseñador gráfico: Henderson Jhoan Colmenares López

Asistente: Alejandra Morales