DIFERENCIA ENTRE SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

López Duque, Carlos Mario
Mariolopez726@gmail.com
Universidad Piloto de Colombia

Resumen— *El artículo tiene como fin explicar las diferencias entre seguridad informática y ciberseguridad. La protección de la información en las organizaciones suele ser mejor día tras día, lo que representa la exigencia y la existencia de nuevas áreas de protección de ataques, ciberataques en el ciberespacio de las organizaciones.*

Abstract- *The article aims to explain the differences between computer security and cybersecurity; the protection of information in organizations is usually better day by day, which represents the demand and the existence of new areas of protection from attacks, cyber-attacks in cyberspace of organizations.*

Palabras clave: *CONPES, Nist, Isaca, seguridad informática, ciberseguridad, ciberdefenza, ciberespacio, confidencialidad, integridad, disponibilidad, ciso, ciberriesgo.*

I. INTRODUCCIÓN

El conocimiento y discrepancia de seguridad informática y ciberseguridad van aumentando cada vez más, las organizaciones pequeñas no ven la necesidad de existencia de diferentes seguridades de información internas ya que la evolución de éstas es tan rápida que no da pie a su pronta implementación.

En algunas de las medianas y grandes empresas la evolución de las nuevas áreas de seguridad es indispensables, ya que éstas suelen certificar sus procesos con alguna norma determinada que permita demostrar que la seguridad en la organización es parte de ellas y así ser más confiables a la hora de prestar sus servicios de negocio con el fin de marcar la diferencia con las otras entidades que no certifican sus procesos de negocio.

II. CONCEPTOS ESPECÍFICOS

Los conceptos a continuación son basados en el internet de entes confiables como lo son: El Consejo Nacional de Política Económica y Social (CONPES) y el Instituto Nacional de Estándares y Tecnología (Nist)

Definición de ciberseguridad según documento CONPES – 3854:

Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio[1].

Definición de ciberseguridad según la Nist:

La capacidad de proteger o defender el uso del ciberespacio de cyber ataques[2].

Definición de seguridad informática según la Nist (security computer):

Medidas y controles que garantizan la confidencialidad, integridad y disponibilidad de activos del sistema de información, incluido hardware, software, firmware e información que se procesa, almacena y comunica[3].

III. CONCEPTO BÁSICO PARA ENTENDER UN POCO MÁS DE CIBERSEGURIDAD

Es importante recalcar que la ciberseguridad es un concepto demasiado amplio; como lo mencionan en la página web de Isaca; una definición simple es la siguiente[4]:

Para entender el término ciberseguridad, primero se debe definir el término ciberriesgo.

El ciberriesgo no es un riesgo específico, es un grupo de riesgos, que difieren en tecnología, vectores de ataque, medios, etc. Abordamos estos riesgos como un grupo en gran parte debido a dos características similares:

A) Todos tienen un gran impacto potencial
B) Todos fueron considerados una vez improbables.

---

[1] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
[2] http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
[3] http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913810
[4] https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Para entender esto, se parte de una representación visual de la curva de riesgo tradicional:

La figura 1 es un gráfico simple que muestra la correlación entre la probabilidad de ocurrencia de un riesgo y su impacto potencial. A medida que se avanza hacia la derecha, aumenta el impacto potencial del riesgo. En el extremo derecho de la curva de riesgo, se evidencia una "cola larga", un grupo de riesgos de muy alto impacto con una probabilidad muy baja de ocurrencia (naturalmente, las organizaciones tienen limitaciones de recursos y centran sus esfuerzos en abordar los riesgos con una alta probabilidad de ocurrencia y un impacto potencialmente significativo).

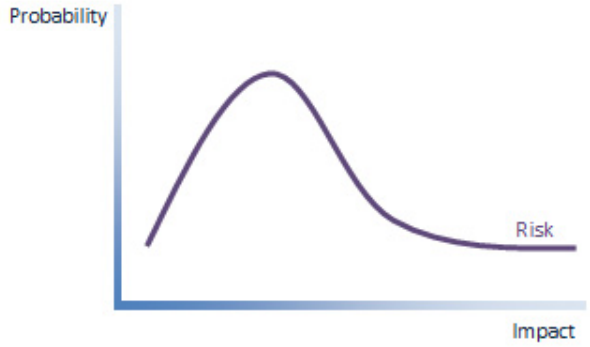

Fig. 1: Probabilidad de ocurrencia de un riesgo y su impacto potencial. Recuperado de https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Luego, se define la zona de enfoque (representada en la figura 2), como el área que contiene los riesgos a los que la organización dirige sus esfuerzos de mitigación. El tamaño de la zona de enfoque está determinado por factores tales como el apetito por el riesgo, la rentabilidad, la actitud del CISO, la cultura organizacional, la disponibilidad de recursos y el panorama relativo a las amenazas.

Como se ilustra a continuación, los esfuerzos invertidos en abordar los riesgos dentro de la zona de enfoque se conocen comúnmente como seguridad de la información. Esos riesgos incluyen malware's tradicionales (virus, troyanos, spyware, adware, etc.), ataques de phishing estándar, ataques de denegación de servicio distribuidos estándar (DDoS), actividades de piratería estándar, etc.

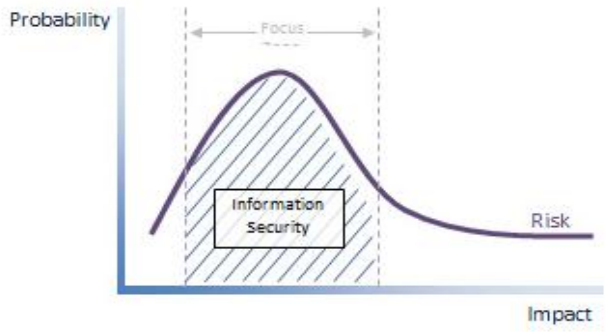

Fig. 2: Zona de enfoque. Recuperado de https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Por supuesto, algo ha cambiado recientemente. El panorama de amenazas evolucionó hasta el punto de que los riesgos que antes se consideraban improbables comenzaron a ocurrir con regularidad. La mayor probabilidad de ocurrencias de riesgo de muy alto impacto se ilustra en la figura 3 como el ítem 1. Esta tendencia puede atribuirse a una mayor madurez de las herramientas y métodos de ataque, una mayor exposición, una mayor motivación de los atacantes y mejores herramientas de detección que permiten una mayor visibilidad. Dicho esto, se debe aceptar que, parte de este cambio, es el resultado de una mayor conciencia sobre este nuevo grupo de riesgos altamente enfocado. El cambio en el panorama de amenazas obliga a expandir la zona de enfoque de una organización para incluir estos riesgos previamente excluidos, que se ilustra a continuación como el ítem 2.

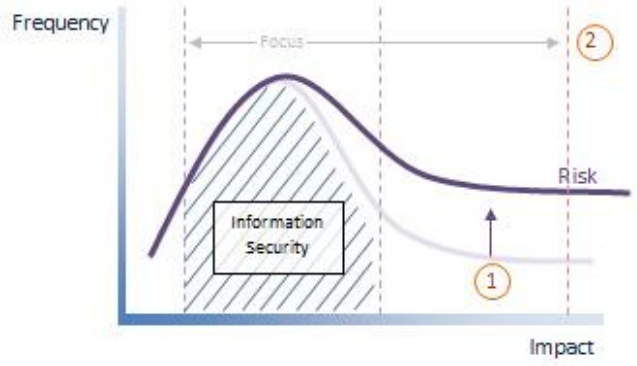

Fig. 3: Mayor probabilidad de ocurrencias de riesgo de muy alto impacto. Recuperado de https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Este nuevo grupo de riesgos de alto impacto que ahora requiere atención se conoce comúnmente como ciberriesgo. Como se ilustra en la figura 4, los esfuerzos invertidos en abordar los ciberriesgos se conocen naturalmente, como ciberseguridad. Este grupo de riesgos incluye todo tipo de situaciones extrañas: malware`s específicos de la organización, especialmente diseñados; hardware y firmware manipulados; el uso de certificaciones robadas; espías e informantes; explotando vulnerabilidades en hardware arcaico; atacando a proveedores de servicios externos; etc. Esta lista también incluye lo que se conoce como amenazas persistentes avanzadas.

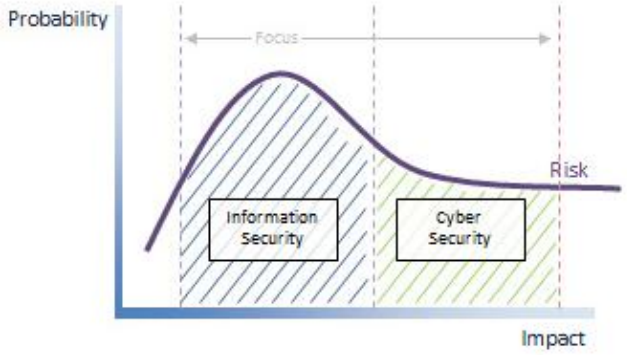

Fig. 4: Esfuerzos invertidos (los ciberriesgos se conocen como ciberseguridad). Recuperado de https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Algunos podrían considerar la seguridad de la información y la ciberseguridad como dos disciplinas diferentes, pero se diría que la ciberseguridad es una subdisciplina de la seguridad de la información (ver figura 5).

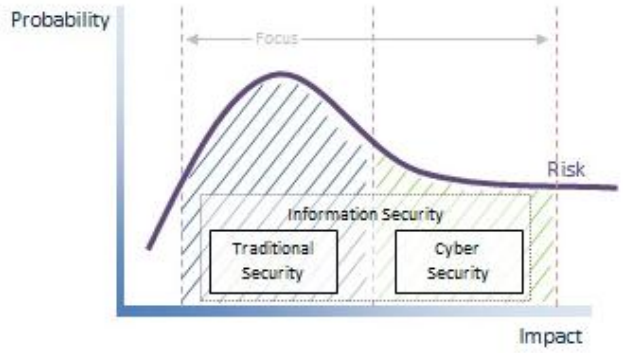

Fig. 5: Ciberseguridad como subdisciplina de seguridad de la información. Recuperado de https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

La ciberseguridad es la suma de los esfuerzos invertidos en abordar el ciberriesgo, gran parte de lo cual, hasta hace poco, se consideraba tan improbable que apenas requería de atención. En tal sentido, se debe recordar que el cambio de la curva de riesgo representa una tendencia continua. Los riesgos de alto impacto serán cada vez más frecuentes, lo que obligará a ser mejores en la protección de activos y en la creación de soluciones creativas para mitigar los riesgos. "Para entender el término ciberseguridad primero se debe definir el término ciberriesgo".

IV. CONCEPTO BÁSICO PARA ENTENDER UN POCO MÁS LA SEGURDIAD INFORMÁTICA

El aseguramiento de la información (IA) consiste en la gestión de riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de información o datos, y con los sistemas y procesos empleados en la realización de esas actividades. El IA se desarrolló a partir de la implementación de la seguridad de la información, que, a su vez, surgió como resultado de las prácticas y los procedimientos vinculados a la seguridad informática[5].

A continuación, se anuncia un ejemplo de la medición de la integridad de los datos según las recomendaciones de Isaca.

Existen muy pocas publicaciones sobre mediciones clave, rendimiento e indicadores clave de riesgos aplicados a la integridad de los datos en un contexto relacionado con la seguridad de la información. A continuación se mencionan algunos puntos que pueden resultar útiles[6]:

Un inventario de los derechos de acceso privilegiado, que indique ¿quién tiene acceso a qué información? ¿quién tiene autorización para hacer qué? ¿y en qué fecha se revisó y actualizó por última vez un documento?

- Un inventario de los datos que es posible extraer, transformar y cargar en otro sistema.
- El número de usuarios que han mantenido derechos y privilegios de acceso históricos.
- El número de cuentas huérfanas o inactivas.
- El número de sistemas de aplicación que contienen derechos de acceso mediante codificación rígida o códigos ocultos ("backdoors").
- El número de veces que fue necesario acceder a los datos de producción para realizar modificaciones o correcciones.
- El número o porcentaje de accesos y/o cambios no autorizados a los datos de producción, que se hubieren identificado.
- El número de problemas de seguridad relacionados con los datos (en un año/un mes).
- El número de sistemas que la solución IAM corporativa principal no cubre.
- Un índice de datos incorrectos o incoherentes.
- El porcentaje del modelo de datos de la empresa (o aplicación crítica) que se ha cubierto con medidas destinadas a preservar la integridad.
- El número de medidas incluidas en bases de datos y aplicaciones para detectar discrepancias en los datos
- El número de medidas aplicadas para detectar el acceso no autorizado a los datos de producción.
- El número de medidas aplicadas para detectar el acceso no autorizado a los sistemas operativos.
- El número de medidas aplicadas para detectar las modificaciones que no han estado sujetas a ningún procedimiento de control de cambios.
- El valor anual de las pérdidas económicas ocasionadas por operaciones de fraude a través de sistemas informáticos.
- La cantidad de ataques destinados a destruir la integridad de los datos en los sistemas de scada.
- La cantidad de comunicados de prensa generados a partir de los problemas que afectaron la integridad de los datos.

V. EJEMPLO DE LA DIFERENCIA ENTRE CIBERSEGURIDAD Y SEGURIDAD INFORMÁTICA DESDE EL PUNTO DE VISTA NACIÓN

Para colocar el ejemplo de la diferencia de estas dos grandes áreas es importante tener en cuenta que el tema de la ciberseguridad en la nación no lo es todo y que se cuenta con unos lineamientos.

[5] https://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

[6] https://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

Primero se debe entender que la nación (Colombia) cuenta con una identificación de infraestructuras críticas que son identificadas por el "comando conjunto cibernético" CCOC7 y que éstas a su vez son determinadas por 3 criterios o variables horizontales de criticidad:

Se definen los siguientes criterios como se muestra en la figura 6 para establecer si una infraestructura estratégica cibernética (IEC) es una infraestructura crítica cibernética (ICC) o no:

1. El impacto social: valorado en función de la afectación de la población (incluye pérdida de vidas humanas), el sufrimiento físico y la alteración de la vida cotidiana. Este se valora en función de la población total colombiana: 49.827.269 de habitantes. Fuente: DANE

2. El impacto económico: valorado en función de la magnitud de las pérdidas económicas en relación con el producto interno bruto de Colombia (PIB). PIB: 377.739.622.866. Fuente: Banco Mundial.

3. Impacto medioambiental: Valorado en función de los años que tarda la recuperación del medio ambiente como se denota en la Figura 6.

Con los siguientes valores mínimos

Impacto social 0,5 % Población Nacional	Impacto económico PIB de un dia ó 0.123% del PIB Anual	Impacto medioambiental
250.000 personas	464.619.736,13	3 años

Fig. 6: Criterios horizontales de criticidad. Recuperado de http://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

La infraestructura crítica de la Nación contempla las siguientes tres fases:

Fase 1: Gobierno, seguridad y defensa, TIC, electricidad, financiero, educación y minero – energético.

Fase 2: Salud y protección social, ambiente, industria comercio y turismo.

Fase 3: Agua, transporte, agricultura – alimentación.

Según lo identificado anteriormente para la nación, ciberseguridad es la identificación de las tres fases respecto a su infraestructura, y la seguridad informática, para este caso es la ciberdefensa en donde la nación la define como:

"Es el empleo de las capacidades militares ante amenazas o actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales"[8].

VI. EJEMPLO DE LA DIFERENCIA ENTRE CIBERSEGURIDAD Y SEGURIDAD INFORMÁTICA DESDE EL PUNTO DE VISTA EMPRESAS.

En una empresa se definen los procesos críticos, core de la compañía; en donde se enfoca su mayor esfuerzo para su protección en cuanto a la seguridad de la información.

Por ejemplo, para determinar si una empresa requiere de un área como la ciberseguridad, primero debe identificar si parte de su infraestructura física y si publica alguna aplicación en el internet o no.

Una vez identificada dicha información, las empresas cuentan con la directriz que consiste en identificar las aplicaciones web que afectan los objetivos de negocio en el ciberespacio, para así determinar si una aplicación web debe ser agregada o no al catálogo de infraestructuras críticas.

Una vez determinado este catálogo de infraestructuras críticas el área de seguridad informática actúa como la protección de dichas aplicaciones con herramientas perimetrales como:

Firewall, ips, proxy´s, ids, anti-spam, anti-apt, antivirus, etc.

VII. CÓMO MITIGAR LOS ATAQUES A LA INFRAESTRUCTURA FÍSICA CRÍTICA DE ATAQUES DESDE EL CIBERESPACIO.

Para mitigar los ataques del ciberespacio no solo es importante conocer cuál es la infraestructura crítica física, ni pensar que cuenta con las herramientas suficientes de protección perimetral. También es necesario e importante conocer el funcionamiento de dichas aplicaciones para identificar cuáles son los principales riesgos que allí se encuentran; esta es la mejor manera y más importante forma de proteger la información. Cabe recalcar que las herramientas perimetrales de seguridad no cubren el 100% de los ataques, por lo que se debe conocer cuál es el alcance de protección de dichas herramientas y a su vez identificar qué y cuáles deberían implementar para la protección de la infraestructura física que se identificó.

Como las herramientas de seguridad perimetrales no son 100% seguras debe contar con un equipo de trabajo llamado seguridad informática que se encargue de la administración de estas herramientas como: implementar las actualizaciones necesarias que mitiguen las vulnerabilidades que se identifican día a día; implementación de las nuevas firmas de seguridad

[7] http://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

[8] http://www.minambiente.gov.co/images/tecnologias-de-la-informacion-y-comunicacion/pdf/02122015_guia_icccolombia.pdf

que identifiquen los nuevos ataques; creación e implementación de nuevas reglas de protección de la información.

VIII. ALGUNOS ATAQUES DE INFRAESTRUCTURAS CRÍTICAS EN EMPRESAS Y LA NACIÓN

A. CENTRO DESDE DONDE LAS FF.MM (FUERZAS MILITARES DE COLOMBIA) REPELEN LOS ATAQUES CIBERNÉTICOS A LA REGISTRADURÍA[9]

Veinticuatro horas al día, y en total sigilo, los analistas revisan las amenazas y hacen frente a las que tienen valor real.

Según el Ministerio de Defensa, se han intentado unos 60.000 ataques contras las elecciones en Colombia en este 2018.

"Cuando notamos una saturación de tres mil, cinco mil, diez mil solicitudes de información que nos pueden estar generando el bloqueo de la página, inmediatamente vamos a identificar la dirección ip de donde están llegando esas solicitudes de información y vamos bloqueándolas", señala el general Óscar Alberto Quintero, comandante del Comando Conjunto de ciberdefensa de las FF. MM.

Y estas amenazas pueden provenir desde cualquier lugar: "No hay fronteras en el espectro electromagnético. Al no haber fronteras, nosotros nos tenemos que preparar para la vigilancia del Estado colombiano y la infraestructura critica del país", añade el general Quintero.

Esa es una gran dificultad para estos expertos: precisar desde qué punto del mundo viene el ataque. Por ejemplo, se puede originar desde Asia, pero se puede ejecutar con un servidor desde Europa.

B. ESTO PASARÍA SI LOS CIBERCRIMINALES USAN INTELIGENCIA ARTIFICIAL[10]

La inteligencia artificial es una de las novedades tecnológicas de moda. Muchas empresas y gobiernos trabajan en entender cómo aplicarla a sus procesos, así como lo que representa para su futuro.

Algunos han planteado debates sobre los temores de la humanidad ante el desarrollo de la inteligencia artificial, sin embargo poco se ha hablado de lo que pasaría si criminales la utilizan para hacer daño.

Ese fue el planteamiento de la compañía de prevención de fraudes Easy Solutions al hacer un experimento con su equipo de investigación y desarrollo al plantearse la hipótesis: ¿Qué tal si los estafadores emplean la inteligencia artificial para crear URL o direcciones específicas en Internet más efectivas que puedan evadir el software de detección?

De acuerdo con el informe anual de seguridad de Symantec, Colombia es el sexto país de América Latina que más número de ciberataques recibe.

Para el experimento, los especialistas crearon un generador de URL basado en inteligencia artificial. De esa manera, modelaron lo que una banda de delincuentes podría hacer con esa tecnología: crear una cantidad incrementada de URL, con el propósito de minimizar la detección de los sistemas antifraude y maximizar con éxito los ataques de phishing (suplantación de identidad).

De acuerdo con la empresa, al automatizar la generación de URL, la eficiencia operacional mejora "dramáticamente".

"Para automatizar la generación de URL, utilizamos los datos de ataques previos, incluyendo URL, institución afectada, dominio comprometido, entre otros. ¿Qué sucedió cuando la banda empezó a emplear IA maliciosa? Su tasa de éxito se incrementó en 3000%", aseguró David Castañeda, vicepresidente de Investigación y Desarrollo de Easy Solutions.

En la última parte del experimento, los expertos de la compañía utilizaron toda la información recabada para mejorar su sistema de inteligencia artificial y así combatir a los ciberdelincuentes utilizando las lecciones aprendidas.

"Entrenamos a nuestro algoritmo para que anticipara el uso de inteligencia artificial maliciosa. De esta forma, fuimos capaces de reducir la eficiencia de tal tecnología, derrotando así el Sistema que creamos cuando actuamos como la banda X", agregó Castañeda.

Para el directivo, la solución a este posible escenario de ataques con inteligencia artificial será combatirlos con inteligencia artificial, si se entienden sus características.

La compañía enfatiza en que el experimento deja tres lecciones: la primera es que la inteligencia artificial da la oportunidad de mejorar los sistemas de seguridad y entrenar al algoritmo para que se anticipe al uso de inteligencia artificial maliciosa, ya que permite analizar la estrategia de otros grupos capaces de aprovechar la inteligencia artificial. "Al entender sus tácticas, podemos mejorar más rápidamente nuestros propios sistemas para derrotarlos."

La segunda es que ésta tecnología utiliza algoritmos inteligentes para identificar patrones nuevos y conocidos, por esto en la actualidad la tasa de detección de las URL de phishing es de hasta un 98.7%.

Por último, especifica que si los cibercriminales emplean la inteligencia artificial para lanzar ataques más nefastos, se está preparado con tecnología más fuerte y eficaz. En la batalla de inteligencia artificial contra inteligencia artificial, siempre se está un paso adelante.

---

[9] https://noticias.caracoltv.com/colombia-decide-2018/conozca-el-centro-desde-donde-las-ff-mm-repelen-los-ataques-ciberneticos-la-registraduria

[10] https://www.dinero.com/internacional/articulo/que-pasaria-si-los-cibercriminales-usan-inteligencia-artificial/257412

Hoy todas las empresas deben contar con un enfoque holístico, multinivel, multicapas dentro de una estrategia de protección de amenazas digitales, siendo la tecnología de machine learning y la inteligencia artificial los componentes esenciales de cualquier estrategia efectiva de defensa antifraude.

C. COLOMBIA ES EL TERCER PAÍS MÁS AFECTADO POR ATAQUES CIBERNÉTICOS EN LA REGIÓN[11]

Brasil, México y Colombia encabezan el listado de blancos de estos ataques en América Latina; las Pymes y sector salud son los más afectados, según cifras de Kaspersky.

Recientemente, la empresa de ciberseguridad Kaspersky, reveló algunos datos sobre ataques cibernéticos en la región. Incrementos de ransomware, detección de troyanos y recomendaciones para evitar estas amenazas hacen parte de lo dicho por la organización.

"Los ataques por ransomware en América Latina han experimentado un aumento anual de 30% entre 2016 y 2017, con 57.512 detecciones en 2016 y 24.110 hasta la fecha en 2017", reveló la compañía al hablar de esta modalidad de ataque, que comúnmente se conoce como un secuestro de información. Uno de los más populares fue wannacry, que pedía dinero a cambio de liberar los datos que había cifrado.

"Algunos ejemplos emblemáticos de estos ataques son Petya o PetrWrap, HDD Cryptor, y el ya reconocido WannaCry que infectó más de 200.000 equipos alrededor del mundo, 98% de los cuales utilizaban sistemas Windows 7. En América Latina, la mayor propagación de éste se dio en México y Brasil, seguido por Chile, Ecuador y Colombia", afirmó la compañía.

Para Santiago Pontiroli, analista de seguridad de Kaspersky Lab en la región, el ransonmware es una de las amenazas que más está creciendo.

Bajo esta categoría, la empresa reveló que Brasil lidera la lista de países con mayor número de secuestro de datos, teniendo el 54.91% de los ataques consignados en la región. México, por su parte, ocupa el segundo lugar con un 23.40% y Colombia ocupa la tercera posición con un 5% del total de los ataques.

Para Pontiroli, los fines que se esconden detrás de estos ataques están relacionados con intereses económicos o de sabotaje, razón por la cual el sector salud y pymes han sido los principales objetivos en los que se han concentrado los delincuentes digitales.

Aunque el ransonmware se identifica como uno de los más dañinos y de mayor propagación, no deja de ser una realidad que el malware, especialmente los troyanos, ocupan la mitad de las detecciones, siendo trojan-ransom el de mayor crecimiento acelerado.

D. SE HAN REGISTRADO CUATRO ATAQUES PARA TUMBAR LA PÁGINA DE LA REGISTRADURÍA": MINDEFENSA[12]

Tres de estos ataques se originaron en Colombia y el otro en Venezuela

En rueda de prensa el ministro de defensa, Luis Carlos Villegas, comunicó a la opinión pública la identificación de cuatro ataques informáticos con los que se buscó tumbar la página web de la Registraduría Nacional del Estado Civil.

Se han registrado cuatro ataques para intentar tumbar la página web de la Registraduría, investigaciones arrojan que tres de ellos fueron desde direcciones IP en Colombia, y el otro desde una IP en Venezuela", manifestó el ministro.

Vale la pena aclarar que cuando el ministro se refiere a una 'IP' habla del número que identifica dispositivos tecnológicos, como los computadores, es decir que estos ataques fueron originarios desde este tipo de artefactos en Colombia y otro en Venezuela.

E. EE. UU. RASTREA A MAFIA DETRÁS DE LA BONANZA DEL BITCÓIN EN COLOMBIA[13]

Tras el operativo 'Tulipán Blanca' en España, se alistan capturas en el Valle y Bogotá.

Agentes antimafia del Servicio de Inmigración y Aduanas de Estados Unidos (ICE –siglas en inglés–) tienen listas las solicitudes de captura de al menos 45 colombianos vinculados a la más grande operación de lavado de activos del narcotráfico a través de bitcoines.

La primera fase de esta operación, conocida como Tulipán Blanca, se cumplió este lunes en España, en donde 11 sujetos que blanqueaban dinero de ventas de cargamentos de cocaína colombiana fueron capturados por la guardia civil y la Europol.

"Ahora, la Fiscalía y Dijín están ubicando a los enlaces en Colombia que usan una conocida red de cajeros para retirar el dinero con el que pagan los cargamentos que varias organizaciones están enviando a Europa", le explicó a este diario un agente federal.

Al parecer, los dueños de la coca operan en Meta, Arauca, Putumayo y Vichada. De hecho, desde principios de febrero varios analistas del mercado advirtieron al Diario El Tiempo

[11] https://www.elespectador.com/tecnologia/colombia-es-el-tercer-pais-mas-afectado-por-ataques-ciberneticos-en-la-region-articulo-714284

[12] https://www.elespectador.com/economia/se-han-registrado-cuatro-intentos-para-tumbar-la-pagina-de-la-registraduria-mindefensa-articulo-743295

[13] http://www.eltiempo.com/justicia/investigacion/ee-uu-rastrea-a-mafia-detras-de-la-bonanza-del-bitcoin-en-colombia-203220

sobre la existencia de grandes movimientos de la criptomoneda en esos departamentos.

Inicialmente, se creyó que se trataba de pagos de secuestros ejecutados por disidencias de las Farc, pero el Gaula de la Policía descartó esta modalidad y agencias de Estados Unidos confirmaron que se trata de una megaoperación de blanqueo de la mafia que involucra sistemas financieros de cuatro países: España, Finlandia, Panamá y Colombia.

F. GOLPE A RED DE NARCOBITCOIN QUE OPERABA EN COLOMBIA[14]

En Finlandia, la más importante plataforma de moneda virtual fue usada por la red: LocalBitcoins.com, cuya razón social está en Helsinki.

En efecto, luego de vender la coca en España y otros países europeos, parte de las ganancias en euros eran usadas para comprar los bitcoins y luego se vendían por pesos colombianos. La red alcanzó a lavar 8 millones de euros, unos 28.000 millones de pesos, que ingresaron a Colombia en la modalidad de 'goteo'.

"Decenas de personas se acercaban a los cajeros y retiraban los bitcoins, que luego eran entregados a los dueños de la mercancía. Usaron 250 puntos", explicó un investigador. Y agregó que en las búsquedas de Google, Caquetá es el departamento que más rastrea la palabra 'bitcóin'.

Estas mafias dieron el salto a la criptomoneda después de que las autoridades comenzaron a identificar las operaciones que hacían para traer los euros al país. Una narcomula fue una de las pistas.

Ya había varias alertas en los indicadores económicos. Colombia cerró 2017 y abrió 2018 como el país campeón en América Latina en el uso de bitcóin. La plataforma LocalBitcoins calcula que cada semana se transan más de 3.345 millones de pesos.

Sin embargo, a mediados de noviembre pasado se alcanzó el máximo histórico: 7.056 millones de pesos.

Para Carlos Mesa, director de la fundación Bitcoin Colombia, es difícil saber con certeza el volumen de negociación de esa moneda por tratarse de un mercado descentralizado. Además, no existe una entidad que canalice esas operaciones, que se pueden hacer a través de distintas plataformas, cajeros y persona a persona.

Mesa señala que este es un mercado en crecimiento, pese a que en los últimos meses muchas personas se han retirado debido a que el precio del bitcóin ha estado a la baja, luego del valor máximo visto a finales del año pasado, cuando rozó los 20.000 dólares por bitcóin. Hasta el lunes, el costo de esa criptomoneda estaba sobre los 6.700 dólares, en promedio.

Con base en cifras de LocalBitcoins, la agencia Bloomberg reveló que en 2017 las transacciones de divisas virtuales en pesos colombianos crecieron 1.200 por ciento, siendo el tercer país del mundo, después de China y Nigeria, y superando a Venezuela, Perú y Argentina.

G. LOS SIETE VIRUS INFORMÁTICOS MÁS DETECTADOS EN AMÉRICA LATINA[15]

Colombia, entre los países de la región con mayor índice de propagación de ransomware.

La cantidad de familias de ransomware (programa que restringe el acceso a determinadas partes del sistema infectado, y pide un rescate a cambio de quitar esta restricción) y sus variantes, ha aumentado de forma exponencial durante el 2017.

El año pasado se identificaron 1.190 variantes de familias de ransomware, que, si se comparan con las 744 registradas en 2016, muestran un incremento del 60 por ciento de un año contra otro.

Al analizar esta información, se observa que, de las 1.190 variantes identificadas en el mundo, 398 tienen presencia en Latinoamérica, lo que significa que un tercio del ransomware mundial tuvo actividad en la región, según un informe presentado por la compañía Eset.

El estudio revela que los siete ransomware más detectados en la región son: TeslaCrypt, con el 21,7 por ciento de los registros; seguido de CryptoWall (16,8 por ciento), Cerber (12,9 por ciento), Crisis (12,3 por ciento) y Locky (10,3 por ciento). El sexto lugar es ocupado por Cryptproject (8,8 por ciento), y en séptima posición aparece WannaCry con el 7,5 por ciento de las detecciones.

Perú ha sido el país con mayor cantidad de detecciones de la región durante el 2017 con el 25,1 por ciento. En otras palabras, una de cada cuatro identificaciones de ransomware en Latinoamérica se realizó en territorio Inca.

El segundo lugar lo ocupa México con el 19,6 por ciento de las detecciones, seguido de Argentina (14,5 por ciento), Brasil (14,0 por ciento) y Colombia (9,6 por ciento). La lista la complementan Chile (5,7 por ciento), Ecuador (4,6 por ciento), Venezuela (3,2 por ciento), Bolivia (2,1 por ciento) y Guatemala (1,4 por ciento), como los diez países con mayores porcentajes de detección en la región.

Del análisis de los registros de 2017, se destaca también que algunas familias tengan mayor incidencia en algunos países, tal es el caso de TeslaCrypt que ocupa el primer lugar de detecciones en países como Argentina, Chile, Colombia,

[14] http://www.eltiempo.com/justicia/investigacion/ee-uu-rastrea-a-mafia-detras-de-la-bonanza-del-bitcoin-en-colombia-203220

[15] http://www.eltiempo.com/tecnosfera/novedades-tecnologia/los-virus-informaticos-mas-populares-en-latinoamerica-195970

México, El Salvador, Panamá, República Dominicana, Paraguay y Nicaragua.

De acuerdo con Miguel Ángel Mendoza, especialista de Eset, el ransomware seguirá evolucionando debido a que es una actividad rentable para los ciberdelincuentes.

"Resulta claro que esta amenaza llegó para quedarse y las tendencias no son alentadoras; el ransomware ha venido evolucionando y aumentando en cantidad, complejidad y diversidad, puesto que se trata de una actividad rentable para los atacantes. Por ello, resulta necesario proteger la información y otros activos, de los códigos maliciosos de esta naturaleza", añadió Mendoza.

H. VAN DIEZ CASOS DE ROBO A BANCOS EN BOGOTÁ, EN LO CORRIDO DEL 2018[16]

El último se registró en un centro comercial de Bosa, la noche del martes.

Todo estaba fríamente calculado. Las primeras averiguaciones de la Policía Metropolitana de Bogotá (Mebog) indican que los ladrones que se llevaron 200 millones de pesos de un banco ubicado en un centro comercial de la localidad de Bosa, en el suroccidente, planearon con varios meses de anticipación el golpe.

Los delincuentes, según explicó el coronel Javier Martín Gámez, subcomandante de la Metropolitana, ingresaron al establecimiento bancario a las 9 de la noche del martes pasado, justo en el momento en el que los cajeros estaban cerrando las cuentas del día. "Estamos en una investigación criminal; los individuos rompen los vidrios del banco cuando los funcionarios iban a ingresar el dinero en la caja fuerte", explicó el oficial.

"Encontramos armas de juguete y seguimos con los trabajos de campo; tenemos pistas que nos pueden indicar quiénes son los responsables", agregó el coronel. Tras el asalto, los delincuentes huyeron en un automóvil, por lo que se desplegó un plan candado que contó con el apoyo del helicóptero halcón de la Mebog para capturarlos.

Como consecuencia de la presión ejercida por las autoridades, los asaltantes abandonaron el carro de placas HJV907 en una calle del barrio Brisas del Tintal, y, para intentar despistar a la policía, le prendieron fuego.

"Ellos decidieron incinerar el vehículo por la reacción rápida que los hizo abordar otro automotor o huir a pie. Estamos en la averiguación de si el carro en que iban fue hurtado", añadió el coronel Gámez.

Beatriz Cruz, una ciudadana del barrio en donde fue abandonado e incendiado el vehículo, le dijo al noctámbulo de 'Citynoticias' que la comunidad tuvo que apagar las llamas con extintores, antes de llegar el cuerpo oficial de bomberos a atender la emergencia.

La Policía Metropolitana de Bogotá anunció que ya hay hombres de los cuerpos de inteligencia adelantando las investigaciones necesarias para dar con el paradero de los responsables, además de informar sobre una recompensa de hasta cinco millones de pesos para quien dé pistas de los criminales.

Este caso es el décimo de hurtos a establecimientos bancarios que se ha presentado en lo que va del año en la ciudad, según el sistema de información estadístico, delincuencial, contravencional y operativo de la Policía Nacional (Siedco).

La cifra es alta si se tiene en cuenta que, de acuerdo con cifras preliminares del grupo de información de criminalidad (Gicri) de la Dijín, en todo el 2017 se registraron 27 atracos a entidades bancarias en la capital del país.

Ante esta situación, la Secretaría De Seguridad, Convivencia y Justicia informó que están trabajando conjuntamente con centros comerciales en la disposición de cámaras de seguridad que apunten al espacio público, con lo que se permitiría contrarrestar casos como el del banco de bosa.

En la entidad confirmaron que dentro de los más de 1.600 dispositivos de vigilancia instalados en la ciudad –que se espera sean 4.000 a diciembre de 2019–, muchos están ubicados a las afueras de centros comerciales.

I. EN EL 2018 SE PREVÉN MÁS ATAQUES CIBERNÉTICOS EN COLOMBIA QUE DEJARÍAN GRANDES PÉRDIDAS[17]

Un estudio de kaspersky lab concluyó que en Colombia los ciberataques continúan en ascenso teniendo en cuenta que el 9% de éstos en Latinoamérica son direccionados a los usuarios en Colombia. Así mismo, fueron identificados más de 500 mil ataques de phishing a nivel nacional; y frente al ataque de ransomware, que consiste en el secuestro de datos, Colombia es el tercero en la región con más riesgo. De esta manera se pronosticaron los siguientes hechos para el 2018, que se recomienda a las empresas y al gobierno, tener en cuenta para evitar grandes pérdidas económicas, físicas y humanas:

1. Adopción y uso de técnicas de ataques dirigidos (APTs) en ciberataques contra usuarios finales. Los delincuentes tendrán más herramientas para afectar al mundo.

2. Múltiples ataques hacia la banca. Los bancos de la región tendrán que enfrentar la nueva realidad de múltiples ataques con técnicas y vectores híbridos que les permitirán a los atacantes sustraer grandes sumas de dinero

3. Ciber-operaciones militares secretas en la región con el fin de sustraer información confidencial de los estados vecinos.

[16] http://www.eltiempo.com/bogota/robo-a-bancos-en-bogota-en-lo-corrido-del-2018-188314

[17] https://www.rcnradio.com/tecnologia/2018-se-preven-mas-ataques-ciberneticos-colombia-dejarian-grandes-perdidas

4. Habrá más virus para infectar a los celulares, especialmente de android.

5. Aumento de ataques a pequeñas y medianas empresas, principalmente las que manejan sistemas de puntos de venta y las encargadas de procesar transacciones de tarjetas protegidas con chip y PIN.

6. Ataques a los sistemas y usuarios de criptomonedas y abuso en el minado para su generación. El incremento en el valor de las criptomonedas ha captado la atención de los cibercriminales y esto ha causado un incremento en el número de malware diseñado para su robo.

7. Las brechas de seguridad y privacidad por medio de dispositivos conectados. El internet de las cosas cobrará mayor relevancia en el escenario de la seguridad informática a través de la inclusión masiva de dispositivos inteligentes en hogares, pasando a formar parte de nuestras vidas de forma constante.

J. EL COSTO FINANCIERO DE LOS CIBERATAQUES ESTÁ AL ALZA[18]

En los últimos años, miles de empresas a nivel mundial han aumentado de manera considerable sus inversiones en ciberseguridad, para defenderse de la también creciente ola de ciberataques que se registran a nivel global. Y es que la mayor inversión en sistemas de defensa para prevenir o mitigar ciberataques, va de la mano con el aumento del costo financiero de los mismos, como se desprende de un reciente estudio realizado por el Ponemon Institute, en colaboración con Accenture.

Según el informe en cuestión, el costo financiero del cibercrimen para las empresas, aumentó en 27,4% en 2017, con respecto al costo financiero de los ciberataques en 2016. El costo financiero de los ciberataques varía según la modalidad, pero, en términos generales, las principales afectaciones que sufren las empresas por cuenta del cibercrimen, se originan en malware, ataques a través de páginas web, denegación de servicios, filtración de información a través de empleados activos o antiguos exempleados, código malicioso que abren accesos a las plataformas corporativas, el famoso phishing – una modalidad de la denominada ingeniería social, el ransomware – o secuestro de plataformas o información,- el robo físico de dispositivos electrónicos, y los robots informáticos, conocidos también como botnets.

Por otra parte, y según algunos estudios, parte del problema que están enfrentando las compañías a nivel global, es que no saben cómo invertir apropiadamente sus recursos para defenderse de los ciberataques como corresponde. Según evidenció el Ponemon Institute, los ataques más costosos en términos financieros para las empresas que los sufren, se producen por malware y ataques dirigidos de tipo web.

Estos dos tipos de ataques, coinciden en que su objetivo es obtener acceso a información de las organizaciones. Para contrarrestar inversiones inapropiadas en sistemas de defensa de ciberataques, las organizaciones deben evaluar a profundidad el tipo de ataques a los que son más susceptibles, y consecuentemente, implementar programas al interior de las organizaciones que permitan equilibrar la relación costo-beneficio de sus sistemas de protección. Es necesario pensar en una estrategia de ciberseguridad donde las organizaciones puedan abordar estas amenazas en constante evolución tomando medidas para proteger a sus empleados, clientes y ciudadanos a largo plazo y no centrarse en una visión "fabricante-centrista".

Construir y mantener una ciberdefensa que se mantenga al día con el panorama emergente de la amenaza es un reto.

Esa tarea la debe realizar los departamentos de IT de las organizaciones, de manera conjunta con los departamentos financieros, teniendo siempre presente que un ciberataque puede resultar mucho más costoso, que la prevención del mismo, sin tener en cuenta costos como la reputación propia de las organizaciones que es algo incalculable. Las organizaciones más expuestas a los ciberataques, actualmente, son las del sector financiero, seguidas por las de servicios y energía y por las del sector aeroespacial y de defensa, entretanto, las menos expuestas se encuentran, en su orden, en los sectores de hospitalidad, educación y ciencias de la vida.

Las organizaciones son plenamente conscientes de los riesgos implícitos que representa un ataque cibernético. Más ahora tras los secuestros de información sufridos a nivel global el año pasado en decenas de organizaciones, por cuenta de dos famosos ciberataques de escalas sin precedentes. Se estima que la inversión de las empresas en defensa y prevención de ciberataques alcance una cifra de US$6 billones anuales, durante los próximos tres años.

En 2017, el incremento de las inversiones de este tipo en las organizaciones a nivel global, fue de aproximadamente 23%. Aterrizar el problema global a la realidad de Colombia resulta pertinente.

La utilización de tecnologías como seguridad adaptativa, inteligencia artificial o microsegmentación, permiten acorralar a los hackers ofreciendo fuertes barreras que deben ser articuladas de manera estratégica por las organizaciones. Esa construcción tiene un costo, pero ese costo puede ser mucho menor de lo que le puede valerle a una organización, un ataque criminal que sea cometido en internet.

K. EMPRESAS COLOMBIANAS VULNERABLES A CIBERATAQUES[19]

Según la más reciente encuesta global de seguridad de la Información desarrollada por EY, las organizaciones en todo el mundo saben del riesgo de sufrir ataques. El 56% de ellas están

[18] https://www.larepublica.co/internet-economy/el-costo-financiero-de-los-ciberataques-esta-al-alza-2598128

[19] https://www.kienyke.com/emprendimiento/empresas-colombianas-son-vulnerables-a-ciberataques

preocupadas por el creciente impacto de las ciberamenazas para sus estrategias y planes de negocios.

Debido al incremento en la conectividad dentro de las organizaciones, por el aumento del uso de dispositivos, se ha introducido nuevas vulnerabilidades. Puntualmente en Colombia, el 78% de las empresas invierte menos de un millón de dólares anuales en estrategias para evitar ataques informáticos.

Las empresas deberían invertir más para proteger su información y la de sus clientes. Juan Mario Posada experto en ciberseguridad afirmó que: "La definición de políticas de ciberseguridad requiere de una comprensión global del negocio de cada empresa y de su entorno".

Aseguró que, sin la definición, las medidas adoptadas podrían ir en contravía de los objetivos estratégicos de la compañía, que en consecuencia genera un enfoque reactivo para enfrentar los problemas. Enfatizó que actualmente la infraestructura tecnológica representa la mayoría del conocimiento empresarial.

Por otro lado, el 73% de las empresas colombianas considera que el conocimiento de sus juntas directivas sobre seguridad de la información y la importancia de protección de la información son insuficientes, lo cual reduce la capacidad de acción de una organización en caso de ataques.

Esta falta de conocimiento se debe al poco presupuesto. El 47% de los encuestados aseguró que ese es su principal obstáculo. Otro de los inconvenientes es la ausencia de talento capacitado y de consciencia ejecutiva sobre la importancia de la protección.

Las principales amenazas percibidas por los ejecutivos fueron los hacktivistas y los empleados maliciosos o descuidados. La proliferación de dispositivos móviles y portátiles expone la información a más riesgos, entre ellos robos y uso inadecuado.

De igual manera, el 42% de las empresas colombianas no cuenta con un grupo de trabajo específico o un centro de operaciones de ciberseguridad que monitoree el comportamiento, amenazas y ataques a sus sistemas de información.

Esto resulta una cifra alta, aún más considerando que el 36% de las compañías solo detectaron incidentes de seguridad cuando un empleado que no es del área de tecnología las detectó.

L. PREPÁRATE ANTE UN CIBERATAQUE[20]

Poner en práctica los conocimientos de expertos podría evitar ser víctima de un ataque cibernético.

La tecnología y su adopción facilitan las relaciones y la vida de los individuos, pero también las de las empresas. Sin embargo, la digitalización conlleva una responsabilidad, si lo que se busca es evitar ser víctima de un ciberataque.

Lucas Paus, investigador de ciberseguridad de ESET, asegura que hay formas de evitar un ciberataque, y sobre todo arruinar al delincuente al frustrarle sus intentos de vulnerar la seguridad cibernética de una compañía.

Recomienda siempre actualizar la solución de seguridad, aplicaciones y sistema operativo. "Las actualizaciones no sólo arreglan errores, si no también fallos y brechas de seguridad. Estar al día con estos aspectos evita que los atacantes exploten las vulnerabilidades conocidas en dichos sistemas.

"Hay que instalar soluciones de seguridad en todos los dispositivos. Esto sirve para proteger desde la computadora, smartphone, tablets y demás dispositivos que se usan en el día a día. Un firewall y antivirus detectará múltiples amenazas como troyanos u otro tipo de malware, evitando fugas o robos de información.

"Además, hay que realizar una copia de seguridad periódicamente de toda la información. Un disco externo puede servir, pero se debe asegurar de no mantenerlo conectado todo el tiempo, ya que, si se es víctima de ransomware, la información de este dispositivo también puede verse comprometida y cifrada. Contar con un respaldo es un as bajo la manga para no pagar por un rescate de la información", explica Paus.

Otra de las maneras para frenar los ataques informáticos es la pronta denuncia de los correos con phishing. "Está práctica es la favorita de los cibercriminales, ya que las personas son el factor más vulnerable en la cadena de seguridad. Para frenar esta amenaza, es muy importante denunciar los sitios de phishing desde los navegadores utilizados, e inclusive reportarlos al programa de antivirus en caso de que no los reconozca".

Paus señala que es importante actualizar las contraseñas y asegurarse de que siempre sean más fuertes y complejas de descifrar. "Debe de contar con mayúsculas, números y signos y, mientras más larga, es mejor."

Muchos especialistas consideran necesario en estos días activar siempre el segundo factor de autentificación.

"Los servicios en línea cuentan con esta medida extra de seguridad que frecuentemente requiere de un código obtenido a partir de una aplicación, o un mensaje SMS, además de una contraseña para acceder a los servicios. A ello hay que sumarle checar la privacidad en las redes sociales, y evitar siempre subir información sensible a plataformas como Facebook", agrega Paus.

Finalmente, el especialista de ESET comenta que hay que verificar los estados de cuenta del banco, y poner atención a anomalías o transacciones desconocidas.

[20] http://www.siliconweek.com/software/preparate-ante-ciberataque-95574

IX. CONCLUSIONES

Conocer que la ciberseguridad se encarga en defender el uso del ciberespacio de los ciberataques sobre los riesgos de mayor impacto, que son menos probables en el ciberespacio, y que la seguridad informática es la encargada de proteger, de contar con las medidas y controles que garanticen la confidencialidad, integridad y disponibilidad de activos del sistema de información, incluido hardware, software e información que se procesa, almacena y comunica en una organización o Nación.

Identificar que existen áreas tan importantes como lo son la seguridad informática y la ciberseguridad, que mitigan los ciberataques de la Nación.

Identificar que existen áreas a nivel de empresa o Nación orientadas a la protección de los datos críticos y de la protección de infraestructuras críticas.

Identificar la importancia que tiene contemplar la posibilidad de crear estas grandes áreas de ciberseguridad y seguridad informática en las organizaciones, para lograr una mayor protección de la información.

Reconocer que la seguridad informática es la encargada de administrar las herramientas de seguridad perimetral, para contribuir en la protección del ciberespacio siendo ésta un complemento de la ciberseguridad.

Conocer las infraestructuras críticas en la organización, permite identificar cuáles serían los controles más apropiados para mitigar los riesgos.

La existencia de los riesgos asociados al core de la compañía o Nación cada vez va en aumento según las cifras expuestas por kaspersky, lo que significa que el auge de la ciberseguridad apenas comienza, y es donde las áreas de seguridad tendrán que estar más preparadas para los ciberriesgos que hasta ahora se están identificando gracias a las grandes herramientas de seguridad con las que hoy en día se cuentan.

Autor

Carlos Mario López Duque, nacido en el año 1986 en Manizales Caldas Colombia; ingeniero de sistemas y telecomunicaciones, graduado de la Universidad Manizales, estudia para optar por el título especialista en seguridad informática en la Universidad Piloto de Colombia.

Trabaja en el Banco AV Villas hace 4 años como analista en seguridad informática, administra herramientas de monitoreo de seguridad de la información y análisis de vulnerabilidades en las plataformas de infraestructura.

REFERENCIAS

[1] Internet – Auditoria y seguridad TI – Online – Disponible en https://m.isaca.org/chapters8/Montevideo/cigras/Documents/cigras%202013%20-%20auditora%20y%20seguridad%20de%20ti%20-%20estado%20del%20arte%20y%20aplicacin%20en%20entidades%20bancarias%20nicols%20serrano.pdf

[2] Internet – El Espectador Tecnología – Online – Disponible en https://www.elespectador.com/tecnologia

[3] Internet – Asociación Colombiana de Ingenieros de Sistemas – Online – Disponible en http://acis.org.co/

[4] Internet – Information Systems Audit and Control Association – Online – Disponible en https://www.isaca.org/

[5] Internet – Departamento Nacional de Planeación – Gobierno de Colombia – Online – Disponible en https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

[6] Internet – National Institute of Standards and technology – Online – Disponible en https://www.nist.gov/

[7] Internet – Noticias Caracol – Online – Disponible en https://noticias.caracoltv.com/

[8] Internet – Noticias El Tiempo – Online – Disponible en http://www.eltiempo.com/buscar?q=ciberataque

[9] Internet – Noticias RCN – Online – Disponible en https://www.rcnradio.com/tecnologia

[10] Internet – La República – Online – Disponible en ¨ https://www.larepublica.co/internet-economy/el-costo- financiero-de-los-ciberataques-esta-al-alza-2598128