Ciberseguridad: Por dónde Empezar...

Cybersecurity: Where to Start...

Carlos Arturo Castillo Medina

Resumen

A diferencia de la mayoría de los documentos que hablan de ciberseguridad donde muestran principios a seguir y efectos de ataques, el presente documento se concentra en la presentación de escenarios en donde la importancia de la ciberseguridad cobra un sentido preponderante y se hace necesario examinar procesos que deben ser desarrollados tomando como principio el concepto de "Sistema de Información". Normalmente se piensa que la ciberseguridad es cosa de hardware, software y de personal certificado; sin embargo, en la mayoría de las organizaciones se olvidan de elementos como las personas, el rol del negocio y el manejo de la información sensible. Por otra parte, el documento muestra un panorama de corte internacional y los avances que se han tenido a nivel nacional en materia de ciberseguridad con el fin de proponer un escenario para el desarrollo de proyectos de nuevo conocimiento en donde, con un enfoque sistémico, la ciberseguridad puede alcanzar resultados significativos integrando los elementos de infraestructura tecnológica y los conceptos de un sistema de información para preservar la Confidencialidad, Integridad y Disponibilidad de la información en escenarios de riesgo logrando generar confianza en la organización.

Palabras clave: Ciberseguridad, vulnerabilidad, sistema de información, cibreataque.

Abstract

Unlike most documents that talk about cybersecurity where they show principles to follow and the effects of attacks, this document focuses on the presentation of scenarios where the importance of cybersecurity takes on a preponderant sense and it is necessary to examine processes that they must be developed taking as a principle the concept of "Information System". Cybersecurity is commonly thought of as a matter of hardware, software, and certified personnel; however, in most organizations they forget about elements such as people, the role of the business and the handling of sensitive information. On the other hand, the document shows an international panorama and the advances that have been made at the national level in terms of cybersecurity in order to propose a scenario for the development of new knowledge projects where, with a systemic approach, the Cybersecurity can achieve significant results by integrating the elements of technological infrastructure and the concepts of an information system to preserve the Confidentiality, Integrity and Availability of the information in risk scenarios, generating trust in the organization.

Keywords: Cibersecurity, vulnerability, information system, cyberattack.

Recibido / Received: 21 de Julio de 2021 Aprobado / Aproved: 15 de Septiembre de 2021
Tipo de artículo / Type of paper: Artículo de Revisión
Afiliación Institucional de los autores / Institutional Affiliation of authors: Universidad El Bosque
Autor para comunicaciones / Author communications: castillocarlos@unbosque.edu.co
El Autor declara que no tiene conflicto de interés.

Introducción

En la actualidad los diseños de las redes de Próxima Generación de Internet (NGI) han traído consigo la convergencia de los diferentes servicios que fluyen sobre una red en conjunto con los aspectos de seguridad de la información (conocida como ciberseguridad), es decir, no se puede pensar solo en el diseño de la red, sino que a su vez es necesario mirar los aspectos que garanticen la seguridad sobre la información que fluye sobre ella, además de los requerimientos de calidad de servicio CoS, QoS y de la gestión de redes y servicios. La seguridad de las redes NGI depende en gran medida de la composición de los servicios[1] y la conectividad de los sistemas subyacentes[2]. Muchos estudios empíricos han demostrado que la minería de conjuntos de nodos importantes es muy crítica en una red, es decir, una parte de los nodos vitales puede llevar al colapso de toda la red interdependiente (por ejemplo, redes de energía y redes de comunicación). También puede ser utilizado por los proveedores de infraestructura y servicios de Tecnologías de la Información (TI) para controlar el tráfico de Internet en muchos nodos críticos para la búsqueda de virus[3]. Debido al aumento en el número de dispositivos interconectados distintos, se ha vuelto difícil desarrollar una solución de seguridad dinámica y confiable que pueda proteger la red contra todos los riesgos potenciales de seguridad[4]. Por lo tanto, es importante analizar y comprender la conectividad de diferentes sistemas a diferentes niveles para identificar vulnerabilidades y mitigarlas. Estas vulnerabilidades incluyen el efecto en cascada, eliminación de nodos, enlaces vitales de identificación, capacidad de control de nodos, ataques de ruta iterativa y estrategias de cambio para propagación a gran escala. Sin embargo, estas soluciones pueden no ser tan efectivas ya que se centran solo en la conectividad de red y sus características (centralizadas). Hay muchas otras propiedades importantes del sistema, la red y su seguridad que no se consideran y afectan directamente el rendimiento y la seguridad de todo el sistema[5].

En efecto, en la actualidad los sistemas de información, el internet y la computación en la nube son el soporte para el almacenamiento, gestión y aplicación de información personal y organizacional, convirtiéndose en el blanco para quienes la quieren robar, manipular o dañar, o desean afectar a sus propietarios. Esto se presenta porque las personas y las organizaciones soportan su rutina en esta "la información" que por lo general no está dentro de perímetro geográfico, de manera que cualquier manipulación o fallo termina afectándolos notoriamente, a nivel individual y colectivo [6].

Ahora bien, la ciberseguridad (Se toma como referencia: *El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Las propiedades de seguridad incluyen uno o más de las siguientes: disponibilidad, integridad (que puede incluir autenticidad y el no repudio) y confidencialidad (Tomado de ITU: Unión Internacional de Telecomunicaciones). Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo a su vez ciberespacio como el entorno complejo resultante de la interacción de personas, software y servicios en Internet, a través de dispositivos tecnológicos y redes conectadas a él, que no existen en ninguna forma física (Tomado de ISO/IEC:27032.))* se enfoca entonces en la protección de la infraestructura computacional y de la información circulante en las redes informáticas, aunque también del diseño de normas, procedimientos, métodos y técnicas que posibiliten seguridad y confiabilidad en los sistemas de información. Esto es importante pues los ataques en el ciberespacio afectan no solo en el mundo digital, sino que pueden concretarse en el ámbito físico, por ejemplo, dañando sistemas estructurales de una organización, una nación o una región [7].

Un Amplio Panorama

Los Smart Cities

El avance en las tecnologías de ciudades inteligentes, sin duda, afecta la vida de las personas y está claro que, en el futuro, influirá en la remodelación de nuestras comunidades y sociedades. Las ciudades inteligentes están brindando beneficios económicos, servicios públicos eficientes, transporte mejorado, seguridad, sostenibilidad, infraestructura inteligente, atención médica

inteligente y una toma de decisiones más efectiva basada en datos. Todos estos beneficios se han logrado mediante el uso de la infraestructura de Internet de próxima generación (NGI) donde todos los componentes de las ciudades inteligentes están conectados en red a través de redes locales e Internet. Las NGI es un ejemplo de un sistema complejo, una red compleja o un sistema de sistemas (SoS). En general, es un sistema dinámico a gran escala compuesto por una gran cantidad de subsistemas, que exhiben características deterministas y estocásticas altamente no lineales y que están regulados en diferentes niveles, que evolucionan con el paso del tiempo y emergen con un nuevo conjunto de desafíos [8].

La iniciativa de las NGI de la Unión Europea ha permitido el desarrollo de proyectos de investigación en torno a temas como: Ciberseguridad y resiliencia, Infraestructura de información confiable en línea, Identidades y confianza en línea, Descentralización del poder gubernamental, El derecho de exclusión voluntaria y Autogobierno, Soberanía de datos, IA (Inteligencia Artificial) ética y aprendizaje autónomo, Una Internet diversa y segura, una Internet accesible y abierta e infraestructura sostenible y justa[5]. Por otra parte, estos avances y tenas de investigación también traen consigo efectos contrarios como los planteados por entes regulatorios, a manera de ejemplo, el Informe de la Comisión Federal de Comercio sobre IoT (Internet of Things) destaca las preocupaciones de privacidad del consumidor y los riesgos de seguridad, y aconseja a las organizaciones que adopten las mejores prácticas para abordar estos problemas. El informe establece que los dispositivos inteligentes son responsables de recopilar grandes cantidades de datos críticos y personales[4], y que los datos no solo están en riesgo por el acceso no autorizado, sino que es vital mantener la integridad de los datos. Debido a que la corrupción de datos puede causar que un objeto que depende de esos datos funcione mal de manera impredecible y peligrosa. Es aquí en donde la ciberseguridad es un problema importante en el mundo interconectado de hoy en día, ya que *existe un gran déficit teórico y aplicado* en la arquitectura existente de ciberseguridad [9].

Además, las amenazas en el ciberespacio se están volviendo más complejas, escalables y dinámicas debido a la expansión de la infraestructura de Internet, en donde el desarrollo de miles de millones de nuevos dispositivos IoT heterogéneos, el aumento de la interconexión y la implementación de nuevo software, como sistemas operativos y aplicaciones trae consigo una alta dependencia entre los sistemas en diferentes jerarquías, aumentando el riesgo de fallas masivas, ya sea a través de una falla accidental o un ataque malicioso. Un concepto similar se aplica a las soluciones de seguridad propuestas para las NGI, es decir, un sistema mal conectado y no seguro puede afectar directamente la seguridad de los subsistemas interconectados y las NGI en general [3].

Internet of Things

El desarrollo del concepto de IoT (Internet de las Cosas – Internet of Things) está asociado con la introducción a gran escala de tecnologías inalámbricas, la integración de máquina a máquina (M2M), la transición a la computación en la nube e IPv6 en los últimos dos o tres años. La popularidad de Internet de las cosas se explica por una característica única de la tecnología revolucionaria: tiene la capacidad de unir a una persona y una "cosa" en cualquier período de tiempo y en diferentes lugares gracias a una variedad de redes de comunicación. En los documentos oficiales, el término "cosa" generalmente se reemplaza con términos como nodo, objeto o dispositivo. Los componentes principales de Internet de las cosas son las redes de sensores USN y el identificador de radiofrecuencia RFID. La cosa en la USN significa un solo sensor o sistema de sensores y una etiqueta o etiqueta especial RFID; en donde se utiliza el protocolo IPv6 que para IoT es el 6LoWPAN siendo la base de red USN. Según los expertos, en dos años la cantidad de dispositivos conectados a Internet alcanzará entre 50 y 100 mil millones de unidades, lo que representaría, hoy en día, muchos dispositivos conectados a través de Internet que pueden funcionar de manera completamente independiente, sin la presencia de una persona. Un buen ejemplo son los sistemas de información de los complejos modernos: sistemas de control, sistemas de control de iluminación, sistemas de riego automático, semáforos, sensores de alarma de incendio y seguridad, etc. Nuevamente se plantea que el problema clave del desarrollo de Internet de las cosas seguirá siendo la seguridad de la información.

En este sentido, es preciso tener en cuenta que el internet de las cosas se fundamenta en tres características principales:

- datos de información generalizada (información compleja sobre el objeto obtenido en cualquier período de tiempo y en cualquier ubicación);
- transmisión confiable (a través de enrutamiento, protocolos de comunicación, encriptación y codificación, seguridad de red);
- procesamiento inteligente de los datos recibidos (gracias a varios cálculos, métodos y tecnologías de análisis y procesamiento de datos de Big Data y la obtención de la información necesaria de los usuarios).

Según estas características, la estructura de Internet de las cosas se divide en tres niveles: nivel de red, nivel de aplicación y nivel de percepción. De los anteriores niveles la seguridad debe velar por la integridad de la información y es aquí en donde el objetivo principal del nivel de percepción es obtener lecturas confiables de sensores y etiquetas RFID. Ahora bien, garantizar la seguridad de la información de Internet de las cosas llega a un nivel fundamentalmente nuevo. Es provocado por dos factores: la heterogeneidad de la estructura (variedad de cosas, diferentes tecnologías de redes) y el aumento en el número de dispositivos. El Internet de las cosas recopila grandes cantidades de información de diferentes dispositivos y procesa datos de diferentes formatos que provienen de fuentes con características heterogéneas. Como resultado, surgen problemas a nivel de red que son particularmente difíciles de resolver. Estos incluyen problemas de escalabilidad de la red causados por el bajo volumen predecible de transferencia de datos desde un gran número de nodos, y que conducen a la posibilidad de ataques DoS y DDoS *(Existen dos técnicas de este tipo de ataques: la denegación de servicio o DoS (por sus siglas en inglés Denial of Service) y la denegación de servicio distribuido o DDoS (por sus siglas en inglés Destributed Denial of Service). La diferencia entre ambos es el número de ordenadores o IP´s que realizan el ataque. Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática. Tomado de: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos.).* Se presta especial atención a las vulnerabilidades del software que pueden interrumpir el funcionamiento de los sistemas de seguridad de la información después de la implementación [10].

Infraestructura Tecnológica

Otro aspecto que vale la pena mencionar es el relacionado con la seguridad en la infraestructura de las organizaciones, en donde las empresas de hoy necesitan mejorar su seguridad mediante una rápida adaptación a los desafíos de la seguridad moderna de redes sin perímetro. Todos los días se enfrentan a numerosos ataques a la red dirigidos a todos sus activos, incluidos varios tipos de información que deben protegerse, entregarse en modo 24x7 y procesos subyacentes a estos negocios. Dadas las circunstancias, la falta de capacidades avanzadas de detección y respuesta a amenazas, así como la alta ocupación de los profesionales de los equipos de tecnología de la información (TI) y seguridad de la información (IS), aunado a la carecía de experiencia en seguridad profunda que exacerbaba la situación, hace necesario la incorporación de un nuevo elemento a la triada formada por: "Detectar-Investigar-Responder" en la cual se basa la seguridad informática, dicho componente denominado "Adapt", que debe basarse en el enfoque de Inteligencia de Seguridad (SI) permitiendo una rápida respuesta a las vulnerabilidades que se presenten.

La infraestructura segura de un sistema debe cumplir con los requisitos para garantizar holísticamente su Seguridad de la Información. Eso significa que debe implementarse desde diferentes puntos de vista: organizacional, técnico, hardware, software, etc. Este enfoque integra de manera efectiva a las personas, las políticas, los procesos, las tecnologías y las herramientas para garantizar que la seguridad de la información funcione mejor cuando los conjuntos de herramientas de seguridad y el personal están alineados en torno a procesos comunes de acuerdo con las políticas de Inteligencia de Seguridad. Todos estos componentes merecen una consideración separada y cuidadosa [11].

Tercerización de Servicios

Sin lugar a duda uno de los principales elementos que dominan el comercio electrónico ha sido la tercerización de los servicios ofrecidos por las organizaciones. Este

elemento hace que los principios que rigen la seguridad de la información se vean afectados en gran escala. En efecto, los principios que permiten asegurar un sistema de información se ven vulnerados cuando los servicios que ofrece una organización son tercerizados y no existe un correcto control sobre ellos. En este sentido, el desarrollo de la computación en la nube y la proliferación de los servicios en Internet, hacen que la selección de servicios en la nube se convierta en un área sometida a un intenso estudio. Las técnicas de selección de servicios existentes suponen que los criterios de selección son independientes, hecho que no permite tener por completo el control de la organización al suponer la independencia de los servicios. Esta suposición no tiene en cuenta el hecho de que existen diferentes tipos de relaciones no lineales entre criterios. En realidad, los componentes en un sistema complejo interactúan entre sí en diferentes formas. Esos diferentes tipos de interacciones influyen en el rendimiento de todo el sistema. Lo anterior permite vislumbrar el desarrollo de un mecanismo de modelado no lineal para resolver la selección de servicios en la nube donde los criterios de selección pueden tener diferentes tipos de interacciones. Para lo cual es necesario tener en cuenta que hay tres tipos de relaciones entre criterios: interactuar positivamente (o apoyar), interactuar negativamente (o en conflicto), e independiente [12]. Este tipo de análisis normalmente no es contemplado en las organizaciones por lo cual lleva a una toma de decisión que puede afectar negativamente la ciberseguridad de la organización. Normalmente los servicios que se ofrecen en la nube son seguros de manera independiente, sin embargo, cuando se tiene un conjunto de servicios tercerizados la seguridad se diluye y la responsabilidad se pierde. Este es un elemento crucial que muchas veces los encargaos de TI no lo consideran prioritario.

Certificaciones

En un mercado cada día mucho más competitivo y en donde los profesionales deben mostrar una mayor integralidad en su formación se hace necesario tener una complementariedad afín con su quehacer. En este sentido, es importante ampliar el espectro de los gestores de redes de tal manera que le permita, no solo realizar el diseño de la red, sino a la vez identificar amenazas, realizar auditorías de red, técnicas de ataque, hacking y evasión, scanning, foot printing y enumeración, así como la prevención de ataques por software malicioso (malware) y su erradicación. Complementando lo anterior, se hace imperante contar con elementos de criptografía, encriptación, pruebas de penetración y hacking encubierto, esteganografía, certificados digitales, así como la recuperación de la operatividad luego de un desastre, conocimientos que no se pueden adquirir en una sola especialización. Aquí nace el concepto de las certificaciones que son ofrecidas por multinacionales o entes que garantizan una serie de habilidades frente a situaciones específicas. A continuación, se muestran las Certificaciones más reconocidas:

- SSCP (Systems Security Certified Practitioner): Esta certificación en seguridad informática es ofrecida por el ISC (Consorcio Internacional de Certificación de Sistemas de Información de Seguridad) y certifica la capacidad del profesional que la posee para administrar e implementar la infraestructura de la empresa, y alinearla con las políticas de seguridad que permiten garantizar la confidencialidad de los datos.
- CRISC (Certified in Risk and Information Systems Control): Se trata de una certificación en sistemas informáticos gestionada por ISACA. Los profesionales que la obtienen pueden identificar evaluar y preparar respuestas a diferentes riesgos de seguridad.
- CISA (Certified Information Systems Auditor): Esta certificación en seguridad informática está destinada a quienes realizan auditorías, controles y evaluaciones de los sistemas de TI y también es gestionada por ISACA.
- CISA.CISM (Certified Information Security Manager): Esta certificación en seguridad informática también la gestiona ISACA. Quienes obtienen esta certificación, además de ser competentes en temas de seguridad, demuestran las siguientes aptitudes: Comprender la relación entre los objetivos de la empresa y el programa de seguridad de la información de la organización. Son capaces de desarrollar y gestionar un programa de seguridad informática.
- CISSP (Certified Information Systems Security Professional): En este caso, se trata de una certificación en seguridad informática ofrecida por ISC. Es una certificación ideal para quienes ya tienen cono-

cimientos amplios, tanto técnicos como de gestión, así como experiencia. Quienes tienen esta certificación son capaces de diseñar, implementar y gestionar programas de seguridad propios.

- CompTIA Security+: Se trata de una certificación en seguridad informática confiable a nivel global que cubre los principios esenciales para la seguridad de la red y la gestión de riesgos. Quien posee esta certificación constata sus conocimientos para proteger y asegurar una red contra hackers.

Ciberseguridad y Pandemia

El presente apartado ha sido tomado de los informes que periódicamente distribuye Cisco Systems *(Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones)* en materia de ciberseguridad. Estos informes develan cómo será el comportamiento de la fuerza laboral de las organizaciones a futuro tras la pandemia y la forma en que los equipos de TI deben hacer frente a la nueva forma de mantener una infraestructura tecnológica que responda a las nuevas tendencias que se vienen adelantando.

La pandemia de COVID-19 ha provocado que las empresas de todo el mundo hagan la transición a un entorno de trabajo remoto a una velocidad y escala sin precedentes. Lo que alguna vez fue una modalidad opcional para los colaboradores de las organizaciones y las empresas se convirtió en algo imprescindible casi de la noche a la mañana: organizaciones de todo el mundo han implementado acuerdos de trabajo remoto para toda su fuerza laboral. A medida que sucedía la transición, las organizaciones tuvieron que adaptar y desarrollar sus enfoques, soluciones y políticas de ciberseguridad para que los colaboradores pudieran trabajar de forma remota, acceder a los recursos de la empresa de manera segura y garantizar la continuidad del negocio. En lo que ha sido un año cargado de incertidumbre, ha surgido una tendencia importante: la de un futuro laboral flexible e híbrido. Después de haber trabajado de manera remota durante un período prolongado, los colaboradores ahora esperan tener la flexibilidad y la capacidad para trabajar desde cualquier lugar, en cualquier momento y con cualquier dispositivo, en una era posterior al COVID, incluso cuando regresen a la oficina [13].

Recorrer correctamente las futuras disrupciones requiere que los líderes de TI adopten una nueva mentalidad. Una con un renovado énfasis en la agilidad de TI necesaria para lograr la resiliencia empresarial, en lugar del enfoque más prescriptivo y reactivo que ha sido la base de la planificación tradicional sobre continuidad del negocio. A diferencia de los esfuerzos actuales de continuidad del negocio, la resiliencia empresarial ubica a las organizaciones para prepararse incluso para lo inesperado [14].

Al utilizar dispositivos y conexiones personales para acceder a aplicaciones y datos corporativos, los colaboradores remotos son vulnerables a ataques de ciberseguridad. Muchos buscan la forma de evadir la VPN y se conectan directamente a servicios y aplicaciones en la nube pública, que sigue siendo el entorno más difícil para defender. A partir de lo anterior, el trabajo que se tiene desde los encargados de ciberseguridad de los equipos TI se ven comprometidos con los siguientes elementos de seguridad que permitirán garantizar un correcto funcionamiento de la red [14]:

- Escalar las VPN para proteger a los trabajadores remotos: las VPN empresariales siguen ofreciendo una de las formas más eficaces y rápidas de ampliar el control y la protección a nivel empresarial para los trabajadores remotos.
- Utilizar la autenticación de varios factores (MFA) para proteger las aplicaciones: MFA, que verifica la identidad de cada usuario antes de permitirle acceder a la red o a aplicaciones y datos confidenciales, es fundamental para proteger la organización.
- Implementar un perímetro de servicio de acceso seguro (SASE) para ayudar a garantizar la protección para el acceso multinube: la seguridad basada en la nube y SASE le permiten defenderse de las amenazas basadas en Internet, independientemente de la conexión, el dispositivo del usuario o el entorno de nube.

Por otra parte, los líderes de TI utilizan servicios en la nube como un medio para mejorar la resiliencia empresarial como consecuencia de la pandemia global. Esto incluye una adopción cada vez mayor del modelo multinube (distribución de aplicaciones, cargas de trabajo y

datos en las instalaciones, centros de datos y proveedores de nube pública) para reducir costos, aumentar la flexibilidad y protegerse contra la propagación del riesgo de fallas catastróficas. Para garantizar una experiencia uniforme para los usuarios y los equipos de DevOps, las organizaciones necesitan una estrategia de red proactiva y multinube que alinee la red con las prioridades de la nube, la seguridad y las operaciones de TI. Las estrategias exitosas de redes multinube se basan en tres pilares fundamentales [14]:

- **Carga de trabajo:** adoptar un modelo operativo en la nube para simplificar las políticas, la seguridad y la administración de cargas de trabajo y servicios en los centros de datos en las instalaciones, múltiples nubes diferentes y otros entornos informáticos.
- **Acceso:** adoptar enfoques de SD-WAN y SASE para garantizar un acceso multinube seguro y uniforme (que incluya SaaS) para los usuarios y dispositivos en redes corporativas y públicas desde el campus, las sucursales, el hogar o fuera de la oficina.
- **Seguridad:** reducir el riesgo asociado con los usuarios, dispositivos y aplicaciones distribuidos en varias nubes y otros entornos informáticos.

Pequeños Ataques con Grandes Resultados

A lo largo de este último año, la pandemia generada por el COVID-19 ha originado que los recursos tecnológicos como computador, Tablet, celular se usen con una mayor frecuencia para una gran variedad de procesos que antes se buscaba hacer de manera presencial y en donde la información se va a ver expuesta en el ciberespacio que normalmente denominamos internet. Términos como vishing, phishing y smishing buscan robar la identidad de una persona y usarla en su beneficio. Son las entidades bancarias las que principalmente están más expuestas. El robo de esta información se basa principalmente en la necesidades y gustos que tienen las personas por ganarse un premio o por la inseguridad que muchas veces se presenta frente a la tecnología y el resguardo de los recursos financieros. A continuación, se describen estos pequeños ataques que usan información privilegiada para ganar confianza y de esta forma perpetrar un ataque que trae consigo un gran beneficio para quien lo realiza:

Phishing: Se basa principalmente en el envío de correos falsos que dirigen a los usuarios a páginas falsas con la apariencia de la página original y que buscan que el usuario brinde información confidencial.

Vishing: Se deriva de dos palabras "voice" y "phishing", lo que indica una combinación de una llamada fraudulenta y el previo envío de un mensaje por correo electrónico. Es decir, el ciber atacante ya ha capturado cierta información por medio de una página fraudulenta (phishing) pero necesita la autenticación o validación de la clave bien sea por medio de un SMS o un token digital. Este es el segundo paso que se necesita y se realiza a través de una llamada (voice). La forma más común que se presenta este proceso es cuando se recibe una llamada del banco indicándole al usuario que se está presentando un problema con su cuenta y que puede perder todo su dinero, inmediatamente se entra en pánico y muchas veces se brinda información confidencial sobre nuestras claves.

Smishing: Para este caso la forma de tomar la información o cautivar a un usuario es por medio de mensajes de texto o principalmente por medio de mensajes de WhatsApp en donde se le indica al usuario que se ha ganado un premio o, por el contrario, se le informa que se ha realizado una compra sospechosa y que es necesario validar información confidencial y se le suministra un teléfono para que se comunique. Cuando el usuario realiza la llamada, es el momento en donde el ciber atacante intenta tomar la información del usuario.

Ciberseguridad en Colombia

El concepto de Seguridad Informática en Colombia es asumido como un elemento que hace parte de las responsabilidades del Ministerio de las TIC, y en donde el concepto de ciberseguridad ha sido acuñado por el Ministerio de Defensa Nacional. En este sentido, la Universidad Militar, La Escuela de Telemática y la Escuela de Postgrados de la Policía son las que han trabajado estas temáticas bajo los frentes de Cibercrimen y Ciberguerra.

Bajo un contexto de grandes amenazas cibernéticas a la infraestructura crítica del Estado, el MinTIC tomó la iniciativa en la estructuración estratégica de la seguridad de la información, la gestión del riesgo, la resiliencia y la formación de una cultura cibernética, en asocio con

el Ministerio de Defensa, el Departamento Nacional de Planeación (DNP) y otras instituciones clave. Este esfuerzo por parte del sector central se materializó en el CONPES 3701 del 14 de julio de 2011, en el cual se establecen los lineamientos para la ciberseguridad y ciber defensa en Colombia. Con esto, Colombia se convirtió en uno de los primeros países en la región en establecer planes de acciones concretas en la defensa del ciberespacio, puesto que se venía desarrollando una serie de normatividades a nivel nacional y sectorial con incidencia en el tema. Estas medidas van desde el derecho a la intimidad y el buen nombre, pasando por el comercio electrónico, la pornografía infantil, delitos cibernéticos y la regulación del espectro.

El CONPES 3701 tiene como objetivo central "fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciber defensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio" [15]. Con base en un diagnóstico de impacto de la masificación de internet en las actividades socioeconómicas de la población, especialmente en la multiplicación exponencial de los actores individuales y corporativos en el ciberespacio y la economía digital, se identificaron algunas falencias en la política inicial de ciberseguridad y ciber defensa. Con el propósito de suplir dichas falencias, se creó el CONPES 3854 el 11 de abril de 2016. Con esta política, se pasa de un enfoque de política de ciberseguridad y ciber defensa a un enfoque de seguridad digital.

Este CONPES 3854 busca que la sensibilización, la identificación y la gestión adecuada del riesgo, así como las buenas prácticas digitales y la inclusión de múltiples partes interesadas y con responsabilidad compartida —como también las acciones de esta multiplicidad de actores— se enfoquen en maximizar las oportunidades en un entorno digital abierto, seguro y confiable, que contribuya al desarrollo de la economía digital y fomente la prosperidad económica y social [16].

Colombia además cuenta con el ColCERT, un equipo nacional de respuestas a incidentes de seguridad digital, que actualmente depende del Ministerio de Defensa Nacional, y es el encargado de atender en primer término los incidentes cibernéticos y proteger la infraestructura crítica cibernética nacional (ICCN: *Esta función es llevada a cabo de forma colaborativa junto con el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares y el Centro Cibernético Policial (CCP) de la Policía Nacional, el CSIRT de Gobierno, el CSIRT Financiero, la Fiscalía General de la Nación, enlaces sectoriales de seguridad digital y demás iniciativas de CSIRTS sectoriales y privados, así como entidades de orden nacional o enlaces con equipos de respuesta de otros países y organismos internacionales que por su misión puedan realizar aportes en cuanto a la respuesta a incidentes cibernéticos. Asimismo, y en caso de que se detecte un incidente que pueda llevar a una crisis nacional, el colCERT reporta de manera inmediata al Coordinador Nacional de Seguridad Digital, para activar el Comité de Seguridad Digital de modo de manejar así la crisis).* De igual forma, se ha venido desarrollando un plan para fortalecer la protección de la infraestructura crítica cibernética mediante una guía para la identificación de la ICCN y programas de protección sectorial de la misma (Asimismo, se expidió la Guía de administración de riesgos, corrupción y seguridad digital, dirigida a todas las entidades de la rama ejecutiva, mediante la cual se suministra una metodología que permita gestionar de manera efectiva los riesgos que afectan el logro de los objetivos estratégicos y de proceso, entre ellos los asociados a la seguridad digital. Igualmente, la Comisión de Regulación de Comunicaciones (CRC) expidió la Resolución No 5.569 de 2018 "Por la cual se modifica el artículo 5.1.2.3 del Capítulo I del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones").

En apoyo a la transformación digital de Colombia, a finales de 2018 el BID aprobó el "Programa para la mejora de la conectividad y digitalización de la economía" a través de un "Préstamo Basado en Políticas" (Policy-Based Loan o PBL, por sus siglas en inglés: *https://www.iadb.org/en/project/CO-L1233*). Este programa concreta iniciativas de fortalecimiento de las capacidades nacionales en ciberseguridad. Si bien el gobierno ha tomado medidas significativas para asegurar el ciberespacio del país con las dos políticas de seguridad cibernética, el sector privado (en particular las pyme) aún se tiene un largo camino por recorrer para estar preparado para las actuales amenazas en este campo [17].

Bajo este marco de gestión del riesgo, se ha identificado que los múltiples grupos y actores que tienen incidencia e interés en la seguridad del ciberespacio y de la infraestructura crítica son los siguientes: el sector Gobierno; el sector defensa; el sector universitario y académico, y el sector mixto y privado. Esto evidencia que la defensa y seguridad del ciberespacio no concierne de manera exclusiva al Estado y sus fuerzas militares [18].

Por otra parte, en el informe Tendencias de cibercrimen en Colombia (2019-2020) se indica que los ciber criminales están usando inteligencia artificial, por ejemplo, para enviar videos a empresas suplantando a ejecutivos, clientes y proveedores para realizar transferencias monetarias. De esta forma, se puede observar que el cibercrimen ya no es realizado espontáneamente por individuos aislados, sino que es cometido de manera estructurada por organizaciones delincuenciales muy especializadas, con carácter transnacional, que hacen segmentación y ubicación de las posibles víctimas a través de las redes sociales y que despliegan gran variedad de técnicas de seguimiento [6].

Desde el punto de vista del BID, los colombianos tienen amplias oportunidades de continuar con estudios en seguridad cibernética tanto a nivel de grado como de posgrado. Además, el MinTIC ha otorgado becas a funcionarios públicos de las áreas de seguridad digital y ciberdefensa, y también patrocina cursos de seguridad digital y capacitaciones para las diferentes ramas del servicio público relacionadas con las TIC. De igual forma, se han realizado varios programas de capacitación en colaboración con otras instituciones como MinTIC, la OEA y la Fundación Citi, y se han beneficiado 40 estudiantes de ingeniería de bajos ingresos. Finalmente, MinTIC tiene una campaña llamada "En TIC Confío" que busca promover y crear conciencia sobre el uso responsable de Internet y las TIC [17].

Lo anterior permite evidenciar la necesidad de abordar el concepto de la ciberseguridad de una manera más holística y que aporte al crecimiento de las organizaciones no solo desde el aspecto tecnológico, sino que permita establecer un estrecho relacionamiento entre los diferentes actores y tecnologías, en pro de un conocimiento de toda la organización de una manera sistémica que concluya en un verdadero Sistema de Información.

Formación del Recurso Humano

La gestión del conocimiento en la actualidad se convierte en el activo intangible más poderoso de las organizaciones modernas, por cuanto, facilita la potencialización de las competencias del talento humano, como aspectos determinantes para generar capacidad instalada para afrontar los nuevos desafíos que demandan las dinámicas de los mercados en el contexto empresarial y financiero de la sociedad actual. Sin embargo, para que esto sea posible, es necesario establecer nuevos enfoques en la gestión del talento humano y alineado con las metas y objetivos en el direccionamiento estratégico de las organizaciones. Ello, con el fin de establecer políticas y procedimientos que faciliten la adquisición, distribución, almacenamiento, transformación y utilización de conocimiento, con el propósito de lograr ventajas competitivas en el mercado [19]. Por otro lado, es necesario recalcar que la economía del conocimiento y la sociedad se caracteriza por la globalización económica, la aparición de los avances tecnológicos en varios dominios industriales y científicos y la primacía progresiva del conocimiento intensivo y tecnología basada en mercados industriales [20].

En este nuevo escenario competitivo, el conocimiento y los activos intelectuales se están convirtiendo en los nuevos factores clave de producción. Por ello, la gestión del conocimiento se convierte en una herramienta poderosa para la toma de decisiones en los distintos sectores económicos, político, sociales, entre otros, dentro de este mundo globalizado. En este sentido, en la medida que las organizaciones modernas cuenten con profesionales y equipos de trabajos capacitados en el uso de las TIC y la seguridad de la información, les permitirá a las mismas, generar mayor capacidad instalada para afrontar con eficiencia y efectividad la ciberseguridad organizacional. De hecho, mediante el fortalecimiento de las competencias del talento humano, se optimizará el uso de los recursos tecnológicos y se minimizará el riesgo de daños y/o pérdida de información, sistemas y equipos por uso inadecuado. Por tal razón, la prevención de los riesgos de ciberseguridad requiere para su adecuado tratamiento, de un conocimiento profundo de la ciberdelincuencia y de las competencias necesarias para trabajar en pro de su prevención e investigación, ya sea en el ámbito policial o en el empresarial [21].

En ese orden de ideas, la adopción de estándares internacionales y buenas prácticas para la prevención de riesgos, permitirá seleccionar profesionales con habilidades, capacidades y conocimientos para entender y administrar adecuadamente los sistemas de gestión de la ciberseguridad [22]. Por otra parte, se destacan avances en el desarrollo de las competencias para la gestión del conocimiento y la implantación de procesos, pero no se está haciendo gestión desde la estructuración de políticas, planes, programas y proyectos, falta avanzar en la apropiación y uso de prácticas y hay una deficiencia en la aplicación de herramientas tecnológicas para gestionar el conocimiento [23].

Conclusiones

En materia de Ciberseguridad nada está escrito. Existe todo un compendio de protocolos, normativas, recomendaciones, buenas prácticas, pero nada de esto puede garantizar que su sistema u organización esté segura frente a un ciberataque. Siempre existirá un punto vulnerable que no se tuvo en cuenta y que los atacantes han podido ver. La documentación existente lo que si puede garantizar es que se pueden minimizar los riesgos y que los ataque no causen tanto daño. En palabras que nos trae la pandemia que se está viviendo, la ciberseguridad es como una vacuna, no garantiza que no te puedas contagiar, pero si te garantiza que no te va a causar tanto daño como sino la hubieses tomado.

Es claro que la ciberseguridad ya no puede considerarse un tema técnico que se delegue en el personal TI de las organizaciones, sino que debe abordarse como un tema estratégico que alcanza a toda la organización. Ahora bien, si se observa de una manera más holística la ciberseguridad no es un tema de una organización, este tema ha transcendido al considerarse un tema de carácter global pues el ciberespacio no tiene país, dando origen al concepto de ecosistema digital, en donde se plantean discusiones sobre la regulación del ciberespacio, la gobernanza en él y la defensa de este.

En la actualidad el concepto de redes sin fronteras dadas por las características de la nube y del ciberespacio, hacen que su diseño sea mucho más profundo y que, se tengan que contemplar aspectos que van más allá de la infraestructura física, que en muchos casos recaen en un sinnúmero de servicios tercerizados que en la medida que ellos aumentan, la seguridad se diluye y nadie responde por un ciberataque. Lo anterior permite determinar la necesidad de contar con un grupo de ciberseguridad que se encargue de gestionar y entender los retos a los que una organización se ve avocada en el momento que terceriza sus servicios. Este grupo de ciberseguridad debe tener todo el plano de servicios y contemplar como cada parte se vería expuesta a un ataque particularizado o en su máxima instancia a un ataque generalizado de todo el sistema.

La Ciberseguridad es un proceso al interior de una organización que no permite que se pueda tercerizar. En efecto, los elementos de seguridad de la información, de la infraestructura, hacen parte del "Core" de una organización y, por lo tanto, no permite que sea manipulable por organismos fuera de la organización. Se pueden tercerizar procesos de servicios hacia los clientes, pero lo que constituye la seguridad debe ser asumida por quien conoce realmente la organización y sabe que espera proteger.

Dada la globalización y el intercambio que crece día a día en nuestra sociedad, gran parte de las relaciones, comunicaciones y procesos son digitales, con lo cual la ciberseguridad no es una alternativa sino un requisito. Los riesgos cibernéticos que afectan a todos los sectores de un país (sector gobierno, sector privado y las personas) tienen unos impactos y una problemática distintos, sin embargo, en cada uno de estos escenarios se deben aplicar medias de seguridad acordes con su naturaleza y su contexto; lo cual implica un conocimiento de su entorno y la correcta aplicación de herramientas tecnológicas que permitan el adecuado nivel de ciberseguridad que se requiere.

El campo de acción que se vislumbra tras los avances tecnológicos y más aún, por los efectos causados por la pandemia, permiten ver la necesidad de un talento humano muy cualificado que permita la articulación de una infraestructura tecnológica con una lectura de su contexto dependiendo las particularidades de su entorno. En este contexto, cobra sentido pensar que la ciberseguridad no se trata de simples recomendaciones hacia las directivas de una organización, se debe entender como el proceso que se debe seguir al interior de una organización para mantener su "negocio" activo

sin perder el horizonte que brinda los adelantos tecnológicos (almacenamiento y procesamiento en la nube, transacciones financieras, trabajo en casa, etc) para tener organizaciones sin perímetro en lo denominado como el ciberespacio. Es aquí en donde las organizaciones deben aunar esfuerzos por constituir verdaderos frentes de trabajo en contra de los ciberataques y garantizar la confiabilidad de la información.

Como se comenzó el documento, la Ciberseguridad no se trata de hardware, software y personas certificas, este concepto va más allá de una mirada a un conjunto de protocolos, cumplimiento de normas o seguimiento de buenas prácticas. Se debe entender de una manera sistémica dentro de un Sistema de Información en donde los ciber atacantes buscaran el elemento más vulnerable de la organización. Cobra sentido pensar que la capacitación y la concientización de todos los miembros de la organización ayudarán considerablemente a soportar las vulnerabilidades que se puedan dar en una organización. Comenzar en una capacitación de creación de claves seguras, manejo y actualización de los sistemas operativos de nuestros equipos de casa y de oficina, el correcto uso del correo de la organización y, a partir de lo vivido en esta pandemia, el aseguramiento de las VPN que se crean, son pequeños detalles que fortalecen en gran medida la Ciberseguridad de la organización.

Referencias

[1] P. H. Meland, «Service injection: A threat to self-managed complex systems», en *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing,* 2011, pp. 1-6.

[2] Z.-Y. Jiang, Y. Zeng, Z.-H. Liu, y J.-F. Ma, «Identifying critical nodes' group in complex networks», *Phys. Stat. Mech. Its Appl.*, vol. 514, pp. 121-132, 2019.

[3] R.-R. Liu, M. Li, y C.-X. Jia, «Cascading failures in coupled networks: The critical role of node-coupling strength across networks», *Sci. Rep.,* vol. 6, n.º 1, pp. 1-6, 2016.

[4] N. Tariq *et al.*, «The security of big data in fog-enabled IoT applications including blockchain: A survey», *Sensors,* vol. 19, n.º 8, p. 1788, 2019.

[5] K. E. Lever y K. Kifayat, «Identifying and mitigating security risks for secure and robust NGI networks», *Sustain. Cities Soc.,* vol. 59, p. 102098, 2020.

[6] M. R. Ospina Díaz y P. E. Sanabria Rangel, «Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia», *Rev. Crim.,* vol. 62, n.o 2, pp. 199-217, 2020.

[7] B. Saavedra y L. Parraguez, «La ciberseguridad: análisis político y estratégico I», *Rev. Fuerzas Armadas,* vol. 91, n.o 243, pp. 44-51, 2018.

[8] W. Basmi, A. Boulmakoul, L. Karim, y A. Lbath, «Modern approach to design a distributed and scalable platform architecture for smart cities complex events data collection», *Procedia Comput. Sci.,* vol. 170, pp. 43-50, 2020.

[9] S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin, y A. Dehghantanha, «Threats on the horizon: Understanding security threats in the era of cyber-physical systems», *J. Supercomput.,* vol. 76, n.o 4, pp. 2643-2664, 2020.

[10] D. Bagay, «Information security of Internet things», *Procedia Comput. Sci.,* vol. 169, pp. 179-182, 2020.

[11] N. Miloslavskaya, «Security zone infrastructure for network security intelligence centers», *Procedia Comput. Sci.,* vol. 169, pp. 51-56, 2020.

[12] L. Sun, H. Dong, O. K. Hussain, F. K. Hussain, y A. X. Liu, «A framework of cloud service selection with criteria interactions», *Future Gener. Comput. Syst.,* vol. 94, pp. 749-764, 2019.

[13] S. Cisco, «El Futuro del Trabajo Remoto Seguro». Cisco Press, 2021. [En línea]. Disponible en: https://www.cisco.com/c/dam/global/es_mx/products/pdfs/future-of-secure-remote-work-report.pdf

[14] S. Cisco, «Informe de tendencias en redes globales 2021». Cisco Press, 2021. [En línea]. Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/2021-networking-report.pdf

[15] D. Departamento Nacional de Planeación, «Documento Conpes 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa», 2011.

[16] C. de C. Departamento Nacional de Planeación, «Documento Conpes 3854, Política nacional de seguridad digital», 2016.

[17] Banco Interamericano de Desarrollo, «Reporte de Ciberseguridad 2020: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe». BID, 2020. [En línea]. Disponible en: https://observatoriociberseguridad.org/#/final-report

[18] X. A. Cujabante Villamil, M. L. Bahamón Jara, J. C. Prieto Venegas, y J. A. Quiroga Aguilar, «Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares», *Rev. Científica Gen. José María Córdova,* vol. 18, n.o 30, pp. 357-377, 2020.

[19] J. J. Cano, «Retos de seguridad/ciberseguridad en el 2030», *Sistemas,* n.o 154, pp. 68-79, 2020.

[20] F. P. García, «Una aproximación a la Ciberseguridad en Sistemas de Control Industrial», *Puente Hierro,* vol. 1, n.o 1, pp. 12-12, 2021.

[21] C. P. Santos, Á. C. Guisado, y J. J. D. Morán, «El fenómeno de la ciberdelincuencia en España: La propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito», *Rev. Polic. Segur. Pública,* pp. 237-270, 2017.

[22] F. J. Díaz, L. H. Molinari, P. Venosa, N. Macia, E. F. Lanfranco, y A. J. Sabolansky, «Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización», 2018.

[23] C. Marulanda, L. López, y G. Cruz, «La cultura organizacional, factor clave para la transferencia de conocimiento en los centros de investigación del triángulo del café de Colombia», *Inf. Tecnológica,* vol. 29, n.º 6, pp. 245-252, 2018.