CASOS DE ESTUDIO DE CIBERCRIMEN EN COLOMBIA

NANCY ADRIANA GONZÁLEZ
ESTUDIANTE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO EN SEGURIDAD INFORMÁTICA II
PASTO – NARIÑO
2020

CASOS DE ESTUDIO DE CIBERCRIMEN EN COLOMBIA

NANCY ADRIANA GONZÁLEZ
Estudiante

MONOGRAFIA

KATERINE MARCELES VILLALBA
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO EN SEGURIDAD INFORMÁTICA II
PASTO – NARIÑO
2020

Nota de aceptación

Firma presidente del jurado

Firma del jurado

Firma del jurado

Pasto, 28 de Agosto del 2020

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZA: Es la posibilidad que ocurra cualquier acción o evento que atente contra la seguridad de la información, aprovecha una vulnerabilidad en un sistema y puede generarse a través de ingeniería social, cuando no hay correcta capacitación y concientización de los usuarios o por el interés de los intrusos de provocar ataques.[1]

ATAQUE: Aprovechar las vulnerabilidades para ingresar con el objetivo de destruir, exponer, alterar o inhabilitar un sistema informático, la información que almacena o la red. Generalmente es provocado por delincuentes informáticos que realizan espionaje, suplantación de identidad entre otros. Utilizan las vulnerabilidades o fallas del software o hardware para tener el control. [2]

BOTNET: Se refiere a un grupo de PC infectados y controlados por un atacante de manera remota. Por lo general un hacker o grupo de ellos crean un botnet utilizando un malware el cual infecta a un grupo de computadores los cuales son parte del botnet llamados bots o zombies. [3]

DENEGACIÓN DE SERVICIO: El objetivo de este ataque es inhabilitar un sistema, una aplicación o una red bloqueando los servicios que ofrece, de esta manera impide que los usuarios legítimos puedan tener acceso, es causado por la saturación de los puertos con flujo de información, esto genera la sobrecarga de los servidores e imposibilita que presten los servicios.[4]

---

[1] MARTINEZ FERREL, Ernesto. Las diferentes amenazas de seguridad informática. {En línea}. 2018. Disponible en: https://sites.google.com/site/lasamenazaslainformatica/

[2] ECURED. Ataque informático. {En línea} Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

[3] Kaspersky. ¿Qué es un botnet? {En línea}. 2013. Disponible en: https://www.kaspersky.es/blog/que-es-un-botnet/755/

[4] COMPUCHANNEL. ¿Qué es un ataque de denegación de servicio? {En línea}. 2018 Disponible en: https://www.internetya.co/ataques-de-denegacion-de-servicio-ddos-un-riesgo-real/

EXPLOIT: Es un tipo de ataque que aprovecha las vulnerabilidades de aplicaciones, redes o hardware para obtener el control de un sistema o robar los datos que están en la red. Cuando en un software existen errores de programación los intrusos pueden utilizan estas debilidades para controlar o infectar un sistema.[5]

GROOMING: Es un engaño que realiza una persona adulta para ganarse la confianza de un menor de edad y abusar de ellos, puede presentarse personalmente o a través de internet generalmente se realiza en redes sociales. El acosador trata de apartar a la víctima de las personas que lo pueden apoyar como familiares o amigos para que se encuentra más vulnerable.[6]

RANSOMWARE: Tipo de malware que bloquea archivos, sistemas informáticos o dispositivos y solicita un rescate para recuperar la información. Se pueden infectar a través de correos SPAM que contienen archivos adjuntos o enlaces a sitios web maliciosos. También se pueden infectar por ingresar a publicidad maliciosa. [7]

SEGURIDAD DE LA INFORMACIÓN: Medidas, herramientas y controles preventivos que deben tener en cuenta los individuos, organizaciones y tecnologías para proteger la información, con el fin de preservar la confidencialidad, autenticidad e integridad de los datos [8]

---

[5] AVAST. Exploits. {En línea}. 2020. Disponible en: https://www.avast.com/es-es/c-exploits

6 Save the children. Grooming que es, como detectarlo y prevenirlo. {En línea} Disponible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

[7] MALWAREBYTES. Ransomware. {En línea} 2019. Disponible en: https://es.malwarebytes.com/ransomware/

[8] UNIVERSIDAD LIBRE. Seguridad de la información {En línea}. Bogotá. 2015 Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

SPAM: Son correos que llegan a las cuentas sin haber sido solicitados y se envían automáticamente, se conoce también como correo basura, se utilizan para hacer publicidad o propagar el malware.[9]

SPYWARE: Es una clase de malware que espía en el equipo informático o la red para tener acceso a información personal y confidencial. Se encarga de recolectar la información sobre las acciones que realiza un usuario con frecuencia, el historial de navegación o la información personal para enviarla a terceros sin que el usuario lo perciba. Un ejemplo de este tipo son los keyloggers los cuales se encargar de monitorizar las pulsaciones del teclado. [10]

TROYANO: Programa malicioso que se presenta a los usuarios como software legítimo, se utiliza por los ciberdelincuentes para acceder a los sistemas, a través de ingeniería social engañan a la víctima para que cargue y ejecute el troyano, cuando se activa los ciberdelincuentes pueden espiar, robar información o tener acceso al sistema por puertas traseras para eliminar, bloquear, modificar, copiar datos o interrumpir el rendimiento de los computadores o la red. [11]

VIRUS INFORMÁTICO: Son programas que alteran el funcionamiento de un sistema, sin que el usuario se percate de esto, generalmente infectan archivos para destruirlos o modificarlos, algunos causan daños graves y otros solo son molestos. Los virus pueden propagarse por medio de software y se pueden copiar de un archivo o computador a otro automáticamente.[12]

VULNERABILIDAD: Debilidad o falla de un sistema informático que deja en riesgo la seguridad de la información, es necesario detectarla y eliminarla lo más pronto

---

[9] SoftwareLab ¿Qué es el SPAM? {En línea} 2020. Disponible en: https://softwarelab.org/es/que-es-spam/

[10] SEGUIN Patrick. Spyware. {En línea} AVAST.2020. Disponible en: https://www.avast.com/es-es/c-spyware

[11] Kaspersky. ¿Qué es un virus troyano? {En línea} Disponible en: https://www.kaspersky.es/resource-center/threats/trojans

[12] TORRES Gonzalo. ¿Qué es un virus informático? {En línea} AVG. 2017. Disponible en: https://www.avg.com/es/signal/what-is-a-computer-virus

para evitar daños graves, se pueden presentar por fallas de diseño, de configuración o falta de procedimientos.[13]

[13]INCIBE. Amenaza vs Vulnerabilidad {En línea}. 2017. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

RESUMEN

En Colombia el cibercrimen es uno de los delitos que ocurre con mayor frecuencia ya sea por estafas, robo de información, suplantación de identidad entre otros, que no solo afecta a personas que utilicen este medio sino que el mayor interés para los intrusos son las empresas y aunque utilicen herramientas para evitar estos ataques, los ciberdelincuentes están atentos ante cualquier vulnerabilidad causando grandes pérdidas, ya que la mayoría de información de las empresas está en los sistemas informáticos y en la red.

En las empresas existe una gran amenaza referente a delitos informáticos sobre todo en el sector financiero, los ciberdelincuentes aprovechan los medios tecnológicos para no ser reconocidos fácilmente y obtener los datos confidenciales que manejan las empresas utilizándolos para su beneficio.

Existen diferentes investigaciones y noticias que informan a diario sobre los delitos informáticos, es necesario conocer las nuevas modalidades de los ciberdelincuentes para asegurar la información antes de presentarse un ataque.

Esta monografía se basa en conocer los delitos informáticos que más han afectado a las empresas de Colombia y las recomendaciones que se deben tener en cuenta para evitar ser víctimas del cibercrimen

Palabras clave: delitos informáticos, ataques, robo de información, estafas, vulnerabilidades.

ABSTRACT

In Colombia, cybercrime is one of the crimes that occurs most frequently, be it due to scams, information theft, identity theft, among others, which not only affects people who use this medium, but the companies are of greatest interest to intruders. And even if they use tools to avoid these attacks, cybercriminals are alert to any vulnerability causing great losses, since most of the companies' information is on computer systems and on the network.

In companies, there is a great threat related to computer crimes, especially in the financial sector, cybercriminals take advantage of technological means to not be easily recognized and obtain the confidential data that companies handle, using them for their benefit.

There are different investigations and news that report daily on computer crimes, it is necessary to know the new modalities of cybercriminals to secure the information before presenting an attack.

This monograph is based on knowing the computer crimes that have most affected Colombian companies and the recommendations that must be taken into account to avoid being victims of cybercrime.

Keywords: computer crimes, attacks, information theft, scams, vulnerabilities.

INTRODUCCIÓN

La información es uno de los activos más importantes para las empresas y es considerada uno de los recursos vitales, la manera que es utilizada puede generar ganancias o pérdidas significativas a la organización, por lo tanto, se debe preservar la seguridad de la misma, para lo cual se cuenta con gran variedad de factores como crear periódicamente respaldos de la información, cuidar las acciones del factor humano o tener herramientas y mecanismos para proteger los datos. Los criminales muchas veces utilizan los medios tecnológicos para cometer acciones ilícitas, porque es más difícil identificarlos, por lo tanto, se debe contar con medidas preventivas, aunque estas no evitan completamente un riesgo si pueden reducir la probabilidad de ser víctimas de los ciberdelincuentes. A pesar de los beneficios que brinda la tecnología también es un entorno en el que se desarrollan actos delictivos. Para comprender la problemática del cibercrimen, es necesario conocer la forma de actuar de un criminal informático, no se debe confiar en todo lo que brinda internet, donde los intrusos pueden engañar a sus víctimas con publicidades falsas o sitios web que pueden dirigir a páginas no oficiales y que no son auténticas, ataques de malware o robos de información. También se debe conocer las leyes que pueden proteger y brindar apoyo a las víctimas de estos delitos ya que penalizan las acciones incorrectas de los delincuentes informáticos. Actualmente existen muchas vulnerabilidades que afectan la información y que han aumentado cada año, dado que a medida que avanza la tecnología los intrusos también encuentran nuevas formas y medios para afectar, modificar o ingresar a la información confidencial. El cibercrimen es una problemática a nivel mundial y es un tema bastante amplio, por tal razón este proyecto se enfoca en las empresas colombianas con el fin de comprender la importancia de la formación de cultura informática segura para sus empleados y de esta manera se pueda minimizar los riesgos, finalmente se mencionan casos

reales ocurridos en empresas colombianas con el fin de dimensionar las pérdidas que puede ocasionar la delincuencia informática.

1 DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Los sistemas informáticos y la tecnología a medida que evolucionan son más indispensables para la sociedad, ya que los usuarios centran sus actividades en estos medios y les facilita la realización de diferentes funciones; sin embargo, existen problemas de seguridad que se han evidenciado por que los intrusos aprovechan la confianza, el descuido o falta de conocimiento de los usuarios para lograr obtener información confidencial o ingresar a los sistemas que los usuarios utilizan.

Principalmente existe una gran problemática en cuanto a los riesgos que se enfrentan las empresas, por lo tanto, es importante implementar los controles necesarios para asumir un ataque de un ciberdelincuente.

En la actualidad el cibercrimen es uno de los delitos más perseguidos por la policía, con la aparición de internet los delitos informáticos han representado un riesgo que va en contra de la privacidad de las personas desde suplantación de identidad hasta robar completamente su información, lo cual genera pérdidas para grandes y pequeñas empresas hasta personas comunes que manejan datos importantes desde sus hogares, pueden llegar a ser víctimas de estos delitos por falta de herramientas y conocimiento en seguridad.

Entre los delitos más frecuentes utilizados por los ciberdelincuentes están las estafas, phishing y la suplantación de identidad además del ransomware que es uno de los malware más reconocidos por encriptar la información de sus víctimas y extorsionarlos si desean recuperar sus datos de lo contrario son eliminados.[14]

14 INFOLAFT. Lo que debe saber sobre el cibercrimen en Colombia {En línea} 2014. Disponible en https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

En cuanto a la problemática del cibercrimen existen dos campos que lo abordan el primero es: el **derecho** referente al delito que se cometió y que debe ser sancionado, este es un ámbito bastante amplio, ya que aún existen estudios para determinar qué acciones pueden ser consideradas delito informático y el campo de **seguridad informática** se refiere a las herramientas, técnicas y prácticas en cuanto a conceptos técnicos y preventivos que se deben tener en cuenta para minimizar los riesgos, se centra en la protección de los sistemas tanto para software como hardware, vulnerabilidades en programas, problemas de seguridad e incidentes informáticos de todo tipo. [15]

El cibercrimen es un problema constante que afecta la privacidad y trae grandes pérdidas a los diferentes sectores de las empresas. Colombia es uno de los países más afectados, las denuncias más frecuentes son por fraudes bancarios, compra de productos o suplantación de identidad.[16]

Existe una alternativa que favorece a las víctimas de los delitos informáticos, la cual se refiere a penalizar las acciones inadecuadas con respecto a la violación de la privacidad de las personas en el mundo cibernético, en Colombia se han creado leyes y normas que sancionan los actos que no son permitidos en el entorno informático, de manera que puedan regular las acciones de los criminales, debido al uso inadecuado de los medios tecnológicos.

[15] Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Compilado por Ricardo Antonio Parada; José Daniel Errecaborde. - 1a Ed {En línea} Ciudad Autónoma de Buenos Aires. Erreius, 2018. Disponible en: http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

[16] Peña Juliana. Legislación aplicable a las conductas delictivas en internet {En línea} Disponible en http://bibliotecadigital.usbcali.edu.co/bitstream/10819/737/1/Legislacion_Aplicable_Conductas_Pena_2009.pdf

1.2 FORMULACIÓN DEL PROBLEMA

En la presente monografía se analizan los delitos informáticos más frecuentes en Colombia, algunos casos reales que han afectado a las empresas, así como a los usuarios, las sanciones que pueden recibir los ciberdelincuentes y las recomendaciones para minimizar los riesgos. Es importante tener en cuenta las nuevas técnicas que utilizan los ciberdelincuentes e informar a las empresas de los riesgos más frecuentes para que puedan optar por las mejores alternativas para contrarrestar los ataques, ya que les ayudará a diseñar planes de contingencia que minimicen el impacto que puede causar la pérdida de información o el daño de los sistemas.

A partir de lo anterior, se llega a generar el siguiente interrogante: ¿Cómo afecta el cibercrimen a las empresas de Colombia y como minimizar los riesgos?

2 JUSTIFICACIÓN

Los delitos informáticos se incrementan en la misma medida que evoluciona la tecnología, las víctimas pueden llegar a ser usuarios comunes que realizan tareas básicas, que por falta de conocimiento reciben un ataque o grandes empresas con información confidencial son vulnerables a los fraudes, virus informáticos, o cualquier tipo de delito que se encuentre en la red, lo cual puede causarles grandes pérdidas.

Es necesario que Colombia se compare con otros países para analizar esta problemática y que sea una de las prioridades combatir la delincuencia informática, ya que existen amenazas informáticas no solo en Colombia sino a nivel mundial. Empezando por cada persona que utilice los medios tecnológicos correctamente puede aportar a la seguridad si tiene el conocimiento necesario y lo práctica, implementando en sus actividades diarias simples normas de seguridad hasta utilizar herramientas más avanzadas que le ayuden a mitigar los riesgos.

En las empresas la información se considera como uno de los activos más importantes, por tal razón es el principal objetivo para los ciberdelincuentes y la manera de obtenerla cada día es más novedosa, los delincuentes informáticos buscan nuevas maneras de conseguir la información sin ser reconocidos, pueden manipularla fácilmente atentando contra la privacidad de las personas tanto física como moral. Si bien es cierto que la responsabilidad de la seguridad de la información es de los usuarios, las empresas deben concientizar a sus empleados, utilizar mecanismos e invertir lo necesario en los servicios de las tecnologías de la información y las herramientas para protegerlos, garantizando la confiabilidad, disponibilidad e integridad a sus clientes, empleados y las actividades que realizan.

Las empresas deben controlar la privacidad de la información y su seguridad depende de las mismas, es necesario que inviertan en la protección de los datos y no subestimen los gastos, esto puede ser mínimo comparado con las pérdidas que

les puede generar cualquier delito informático en el momento de no tener disponible la información, principalmente se debe reconocer que es una realidad que afecta a cualquier empresa, aunque no se puede tener un sistema completamente seguro es necesario implementar herramientas y mecanismos de seguridad para reducir riesgos.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar la problemática que tienen las empresas colombianas respecto al cibercrimen y proporcionar recomendaciones para mitigar los riesgos

3.2 OBJETIVOS ESPECÍFICOS

- Analizar el impacto negativo que genera la ciberdelincuencia para las empresas colombianas.

- Presentar estadísticas de ciberdelitos del año 2019 en comparación el con años anteriores generados en Colombia.

- Brindar recomendaciones necesarias para prevenir, controlar y regular las vulnerabilidades en los sistemas informáticos para afrontar las amenazas y riesgos en contra de la ciberseguridad

- Presentar mecanismos de concientización a los usuarios y empresas de la importancia de aplicar herramientas y normas de seguridad que fortalezcan la privacidad y confianza que pueden brindar los sistemas informáticos para minimizar los riesgos.

4 MARCOS DE REFERENCIA

4.1 MARCO TEÓRICO

El cibercrimen se deriva de las palabras ciber y crimen. Ciber según el sitio de significados.com es un prefijo que se utiliza para términos relacionados con internet. Crimen es un delito o acción grave que va en contra de la ley y es penalizada. Algunos de los delitos comunes del cibercrimen son propagación de virus, descargas ilegales, phishing, robo de información entre otros. Teniendo en cuenta lo anterior se puede definir el cibercrimen como las actividades delictivas donde los intrusos utilizan como medio un sistema informático o redes para cometer sus acciones. [17]

La evolución que ha tenido la tecnología ha permitido el desarrollo y mejora de la sociedad; sin embargo, existen problemas de seguridad que representan lo negativo dando paso al cibercrimen, donde algunas veces los delincuentes informáticos utilizan técnicas ya reconocidas que pueden ser detectadas pero la mayoría de veces difícilmente se pueden reconocer ya que borran cualquier evidencia. Los atacantes encuentran cada vez mecanismos más avanzados para ingresar a la información, en algunos casos hasta solicitan dinero para recuperarla.

Los delitos informáticos contienen diferentes tipos de actividades ilegales y es difícil hacer una clasificación incluso a diario pueden aparecer nuevas formas delictivas; sin embargo, según el Convenio sobre la ciberdelincuencia del consejo de Europa realiza una clasificación aproximada de 4 tipos de infracciones:[18]

[17] Significados.com. Ciber. {En línea} 2015. Disponible en: https://www.significados.com/ciber/

[18] Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Compilado por Ricardo Antonio Parada; José Daniel Errecaborde. - 1a Ed {En línea} Ciudad Autónoma de Buenos Aires. Erreius, 2018. Disponible en: http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

- **Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos:** en este tipo de delitos se encuentran los accesos ilícitos, espionaje, manipulación de datos entre otros
- **Delitos según su contenido:** racismo, en contra de la religión, juegos ilegales, difamación entre otros.
- **Delitos según infracciones**: de la propiedad intelectual y derechos afines.
- **Delitos informáticos:** fraudes, falsificaciones, suplantación de identidad, utilizar dispositivos sin permiso.

La ciberdelincuencia afecta a organizaciones así como a usuarios comunes, pero las más afectadas han sido las pequeñas empresas, ya que por contar con un sistema de seguridad básico o nulo pueden los intrusos conseguir más fácil la información y afectar a los clientes de la misma manera o aprovechar las vulnerabilidades para obtener sus beneficios. A pesar de ser los medios virtuales una gran ayuda para las empresas, debido a que permiten fortalecer sus finanzas, por medio de la implementación de redes y sitios web, existen riesgos que las afectan.

Según investigaciones de las cifras más recientes del Centro Cibernético de la Policía Nacional para minimizar los riesgos de ataques como suplantación de tarjetas SIM, vishing, fraudes por whatsapp, fraudes de criptomonedas, ransomware entre otros, empresas colombianas invirtieron alrededor de 190 mil millones de pesos en el año 2017. [19]

Los intrusos se han interesado especialmente por empresas del sector financiero donde han realizado estafas, suplantaciones, vishing, fraudes, robos de información entre otros. Las empresas que utilizan más las tecnologías informáticas están más propensas a los ataques informáticos, ya que sus empleados seguramente no han sido suficientemente capacitados sobre los

[19] EL TIEMPO. Cibercrimen le cuesta a Colombia 190.000 millones de pesos al año. {En línea} 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesos-al-ano-380830

riesgos que puede provocar la descarga de archivos, abrir correos desconocidos o brindar información confidencial, de esta manera se aprovechan los intrusos para conseguir la información o enviar algún tipo de malware, en este sentido la mayor vulnerabilidad para las empresas la representan sus empleados. [20]

Según Jay García arquitecto de la firma Controles Empresariales “en Colombia los casos de cibercrimen han aumentado cerca del 28% cada año de acuerdo a reportes del Centro Cibernético Policial, donde afecta en gran parte la seguridad y privacidad de los usuarios.” [21]

Según el coronel y consultor internacional de ciberseguridad Fredy Bautista “el cibercrimen es uno de los delitos donde los criminales obtienen mayor beneficio, desafortunadamente por esta situación en el 2022 se podría generar hasta 8000 millones de dólares en pérdidas para las empresas” [22] también se refirió a las tendencias del cibercrimen: “Los ataques estarán centrados en inteligencia artificial donde las empresas podrían recibir audios o videos suplantando a ejecutivos, clientes y proveedores para conseguir transferencias de dinero. Falsos perfiles en redes sociales para difusión de malware, uso de Botnet para la difusión de correos extorsivos e incluso, uso de mercados ilegales en Darknet que funcionan para la venta de datos bancarios en internet. Este tipo de amenazas son llamados de alerta para que las compañías se preparen ante cualquier incidente”[23]

---

[20] Idem

[21] GARCIA Jay, Cibercimen le cuesta a Colombia más de $190 mil millones de pesos al año. Citado por: EL TIEMPO. Distintos ataques afectan a empresas y agencias gubernamentales en Colombia. {En línea} 2019 Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesos-al-ano-380830

[22] BAUTISTA Fredy. Colombia el país con más ransomware en Latinoamérica en 2018. Citado por: ARIAS Diana. {En línea} 2019. Disponible en: https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/

[23] BAUTISTA Fredy. Tendencias del cibercrimen en Colombia 2019-2020. Citado por TicTac. {En línea} 2019. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

En Colombia se obtuvieron las siguientes cifras: [24]

- En el 2018 se obtuvieron 21687 casos de delitos informáticos, un 36 % más que en el 2017
- Diariamente se denuncian alrededor de 60 casos de ciberataques realizados tanto a ciudadanos como a empresas
- El 25 % de ataques se realizan a empresas financieras.
- Lastimosamente existen casos de ciberataques que no son denunciados por miedo de las víctimas.

Según encuestas realizadas por el Índice de Seguridad Unisys en 2019, Colombia registro el segundo nivel más alto respecto a la preocupación por la seguridad en la ciberdelincuencia, en el primer nivel esta Filipinas. De acuerdo a la encuesta el 90% de los colombianos manifestó la mayor preocupación sobre el acceso o uso de la información de sus tarjetas de crédito, luego sobre robo de identidad y al 87% le reocupa el acceso a su información personal. [25]

Un ejemplo de lo anterior, es el caso de phishing que ocurrió en el año 2017 en Bancolombia, en el cual se pretendía estafar a los usuarios del banco, utilizando el nombre y la imagen de la empresa, donde a los usuarios les llegaba un correo desde la cuenta informacion@bancolombia.com.co informando que la cuenta del cliente fue bloqueada por intentos fallidos realizados anteriormente, para restaurar la cuenta les solicitaba ingresar de inmediato a un enlace enviado por el intruso donde deberían proporcionar sus datos y de esta manera pretendían robar información.[26]

---

[24] ARIAS Diana. Colombia el país con más ransomware en Latinoamérica en 2018. {En línea} 2019 Disponible en: https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/

[25] DECIDEO. 90% de los colombianos está seriamente preocupado por el fraude de tarjetas bancarias" {En línea} 2019. Disponible en: https://www.decideo.com/90-de-los-colombianos-esta-seriamente-preocupado-por-el-fraude-con-tarjetas-bancarias-Nuevo-Indice-de-Seguridad_a2311.html

[26] DINERO. Suplantando a Bancolombia para estafar clientes. {En línea} 2017. Disponible en: https://www.dinero.com/empresas/articulo/campana-de-phishing-afecta-a-miles-de-clientes-de-bancolombia/242871

4.2 MARCO CONCEPTUAL

4.2.1 Ataques más comunes en el ciberespacio Colombiano: Para profundizar en el tema se deben conocer los ataques más comunes que se presentan y su origen. Estos ataques pueden afectar a empresas, usuarios comunes, hasta estados y sociedades, es una de las amenazas más significativas para el mundo. Por lo tanto, se debe priorizar la seguridad en este entorno sobre todo cuando las actividades que se realizan y la información que se utiliza dependen del uso de la red y los sistemas informáticos.

De acuerdo con la información de la revista portafolio en el año 2018, según investigaciones de la compañía tecnológica Microsoft, Colombia se encontraba en el segundo país de América Latina más expuesto a riesgos de delitos informáticos. En la investigación de la revista portafolio además se encontró que en Colombia el 12% de sistemas móviles han sido atacados por malware[27]

Según la revista Semana en un artículo publicado en 2019 de acuerdo a un estudio realizado a 60 países, Argelia obtuvo el primer puesto con respecto a problemas de seguridad informática y Colombia ocupaba el puesto 39, es decir para el año 2019 la seguridad en Colombia era regular[28].

A continuación, se definen los diferentes ataques más comunes en el ciberespacio Colombiano y temas relevantes del cibercrimen:

4.1.1.1Ataques bancarios: Los intrusos centran su atención en las entidades bancarias, ya que obtienen beneficios lucrativos, además pueden obtener información privada que los beneficia. A pesar que las empresas utilizan mecanismos de seguridad los intrusos emplean técnicas para engañar a sus

[27] PORTAFOLIO. Colombia es el segundo país latinoamericano con mayor riesgo de conducta negativa en internet. {En línea} 2018. Disponible en: https://www.portafolio.co/tendencias/trucos-con-los-que-buscan-hacerle-el-quite-al-reconocimiento-facial-536538

[28] SEMANA. Así esta Colombia en el ranking de ciberseguridad mundial. {En línea} 2019. Disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

víctimas como: ingeniería social o ataques de malware. Según un informe de Digiware de ataques dirigidos al sector financieros en Colombia y América Latina, aproximadamente al mes un banco podría recibir hasta 10 ataques cibernéticos en su infraestructura y los daños causados a estas empresas podrían estar entre 97.000 a 268.000 millones de dólares anuales. Por esta razón se está considerando brindar un seguro por riesgo cibernético[29]

4.1.1.2 Cibercrimen: Se refiere a conductas inadecuadas consideradas como delitos realizados en el ciberespacio. Entre estos podemos encontrar suplantación de identidad, robo de información, fraudes, estafas entre otros. No solo afectan la privacidad y la economía, también perjudican la integridad de las personas víctimas de estos delitos. De acuerdo con Digiware en Colombia existen casos de fraudes a través de correos electrónicos realizados a entidades financieras con un 39%, telecomunicaciones 25%, gobierno 15% industria 9%, sector energético 3%, correspondientes a ataques diarios. Las denuncias más frecuentes han sido por transacciones bancarias, compra de productos o suplantación de identidad. Para evitar este tipo de delitos se recomienda a los usuarios no realizar transacciones con colaboración de otras personas, cuando se presenta inconvenientes dirigirse directamente a la entidad bancaria, no ingresar a los links que llegan a los correos electrónicos aparentemente emitidos de las entidades. [30]

4.1.1.3 Ciberespacio: Es un entorno no físico creado por equipos computacionales unidos para interoperar en una red, las personas que se conectan a estos equipos pueden interactuar como en el mundo real sin estar presentes físicamente, además las personas pueden comprar en línea, compartir información, explorar entre otros. [31]

---

[29] VALBUENA Sindy. Bancos en Colombia pueden recibir hasta 10 ataques cibernéticos al mes {En línea} 2018. Disponible en: https://www.rcnradio.com/tecnologia/bancos-en-colombia-pueden-recibir-hasta-10-ataques-ciberneticos-al-mes

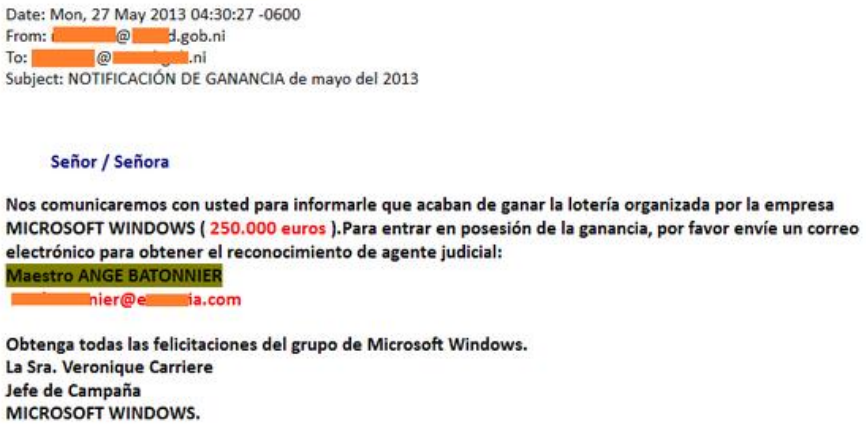
[30] UID. Delitos informáticos en Colombia. {En línea} 2020. Disponible en: http://uid.org.co/delitos-informaticos-en-colombia/

[31] ECURED. Ciberespacio. {En línea} 2020. Disponible en: https://www.ecured.cu/Ciberespacio

4.1.1.4 Estafa Nigeriana: Referente a la estafa donde engañan a la víctima a través de un correo electrónico, indicándole a la víctima que gano algún premio especialmente ofreciéndole dinero solicitando datos o dinero para hacer la entrega del supuesto premio. Los delincuentes envían un correo llamativo como "URGENTE" "HA GANADO UN PREMIO", este correo llega a nombre de alguna empresa reconocida para generar mayor credibilidad informando que gano algún premio o suma de dinero con valores elevados y solicitan datos a las víctimas, el premio nunca llega; sin embargo, la información suministrada es utilizada por el delincuente para realizar otros fraudes, enviar correos spam, extraer dinero entre otros. [32] A continuación, se presenta un caso real de correos falsos que llegaron a usuarios:

[32] OSI. Fraudes online {En línea} 2013. Disponible en: https://www.osi.es/es/actualidad/blog/2013/06/28/fraudes-online-vi-has-ganado-un-premio

Figura 1. Caso de la lotería de Microsoft



Date: Mon, 27 May 2013 04:30:27 -0600
From: [redacted]@[redacted]d.gob.ni
To: [redacted]@[redacted].ni
Subject: NOTIFICACIÓN DE GANANCIA de mayo del 2013

Señor / Señora

Nos comunicaremos con usted para informarle que acaban de ganar la lotería organizada por la empresa MICROSOFT WINDOWS (250.000 euros).Para entrar en posesión de la ganancia, por favor envíe un correo electrónico para obtener el reconocimiento de agente judicial:
Maestro ANGE BATONNIER
[redacted]nier@e[redacted]ia.com

Obtenga todas las felicitaciones del grupo de Microsoft Windows.
La Sra. Veronique Carriere
Jefe de Campaña
MICROSOFT WINDOWS.

Fuente: OSI. Fraudes online. [Ejemplo correo fraudulento que suplanta a Microsoft]. En: OSI Oficina de seguridad del Internauta. 2013. Disponible en: https://www.osi.es/es/actualidad/blog/2013/06/28/fraudes-online-vi-has-ganado-un-premio

En la anterior, imagen se visualiza un caso real donde se informa de un premio de lotería, solicitando los datos del usuario y muchas veces las víctimas no se percatan de la falsedad de estos mensajes sin investigar antes si es real la procedencia y que es enviado en circunstancias extrañas. Es recomendable reflexionar y preguntarse si ha participado en algún concurso o encuesta, no se recomienda proporcionar datos personales, cuando llega de alguna cuenta de correo gratuita es sospechoso, cuando no genera mucha información también se debe desconfiar. [33]

4.1.1.5 Estafas electrónicas: Es uno de los delitos más comunes en Colombia. El uso de redes sociales acompañadas del mundo digital permite que los intrusos obtengan sus beneficios, desafortunadamente muchas de las víctimas por miedo no denuncian. La delegada de la seguridad Ciudadana de la fiscalía General Claudia Carrasquilla manifestó “que el aumento del delito de estafas electrónicas

[33] Ídem

está relacionado con la facilidad que tienen los delincuentes informáticos para acceder a la información de sus víctimas, ya que se confían de páginas que aparecen sin comprobar la autenticidad de esta, ni de los productos ofrecidos.” [34] Un caso de este tipo fue judicializado por la Fiscalía cuando fueron capturadas 8 personas de una organización que a través de internet ofrecían servicios para organizar eventos sociales como bodas y citaba a los interesados a reuniones para conocer los descuentos, donde solicitaban un adelanto para los detalles de la fiesta la cual no se realizaba. Los estafadores aproximadamente recibieron alrededor de 240 millones de pesos entre febrero de 2017 a noviembre del 2018, por 35 supuestos eventos.[35]

4.1.1.6 Forjacking: Es una nueva modalidad donde se introduce código dañino en páginas web para robos de información, generalmente afectan a los proveedores y cadenas de abastecimiento de las entidades atacadas. Esta técnica la utilizan los ciberdelincuentes interceptando los datos confidenciales que son proporcionados cuando se compra por internet, como datos de cuentas bancarias. Los sitios web donde se realizan las compras son secuestrados por los intrusos para obtener los datos de los clientes, de esta manera los datos que se brindan llegan hasta los servidores de los intrusos y son utilizados para diferentes tipos de delito. Para evitar este tipo de ataque es necesario tener actualizados las últimas versiones de los navegadores, no ingresar a páginas que no sean confiables, tener cuidado con las páginas que utilizan JavaScript ya que frecuentemente se utiliza por delincuentes informáticos. [36]

---

[34] CARRASQUILLA Claudia, Cada día se presentan 138 denuncias por estafa en Colombia. Citado por: EL TIEMPO. Documento de la fiscalía señala que en los primeros 8 meses del 2019 se reportaron 33986 delitos. {En línea} 2019 Disponible en: https://www.eltiempo.com/justicia/delitos/denuncias-por-estafa-en-colombia-411020

[35] EL TIEMPO. Cada día se presentan 138 denuncias por estafa. {En línea} 2019 Disponible en: https://www.eltiempo.com/justicia/delitos/denuncias-por-estafa-en-colombia-411020

[36] BECK. Que es el forjacking. {En línea} 2019. Disponible en: https://abdc.es/blog/formjacking-que-es-como-evitarlo/

4.1.1.7 Impacto del cibercrimen: Cuando se menciona noticias sobre cibercrimen las personas erróneamente suelen pensar que estos incidentes se presentan a grandes empresas y que su compañía no recibiría un ataque, sin embargo los delitos informáticos son una de las principales amenazas que afecta a la economía mundial. Interpol informa que solo en Europa las pérdidas generadas por el cibercrimen aproximadamente llegan a los 750.000 millones de euros, lo cual significa que el impacto del cibercrimen afecta considerablemente la economía nacional y local. [37] En el presente año 2020 con el aumento del uso de la tecnología tanto para empresas como usuarios comunes se considera que poco a poco las contraseñas podrían desaparecer, se debe tener en cuenta el estudio de la inteligencia artificial y la protección colaborativa deberá ser implementada. Los delitos informáticos perjudican a las empresas con pérdidas de aproximadamente 1 billón de dólares anuales tres veces más que los costos por desastres naturales. [38] Es necesario para las empresas contar con especialistas en seguridad de la información ya que se debe detectar a tiempo los problemas de seguridad que existen en las empresas y que dejan en riesgo la información, ya que al afectar uno de los pilares que la hacen segura como la confidencialidad, integridad o disponibilidad afecta las actividades normales de la empresa y puede generar pérdidas, teniendo en cuenta este panorama las empresas deben utilizar los recursos tecnológicos a su favor y protegerse. Según Marco Casarin gerente general de Microsoft Colombia, explica algunos temas que se debe tener presente este año 2020:[39]

- **Inteligencia artificial:** gracias a la inteligencia artificial es posible identificar patrones o anomalías y optar por medidas defensivas más rápidas y efectivas que sean eficientes, sin embargo, estos beneficios también pueden ser

[37] HERRERO Miguel. El cibercrimen también te afecta. {En línea} INCIBE. 2015. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/economia-cibercrimen

[38] Forbes Staff. ¿Cómo combatir la ciberseguridad en este 2020? {En línea} 2020. Disponible en: https://forbes.co/2020/01/25/tecnologia/como-combatir-la-ciberseguridad-en-este-2020/

[39] Idem

utilizados por los ciberdelincuentes para crear malware más destructivo y difícil de detectar. [40]

- **Expansión del internet de las cosas requiere que las cadenas de suministro tengan protección colaborativa:** con el aumento de la tecnología, las empresas de suministro están utilizando máquinas más autónomas y complejas y los datos que utilizan se crearan y almacenaran fuera de internet, por lo tanto, los intrusos buscan vulnerabilidades en los software obsoletos, dispositivos no seguros o cuentas predeterminadas. [41]
- **Garantizar la flexibilidad laboral con mayor seguridad en la nube:** las empresas deben brindar a los empleados herramientas de seguridad para que puedan realizar sus actividades de manera más segura, que mejore la movilidad y productividad utilizando mecanismos y normas actuales. Pueden aplicar soluciones de nube pública las cuales brindan seguridad adicional como ubicación en el inicio de sesión o autenticación secundaria.[42]
- **Aumento de identidad y muerte de contraseñas:** en el año 2019 fueron expuestos más de 4.000 millones de registros por violación de datos. El 63% de las fugas de datos se debe a contraseñas débiles, por lo tanto, se debe tener en cuenta mecanismos más seguros como la autenticación multifactor la cual puede reducir el riesgo de suplantaciones de identidad aplicando medios biométricos y certificados basados en la identidad. [43]

4.1.1.8 Malware: Son programas maliciosos, cuyo fin es dañar dispositivos y robar datos con algún fin lucrativo. Algunos de ellos son virus, troyanos, spyware, gusanos, ransomware entre otros. Actualmente se están presentando ataques de malware aprovechando las campañas o información sobre coronavirus, según informes de Nokia, Microsoft y agencias de seguridad los más comunes son:

[40] Idem
[41] Idem
[42] Idem
[43] Idem

Troyano coronavirus el cual se dirige a usuarios de Windows, presenta un mapa de casos de coronavirus por ciudades y regiones en tiempo real, una vez el usuario ingresa descarga un software maligno, el cual obtiene credenciales de usuario y datos personales. Otro caso de malware es Covidlock se refiere a una aplicación para los sistemas Android que supuestamente informa la ubicación de personas cercanas con COVID-19 y rastrear su propagación, pero se trata de un ransomware, el verdadero objetivo de esta aplicación es bloquear el dispositivo y solicitar rescate para recuperar su funcionamiento. [44]

4.1.1.9 Phishing: Se refiere al método utilizado por ciberdelincuentes para engañar a sus víctimas solicitando información confidencial como contraseñas, a través de correos electrónicos o páginas web falsas. Existen varios casos de phishing uno de estos se presentó en el año 2016 en el cual los seguidores de James Rodríguez, fueron víctimas de un ciberdelincuente quien solicitaba datos personales, les hizo creer que se comunicaban con el futbolista y ellos proporcionaron información confidencial como claves de correo. El ciberdelincuente fue reconocido y condenado a 4 años de prisión. [45]

4.1.1.10 Ransomware: Los intrusos obtienen información para luego solicitar un rescate. Colombia presentaba el mayor ataque de malware en el 2018, según un informe realizado por la compañía de ciberseguridad Eset. Según el informe mencionado en el 2018 Colombia presentaba el 30% de los casos estudiados, Perú el 16%, México 14%, Brasil 11% y Argentina 9%. En este tipo de ataque se

[44] LA CRONICA DEL QUINDIO. El malware se disfraza de COVID-19. {En línea} Quindio. 2020. Disponible en: https://www.cronicadelquindio.com/noticia-completa-titulo-el-malware-se-disfraza-de-covid-19-nota-138164

[45] DINERO. 90% de los colombianos preocupados por fraude de tarjetas. {En línea} 2019 Disponible en: https://www.dinero.com/economia/articulo/transacciones-digitales-como-evitar-el-fraude-online/279725

encuentran SamSam que controla remotamente el equipo y Crysis que puede introducirse a través de correos o redes sociales. [46]

4.1.1.11 Riesgos del cibercrimen: actualmente la mayoría de las actividades que realizan las personas están relacionadas con el mundo cibernético, a pesar de las ventajas que se puede encontrar en la red, también es utilizado con fines negativos, los ataques que se presentan en el ciberespacio son un reto para las empresas, ya que pueden afectar las funciones y finanzas, donde la información podría ser modificada, robada, o eliminada, por lo tanto cuando se identifica un riesgo en una empresa es necesario buscar la vulnerabilidad y aplicar las medidas de seguridad necesarias para evitar el desarrollo de un ataque.[47] La falta de conocimiento sobre los riesgos que se encuentran en la red es la principal causa de los problemas informáticos, las personas ignoran muchas de las advertencias y amenazas y no comprenden los alcances de un ciberdelincuente por lo tanto siguen realizando conductas que los convierte en víctimas de los ataques. Las empresas son responsables de la seguridad de los datos y de la privacidad que debe tener el manejo de la información de los clientes, por lo tanto las empresas deben conocer los riesgos más comunes del cibercrimen, lo cual ayudara a evitar grandes problemas y mitigar las vulnerabilidades, entre estos riesgos encontramos[48]:

[46] EL TIEMPO. Colombia el país de Latinoamérica más afectado por ransomware en el 2018. {En línea} 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/los-paises-mas-afectados-por-ransomware-en-2018-313224

[47] AMCHAM COLOMBIA. ¿Cómo pueden afrontar las empresas colombianas los riesgos cibernéticos? {En línea} Bogota. 2019. Disponible en: https://www.amchamcolombia.co/es/comunicaciones/noticias-afiliados/2907-como-pueden-afrontar-las-empresas-colombianas-los-riesgos-ciberneticos

[48] JULIA Samuel. 5 riesgos de seguridad informática en tu empresa que podrías evitar. {En línea} GADAE. 2020. Disponible en: https://www.gadae.com/blog/riesgos-de-seguridad-informatica/

- **Tener equipos informáticos sin antivirus:** es importante que los sistemas informáticos tengan instalado y actualizado los antivirus para evitar presencia de virus informáticos, troyanos o gusanos. [49]
- **No tener copias de seguridad:** las empresas contienen información relevante de sus productos, clientes o empleados como bases de datos o algún software para gestionar las actividades, es importante que realicen copias de seguridad periódicamente, las cuales además deben estar cifradas de lo contrario el riesgo a perder la información y no recuperarla genera un grave problema que afecta a toda la organización, incluso detiene el normal funcionamiento de las actividades de la empresa y su productividad. Las copias de seguridad deben realizarse correctamente porque en algunos casos se realizan copias de manera errónea y se tienen los mismos riesgos por ejemplo cuando se almacenan en los equipos informáticos los cuales pueden también afectarse y perder la información, en USB o discos duros externos que al estar conectados a los computadores podrían infectarse, por lo tanto, es recomendable realizar varias copias de seguridad en diferentes medios ya sean en la nube y en dispositivos de respaldo. [50]
- **Abrir correos desconocidos:** evitar descargar archivos adjuntos desconocidos o abrir enlaces de procedencia sospechosa y no brindar información confidencial cuando los correos que se reciben dirigen a páginas que solicitan datos privados, los correos pueden contener virus o casos de phishing. [51]
- **Abrir mensajes sospechosos en redes sociales:** algunas veces en las redes sociales llegan mensajes de desconocidos indicando ingresar a un enlace el cual puede contener virus o se la utiliza por los ciberdelincuentes para realizar alguna técnica de ingeniería social. [52]

---

[49] Idem

[50] Idem

[51] Idem

[52] Idem

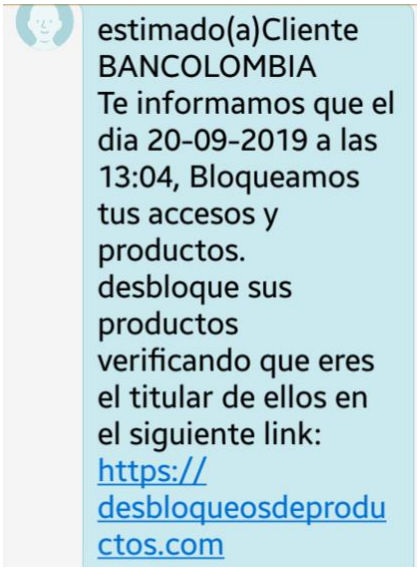
- **Introducir memorias USB o dispositivos en la computadora:** se debe analizar por un antivirus el dispositivo que se introduce antes de ser utilizado, ya que a pesar de ser útiles son introducidas en otros computadores que pueden estar infectados y contener virus, es recomendable enviar información de un sitio a otro por medios seguros como la red privada o programas en la nube. [53]

4.1.1.12 Smishing: Este delito informático utiliza mensajes de texto donde se solicita a la víctima comunicarse con un número o ingresar a una página web, el intruso puede suplantar el número de un conocido o de una entidad reconocida para generar confianza en la victima y así obtener información confidencial. Un caso de este tipo sucedió en el 2019 cuando clientes de Bancolombia recibían mensajes de este tipo[54]:

[53] Idem

[54] DIAZ Juan. Cuidado el smishing está al acecho. {En línea} LAS 2ORILLAS. 2019 Disponible en: https://www.las2orillas.co/cuidado-el-smishing-esta-al-acecho/

Figura 2. Mensaje Suplantando Entidad Bancaria Bancolombia



Fuente: DIAZ Juan. Cuidado el smishing está al acecho. [Imagen]. Las 2 Orillas. 2019. Disponible en: https://www.las2orillas.co/cuidado-el-smishing-esta-al-acecho/

En la anterior, imagen se puede observar que el mensaje solicita el ingreso a una url en el cual solicitaran al cliente datos confidenciales para supuestamente confirmar si es el titular y que haga uso normal de la cuenta sin embargo es un engaño para obtener sus datos y utilizar esa información.

4.1.1.13 Vishing: Es un tipo de delito informático proveniente del phishing, que engaña a las víctimas por medio de llamadas telefónicas, donde un delincuente informático puede suplantar la identidad de una entidad reconocida y solicitar datos confidenciales o la descarga de algún programa que puede ser un malware. Combina voz y phishing esto quiere decir que hacen creer a la víctima que se comunican con personal de confianza de una entidad, por lo tanto es recomendable no brindar información confidencial por llamada. En el año 2018 se presentó un caso en el cual estafadores se comunicaban con las víctimas a través de llamadas suplantando al personal del bando BBVA, informando que tenían cargos en sus cuentas de $1.800 supuestamente por un seguro de vida, para

realizar la cancelación del seguro y generar el reembolso, les solicitaban datos personales, con lo cual utilizaban dicha información para cometer fraudes.[55]

4.3 ANTECEDENTES

Para el desarrollo de este proyecto se tomaron como referencia trabajos similares relacionados con el cibercrimen en Colombia:

Monografía "Estado actual del cibercrimen en Colombia con respecto a Latinoamérica" trabajo de grado presentado por Luisa Fernanda Acuña López y Sandra Milena Villa Motato a la Universidad Abierta y a Distancia en Risaralda, en el año 2018 para optar como especialista en seguridad informática. En este proyecto se realiza un análisis sobre el impacto negativo de la ciberdelincuencia en empresas colombianas dando a conocer los beneficios de las tecnologías de la información sin embargo también se presenta el uso inadecuado que algunas personas hacen de estos medios y se compara con leyes de protección de datos en Colombia y otros países de Latinoamérica. Esta investigación sirvió de referencia para el análisis realizado en el presente proyecto.[56]

Proyecto "¿Qué tal está Colombia en cuestión de ciberseguridad?" Presentado por Víctor Antonio Hoyos Buitrón a la Universidad Militar Nueva Granada en Bogotá, en el año 2015, menciona los riesgos de las empresas que tienen comunicación a través de la red y la problemática que implica la falta de conocimiento por parte de sus empleados con el fin de proteger los datos lo cual representa el mayor riesgo

[55] EL ECONOMISTA. Caso de vishing con pretexto de reembolso. {En línea} 2018. Disponible en: https://www.eleconomista.com.mx/finanzaspersonales/Nuevo-caso-de-vishing-opera-con-el-pretexto-de-rembolsos-20180826-0062.html

[56] ACUÑA Luisa y VILLA Sandra. "Estado actual del cibercrimen en Colombia con respecto a Latinoamérica" {En línea} 2018.Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/25619/%20lfacunal.pdf?sequence=1

para las compañías, esta referencia sirve de apoyo para informar sobre la problemática que causa el cibercrimen e implementarla en el presente proyecto. [57]

Monografía “Metodología para la forensia informática” realizado por Edgar Calderón Toledo a la Universidad Autónoma del Estado de Hidalgo en el año 2008, para optar como licenciado en sistemas computacionales. En el proyecto se presenta una investigación sobre delitos informáticos y su penalización según el tipo de ataque, además se realiza una explicación de diferentes conceptos informáticos utilizados en la realización del presente proyecto.[58]

Proyecto “Cibercrimen una aproximación a la delincuencia informática” realizado por Amir Nayi Abushihab Collazos a la Universidad Santo Tomas. En el proyecto se informa sobre los riesgos que presenta la información que se almacena en los sistemas informáticos y se explica la ley 1273 de 2009, la cual penaliza los delitos que atentan contra la seguridad de la información, ésta se tuvo en cuenta para la realización del presente proyecto.[59]

---

[57] HOYOS Victor. ¿Qué tal está Colombia en cuestión de ciberseguridad? {En línea} 2015. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7794/Qu%E9?sequence=1

[58] TOLEDO Edgar. Metodología para la forensia Informática. {En línea} 2008. Disponible en: http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/bitstream/handle/231104/319/Metodologia%20para%20la%20forensia%20informatica.pdf?sequence=1

[59] ABUSHIHAB Amir. Cibercrimen una aproximación a la delincuencia informática {En línea} Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/1995/Abushihabamir2016.pdf?sequence=1&isAllowed=y

4.4 MARCO LEGAL

El robo de información es uno de los graves problemas que se presentan en el mundo cibernético, ya que intrusos pueden manipular esos datos para su beneficio y perjudicar a las organizaciones. Muchas de las empresas no están preparadas para este tipo de ataques. Anteriormente para Colombia esto no era un tema de interés, pero por la manera como ha aumentado el cibercrimen las empresas colombianas han empezado a involucrarse implementando políticas, herramientas, normas de seguridad y hasta llegar a participar con empresas de otros países en temas de seguridad ante delitos informáticos.

En el año 2013 Colombia fue invitada por el Consejo de Europa, como resultado de las Gestiones del Gobierno Nacional los cuales tienen como objetivo implementar leyes que prohíban los delitos informáticos y la cooperación internacional para afrontar el delito cibernético. Colombia logro ser invitada por el consejo de Europa después de realizar un largo proceso que inicio en el 2011, luego de difundir el documento CONPES 3701 referente a la Ciberseguridad y Ciberdefensa [60]donde el Ministro de Relaciones Exteriores solicito la prevención y lucha sobre el Delito Informático, para esto la canciller María Holguín solicitó al Consejo de Europa la invitación de Colombia a la Convención de Budapest. En septiembre del 2013 luego de ser analizada la normatividad de Colombia contra el Delito Informático, logró que el Consejo de Ministros de Europa aceptara que Colombia participara en la Convención sobre Delito Cibernético. [61]

[60] Cancillería. Concejo de Europa invito a Colombia a adherir a la convención sobre Delito Cibernético. {En línea} Bogotá. 2013. Disponible en: https://www.cancilleria.gov.co/newsroom/news/consejo-europa-invito-colombia-adherir-la-convencion-sobre-delito-cibernetico

[61] Idem

Figura 3. Consejo de Europa invita a Colombia a participar en la Convención sobre delito cibernético

Fuente: Cancillería. Consejo de Europa invita a Colombia a participar en la Convención sobre delito cibernético. [Imagen]. Bogotá. 2013. Disponible en: https://www.cancilleria.gov.co/newsroom/news/consejo-europa-invito-colombia-adherir-la-convencion-sobre-delito-cibernetico

Es importante estudiar el delito informático además del punto de vista del delito cometido las empresas deben conocer el respaldo legal que penalice el delito en Colombia, ya que existen leyes que ayudan a proteger los datos entre estas se encuentran:

4.4.1 CONPES 3701 de 2011: En el 2011 no existía en Colombia un lineamiento nacional para conservar la seguridad informática, por tal razón se identificaron 3 problemas principales:

- Falta de coordinación en la iniciativas y operaciones de ciberseguridad y ciberdefensa.
- Falta de capacitación especializada en ciberseguridad y ciberdefensa.
- Debilidad en la regulación y legislación en la protección de los datos.

Por estas fallas presentadas el Estado Colombiano emitió el documento CONPES (Consejo Nacional de Política Económica y Social) 3701 que establecía los lineamientos necesarios de política para la seguridad y la ciberdefensa y mejora la seguridad del Estado en cuanto a las amenazas que se presentaban ante la seguridad informática, fortaleciendo la protección de los datos. [62]

4.1.2 Ley 1273 de 2009: Referente a la protección de la información y de los datos donde se protegen además los sistemas que hagan uso de la tecnología de la información y de las comunicaciones. Esta ley penaliza actividades ilegales respecto al uso indebido de datos personales, por lo tanto, es de gran importancia para las empresas tener en cuenta esta Ley que las protege, donde intrusos han causado daño obteniendo clonación de tarjetas bancarias, acceso y alteración de sistemas. Esta Ley se divide en dos capítulos: [63]

- De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.
- De los atentados informáticos y otras infracciones.

En el primer capítulo está el acceso abusivo de un sistema informático, obstaculización ilegitima de un sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web.
En el segundo capítulo se encuentra el hurto por medios informáticos y semejantes y la transferencia no autorizada de activos.[64]

---

[62]MOSQUERA Darío. Perspectiva global para la aplicación de la seguridad informática. {En línea} Universidad Piloto de Colombia. 2016. Disponible en: http://35.227.45.16/bitstream/handle/20.500.12277/2662/00003815.pdf?sequence=1&isAllowed=y

[63]Diario oficial. Ley 1273 de 2009. {En línea} 2009. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[64] Ibid, p. 3.

4.1.3 Ley 1581 de 2012: Es frecuente que datos personales como nombres, identificación, teléfonos de contacto, email sean solicitados para crear cuentas en redes sociales, solicitadas para encuestas, diligenciar formularios para entidades, entre otras. La ley 1581 obliga a las empresas a proteger los datos mediante la autorización del titular para el uso de los mismos, tener políticas de seguridad de la información y controlar los datos confidenciales, de igual manera quien proporciona la información tiene derecho a conocer, actualizar y rectificar los datos que se recolectaron sobre ella. [65]

4.1.1 Decreto 1377 de 2013: El cual establece que se debe realizar un contrato entre el responsable de los datos y la persona que proporciona los datos, donde el primero deberá encargarse de los daños que se puedan causar por el uso incorrecto de los datos [66]

Estos reglamentos permiten tener un respaldo a las víctimas del cibercrimen que pueden ser diferentes las causas, pero también es necesario que las empresas estén informadas sobre las nuevas modalidades que utilizan los ciberdelincuentes y se preparen ante cualquier riesgo, utilizando herramientas, mecanismos y aplicando las mejores prácticas de seguridad.

[65] Germannube. Ley 1281 de 2012, Protección de datos Colombia {En línea} YouTube. 2013. 1:20 minutos. Disponible en: https://www.youtube.com/watch?v=9ypqfqlu-kw

[66] ACTUALICESE. Aspectos que regula el Decreto 1377 de 2013 {En línea} 2014. Disponible en: https://actualicese.com/aspectos-que-regula-el-decreto-1377-de-2013-en-el-contrato-para-el-tratamiento-de-datos-personales/

5 ESTADO ACTUAL DEL CIBERCRIMEN EN COLOMBIA

Las nuevas tecnologías brindan beneficios tanto a usuarios comunes como a empresas ya que facilitan muchas de las actividades que se realizan, actualmente la mayoría de información se encuentra almacenada en estos medios; sin embargo, junto con la evolución de la tecnología, el cibercrimen también se ha desarrollado, los delincuentes informáticos encuentran nuevas formas y técnicas para ingresar a la privacidad de los datos o cometer algún tipo de acción para realizar sus ataques.

En el presente año 2020 con la aparición del coronavirus se ha tomado medidas preventivas como el aislamiento, esto ha hecho indispensable la comunicación digital y la tecnología ha jugado un papel importante es esta situación ayudando a muchas personas y funcionarios de las empresas a seguir desarrollando sus labores desde sus viviendas, además de variedad de contenido ya sea para entretenimiento, comunidades virtuales, aprendizaje en cursos online, video llamadas etc. de esta manera se ha evidenciado la importancia la comunicación digital sobre todo en tiempo de crisis. Sin embargo, existen vulnerabilidades que son aprovechadas por los ciberdelincuentes los cuales utilizan la ingeniería social, donde engañan a sus víctimas ya sea para robar información, obtener sus datos confidenciales o realizan algún tipo de delito informático. [67]

Según Fortinet, líder global en soluciones de ciberseguridad durante marzo del presente año 2020 en la mayoría de países se realizó cerca de 600 campañas diarias de phishing en la cual encontraron una estafa digital que envía mensajes con enlaces de contenido malicioso y solicita a los usuarios información confidencial en páginas web falsas o llegan descargas que contienen virus que pueden controlar los dispositivos y robar información. Forinet comparo los

[67] MORALES Juan David. Ciberestafas en tiempos de coronavirus ¿Cómo no caer en ellas? {En línea} EL TIEMPO. 2020. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/estafas-en-internet-han-aumentado-durante-la-pandemia-del-coronavirus-486284

primeros meses del año 2020 con los meses del año 2019 evidenciando un aumento del 17% de virus informáticos en enero y aumento del 52% de virus en febrero. [68]

Según Juan Carlos Puentes, Country Manager de Fortinet Colombia "Por lo general, el mayor número de ataques vienen en forma de exploits, que se aprovechan de las brechas y vulnerabilidades de los sistemas corporativos. Este trimestre, se ha visto un cambio en el comportamiento de los ciberdelincuentes, quienes ahora están intentando entrar en las redes a través de ataques de phishing, abusando de la confianza y la ingenuidad de las personas que buscan información sobre el COVID-19" [69].

En algunos casos que se realizan ataques informáticos los ciberdelincuentes tienen en cuenta la necesidad de las personas de estar informadas, la incertidumbre o miedo con respecto a la situación de la pandemia que se está presentando. Los especialistas en seguridad actualmente han detectado troyanos bancarios, aplicaciones maliciosas para Android y programas de acceso remoto. Según investigaciones de ciberseguridad desde el mes de febrero hasta mediados de marzo fueron identificados 300 dominios de phishing con supuestos mensajes sobre coronavirus, 35 sitios que distribuían virus informáticos y robo de datos bancarios. [70]

Los ciberdelincuentes analizan y se mantienen informados de los temas de actualidad para tomarse el tiempo en desarrollar campañas, paginas o algún tipo de engaño que para el usuario sea lo más auténtico posible, como los mapas sobre propagación del coronavirus, suplantación de fuentes de información descarga de aplicaciones son estrategias utilizadas por los ciberdelincuentes.

---

[68] MEJIA Mariana. El phishing es el ciberataque más común en medio del confinamiento. {En línea} 2020. Disponible en: https://caracol.com.co/radio/2020/05/07/tecnologia/1588814967_884881.html

[69] PUENTES Juan. Aumenta el cibercrimen en Colombia en el contexto de COVID-19. Citado por: ACIS. COVID 19 La tormenta perfecta para ciberdelincuentes {En línea} Bogotá. 2020. Disponible en: https://acis.org.co/portal/content/noticiasdelsector/aumenta-el-cibercrimen-en-colombia-en-el-contexto-de-covid-19

[70] MORALES. Op. cit

También han aprovechado la necesidad de las personas para ofrecer supuestos cupones de descuentos, ofertas o informando que ganaron algún tipo de beneficio. De acuerdo a Carlos Gómez ingeniero de ventas de SonicWall también llegan correos y mensajes cada vez más creíbles suplantando a entidades bancarias los cuales solicitan datos confidenciales. [71]

Una gran vulnerabilidad es la sociedad de adultos mayores o personal de las empresas que no está relacionada continuamente con el mundo cibernético y por las circunstancias que presentamos de la pandemia se han tenido que adaptar a las nuevas tecnologías que se utilizan principalmente para comunicarse con sus familiares, para que los estén monitoreando o para realizar las labores encomendadas por las empresas, desafortunadamente la mayoría de ellos no tienen conocimiento sobre estafas, virus informáticos, robos de información etc. de manera que no pueden distinguir lo falso o verdadero que se presenta en internet.

También deben los padres estar atentos a los niños ya que al estar tanto tiempo conectados a internet son víctimas de engaños que no solo vulneran sus datos personales o roban su información además se pueden presentar delitos informáticos comunes dirigidos a los niños como el ciberacoso, exposición a contenidos nocivos, grooming entre otros. [72]

Aunque los niños y adultos mayores son más vulnerables ninguna persona que utilice medios tecnológicos está exenta a recibir algún tipo de ataque informático, existen personas que conocen la tecnología y la utilizan con frecuencia sin embargo llegan a ser víctimas de los ciberdelincuentes ya sea por desconocimiento o falta de precaución.

En la actualidad los casos de cibercrimen han aumentado ya que por el aislamiento obligatorio ha generado que las personas permanezcan más tiempo en internet, utilizando sus servicios y su contenido.

Con la nueva modalidad de teletrabajo es necesario que las empresas implementen medidas de seguridad para proteger a los empleados de los ataques

[71] Idem

[72] Idem

informáticos, es fundamental enseñar a los funcionarios que trabajan de manera remota las recomendaciones necesarias para proteger la información. Los errores cometidos por el factor humano, la falta de conocimiento o descuido representan la mayor vulnerabilidad para las empresas.

Lo más importante para minimizar los riesgos es conocer las vulnerabilidades que se están presentando actualmente, se debe empezar por la educación sobre ciberseguridad, para la comunidad de adultos mayores es recomendable que los familiares dediquen tiempo para informar que a pesar de los beneficios que brinda internet también existe información falsa y que tengan cuidado con las páginas que visitan ya que pueden ser engañados. En general es importante evitar ingresar a páginas que no sean oficiales, verificar que en la parte superior de la barra de navegación aparece el candado que indica que la página es segura y no confiar de todo lo que aparece en internet.[73]

Roberto Martínez analista de kaspersky, Carlos Gómez ingeniero de ventas de SonicWall y Renee Tarum vicepresidente de seguridad de la información de Fortinet recomiendan sospechar de cualquier contenido que llegue por correo o mensaje donde se solita información confidencial, tener instalado el antivirus y herramientas de seguridad, tener actualizado navegadores y el sistema operativo, utilizar contraseñas complejas y verificar que las páginas web que se visitan sean seguras.[74]

[73] Idem

[74] Idem

6 ANÁLISIS DEL IMPACTO NEGATIVO DEL CIBERCRIMEN PARA LAS EMPRESAS COLOMBIANAS

Según publicación del periódico EL TIEMPO en un estudio realizado por investigadores del Tanque de Análisis y creatividad de las TIC, la cámara colombiana de informática y telecomunicaciones y el centro de capacidades para la ciberseguridad de Colombia de la Policía Nacional, sobre tendencias del cibercrimen en Colombia, en el año 2019 se reportaron 28.000 casos de ciberataques en Colombia, con un incremento del 54%, en comparación al año 2018, de los cuales 15.000 corresponden a infracciones penalizadas por la Ley 1273 de 2009. [75]

Además, en la publicación del periódico EL TIEMPO también se informa sobre la problemática que genera estos delitos para medianas y grandes empresas, donde se obtuvo en el segundo trimestre del 2019 aproximadamente 14 millones de intentos de ciberataques, donde la técnica más utilizada es la ingeniería social cuyo objetivo es utilizar engaños para obtener información confidencial falsificando la identidad de los usuarios, correos o realizando modificaciones. Estos delitos han causado pérdidas para las empresas entre 300 y 5000 millones de pesos. [76]

Para Freddy Bautista coronel y consultor internacional de ciberseguridad, posiblemente en poco tiempo los ataques se realizarán a través de la inteligencia artificial de manera que las empresas recibirían audios o videos de supuestos ejecutivos, clientes o proveedores para engañarlos y así obtener dinero. Es posible que también se aumente la creación de perfiles falsos en redes sociales para enviar malware o el uso de botnet para enviar correos de extorsión. [77]

---

[75] TECNOSFERA. En 2019 se reportaron más de 28000 casos de ciberataques en Colombia {En línea} EL TIEMPO. 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

[76] Idem

[77] Idem

De acuerdo con investigaciones realizadas en el año 2019 las entidades más afectadas fueron las empresas financieras por los descuidos o falta de información de los usuarios lo que genera un alto riesgo frente a las amenazas. En el año 2019 fueron registrados 48 billones de intentos de ataques cibernéticos en Colombia generados principalmente a las empresas financieras. La plataforma Fortinet Threat Intelligence Insider Latin America, es una herramienta gratuita encargada de informar sobre delitos informáticos actuales cada trimestre para 10 países, en su reporte presentó un aumento de amenazas en Colombia, donde se encontraron 131 millones de intentos de amenazas informáticas en el año 2019 siendo los más frecuentes phishing y la ingeniería social.[78]

Uno de los delitos más denunciados en Colombia hasta el año 2019 ha sido el hurto por medios informáticos con 31.058 casos, esto se debe a que los intrusos aprovechan la interacción entre clientes y las entidades bancarias teniendo en cuenta el dinero que se encuentra en las cuentas, otro de los delitos que presenta un número significativo de denuncia es la violación de datos personales, en la cual se obtuvieron 8.037 casos; en tercer lugar está el delito por acceso abusivo a un sistema informático que tiene 7.994 casos, en el delito de transferencia no consentida de activos se obtuvieron 3.425 casos y con respecto al uso de software malicioso se tienen 2.387 casos. En virtud de lo anterior, se puede evidenciar que en Colombia muchas de las organizaciones en algún momento han sido víctima de alguno de los delitos mencionados, dadas por vulnerabilidades de los sistemas informáticos. [79].

La vulnerabilidad para las empresas radica en que la mayoría de estas no invierten en la protección de la información, no tienen presente que es una realidad que cualquiera puede llegar a ser víctima de ataques de ciberdelincuentes y que puede generar grandes pérdidas, hasta la inestabilidad para la organización

[78]EL ESPECTADOR. En 2019 se registraron 48 billones de intentos de ciberataques en Colombia {En línea} 2020. Disponible en: https://www.elespectador.com/tecnologia/en-2019-se-registraron-48-billones-de-intentos-de-ciberataques-en-colombia-articulo-908787

[79] YOHAI Alberto. Tendencias cibercrimen Colombia 2019-2020 {En línea} Bogotá. 2019. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

afectando su funcionamiento normal, además las empresas a pesar de contar con una infraestructura tecnológica adecuada algunas veces tienen falla en la capacitación del personal en cuanto a seguridad digital. De acuerdo al Centro Cibernético Policial uno de los riesgos para las empresas es la suplantación del correo corporativo desde el cual pueden solicitar datos personales a los usuarios o trasferir sumas de dinero y generar pérdidas de aproximadamente 380 millones de pesos. [80] Para las empresas ser víctimas de un ataque es un impacto negativo, para el cual muchas veces no están preparadas y cuando es conocido el ataque realizado a dicha organización pierde credibilidad por parte de sus clientes, ya que no se sienten seguros. Cada día los ciberdelincuentes encuentran ataques más sofisticados algunos que ni siquiera han sido identificados por las empresas. En todo momento existirán riesgos, dado que los intrusos pretenden obtener beneficios con la información de las empresas.

En un informe realizado por Thomson Reuters la mitad de grandes empresas globales han sido víctimas de ataques cibernéticos, los más comunes son fraudes, robos, suplantación de identidad y delitos financieros. Según el informe el 47% de los encuestados revelo que su empresa ha sido víctima de al menos un delito financiero donde el cibercrimen y fraudes se presentaron con mayor frecuencia. Estos delitos dejaron perdidas aproximadas de 1.45 billones de dólares, de estos casos el 41% no fueron denunciados ya sea por corrupción, sobornos que pueden incluir a personal interno, y sobre todo por daños a su reputación, pérdidas financieras y por el impacto negativo de la confianza de sus usuarios o inversionistas si llegan a conocer estas vulnerabilidades.[81] Desde el año 2017 se han conocido 52.000 denuncias sobre delitos informáticos entre estos se

[80] PORTAFOLIO. El secuestro de información desangra a las empresas del país {En línea} 2019. Disponible en: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

[81] Redacción profesional Líder. Casi 50% de las empresas han sido víctimas de delitos financieros {En línea} EL ESPECTADOR. 2018. Disponible en: https://www.elespectador.com/economia/casi-el-50-de-las-empresas-han-sido-victimas-de-delitos-financieros-articulo-798201

encuentran: el robo de información y suplantación de identidad como los más comunes, ocupando Bogotá el primer lugar, después Cali y Medellín. [82]

El impacto que produce el cibercrimen en las empresas genera grandes pérdidas en su productividad, daños a su reputación o estar involucrados en problemas legales cuando existe fuga de información y los intrusos aprovechan los datos que obtienen para hacer uso de estos y realizar actos delictivos.

Estudios realizados por Tendencias del Cibercrimen 2019-2020, presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial, a través estadísticas dio a conocer los delitos que se están presentando actualmente y que posiblemente enfrentaran las empresas colombianas en el 2020, este estudio revela los datos estadísticos más representativos en Colombia y las nuevas técnicas utilizadas, según las denuncias de empresas y ciudadanos, uno de estos es el ataque por malware. De los 447 delitos informáticos analizados se encontraron 33 nuevos tipos de programas maliciosos que han infectado, como por ejemplo: enlaces, archivos adjuntos y páginas web. Para evitar estos riesgos es importante conocer cómo se generan estos delitos e identificar las vulnerabilidades para realizar las respectivas correcciones y aplicar técnicas, normas y herramientas de seguridad que protejan los recursos tecnológicos, humanos y los procesos[83].

Desafortunadamente algunas empresas no se preocupan por la seguridad y no realizan los respectivos controles e inversión en la seguridad de la información, solo hasta que sucede algún ataque pueden dimensionar los daños que pueden causar.

En la siguiente figura, se puede observar el aumento o descenso de casos de delitos informáticos presentados en Colombia a partir del año 2015 al 2019, donde el 54.5 % de estos delitos se han reportado de manera presencial ante las

---

[82] TicTac. Tendencias del cibercrimen en Colombia 2019-2020 {En línea} CCIT. 2019. Disponible en: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[83] YOHAI. Op cit

autoridades y el 45.5% se ha realizado de manera virtual, el cual se puede realizar con la aplicación ADenunciar.[84] Entre 2015 y 2018 se observa que los delitos informáticos aumentaron mientras en 2019 en comparación con los años anteriores disminuyeron.

Figura 4. Tipifica las conductas de delitos informáticos en Colombia

Fuente: YOHAI Alberto. Tipifica las conductas de Delitos Informáticos en Colombia. [Imagen]. Tendencias cibercrimen Colombia 2019-2020. Bogotá. 2019. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Las vulnerabilidades más frecuentes en Colombia se presentan por phishing con un 42%, suplantación de identidad con 28%, envió de software malicioso con 14% y fraudes hacia personas que realizan medios de pago en línea 16%. En algunos casos los cibercriminales contratan Money Mules las cuales son personas que prestan su nombre o cuenta bancaria para recibir el dinero obtenido de manera ilegal para luego transferirlo a las cuentas de los responsables de estos actos.[85]
Aunque exista información sobre recomendaciones que se deben tener en cuenta para minimizar los riesgos ante el cibercrimen este sigue aumentando. En el año 2019 Felipe Gómez director de data center, cloud y seguridad de CenturyLink, señalo a Colombia como el quinto país en Latinoamérica con más tráfico

[84] Ídem

[85] ABC Sociedad. Mulas de dinero {En línea} 2018. Disponible en: https://www.abc.es/sociedad/abci-mulas-dinero-nuevo-fraude-puedes-participar-sin-querer-201812311104_video.html

malicioso. Las pérdidas para las empresas podrían aumentar y la información ser más vulnerable ya que a medida que aumenta la tecnología las personas utilizan estos medios para guardar sus datos sin tener precauciones y realizar la mayoría de sus actividades, por lo tanto, las empresas deben estar atentas y actuar ante estas amenazas.[86]

Sonda la red de Latinoamérica de servicios de tecnologías de la información en abril del año 2019, abrió el centro de operaciones más moderno de ciberseguridad de Latinoamérica en la cual invirtieron más de 850.000 dólares, es de gran ayuda para las empresas ya que cuenta con espacio para soportar las actividades realizadas en el ciberespacio y proteger la información por medio de tecnologías avanzadas como inteligencia artificial, automatización robótica de procesos, analítica de datos son algunas de estas tecnologías. Para Cristhian Onetto vicepresidente regional de transformación de Sonda, Colombia ha sido víctima de gran cantidad de ciberataques que ha aumentado en los últimos años, donde el phishing se presenta con mayor frecuencia y más del 37% de empresas han sido víctimas de algún tipo de ataque cibernético. [87]

Cristhian Onetto también menciona la problemática que existe para empresas bancarias ya que son las más sensibles en cuanto a ciberseguridad por los ataques que se pueden presentar hacia las cuentas de los usuarios o tarjetas, lo que representa un gran desafío para las empresas, debido a la confianza digital que depende de dos factores el fortalecimiento de cultura y la utilización de tecnologías antifraude. Este proyecto está asociado con MinTic y la Cámara Colombiana de Informática y Telecomunicaciones. [88]

---

[86] RADIO SANTA FE. Compañías colombianas son más reactivas que preventivas en materia de cibercrimen {En línea} Bogotá. 2019. Disponible en: http://www.radiosantafe.com/2019/08/13/companias-colombianas-son-mas-reactivas-que-preventivas-en-materia-de-cibercrimen/

[87] ACTUALICESE. El ciberdelito es una industria en crecimiento. Las compañías necesitan compañías que las apoye {En línea} 2019. Disponible en: https://actualicese.com/el-ciberdelito-es-una-industria-en-crecimiento-las-companias-necesitan-una-guia-que-las-apoye/

[88] Idem

A partir de lo presentado anteriormente, se concluye que el impacto negativo que genera el cibercrimen puede presentar grandes pérdidas especialmente deben estar preparadas las empresas financieras ya que los delincuentes informáticos tienen mayor interés en realizar sus ataques tanto a la empresa como a sus usuarios por que pueden obtener beneficios monetarios, además de estar en riesgo el activo más valioso: la información. Por lo tanto, es necesario que las empresas brinden mayor seguridad informática a través de técnicas y prácticas de seguridad que se pueden implementar e invertir en dispositivos que ayuden a fortalecer la privacidad de los datos que se utilizan.

6.1 CASOS REALES QUE HAN AFECTADO A EMPRESAS COLOMBIANAS

Entre abril y junio del año 2019 Colombia fue víctima de 42 billones de intentos de ciberataque según investigaciones de la firma de seguridad Fortinet. El mayor ataque presentado fue por exploits, donde un programa o código aprovecha la vulnerabilidad de seguridad de una aplicación o sistema para beneficio de un intruso. Por otra parte, el 98% de ataques a redes se ha realizado por vulnerabilidades que permiten activar comandos con los cuales se realizan ataques de denegación de servicio entre estos están el troyano DoublePulsar, el cual apareció en el año 2018, encargado de distribuir malware como el Wannacry y ataques en bancos de Chile y México, este ataque fue uno de los cuatro más reconocidos en Colombia en el segundo trimestre del año 2019.89 Este ataque se presenta principalmente en empresas donde no invierten lo necesario en mecanismos de ciberseguridad y no tienen en cuenta el uso de parches de seguridad y actualización de programas. El 86 % de los malware en Colombia se trata de un troyano que infecta los archivos adjuntos con contenido malicioso.90

[89] Redacción atmosfera. Colombia sufrió 42 billones de intentos de ciberataque en 3 meses. {En línea} EL TIEMPO. 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666

[90] Idem

Otro de los ataques más frecuente es el phishing donde el atacante engaña a través de técnicas a su víctima para infectar sistemas y tener acceso a información confidencial. [91]

Para los intrusos resulta más fácil atacar empresas pequeñas y medianas, ya que en su mayoría no cuentan con las suficientes medidas de seguridad. Existen muchos casos de cibercrimen como el ocurrido en el año 2019 donde la compañía Eset, detecto el ataque llamado phishing, en el cual los intrusos pretendían robar información de usuarios de una entidad bancaria presentando una página similar a la que ingresan los usuarios, a través de esta solicitan información confidencial para realizar fraudes y otros delitos. Este consistía en que a los clientes les llegaba un correo de la supuesta entidad bancaria solicitando ingresar datos para inicio de sesión y su contraseña, ya que los canales estaban bloqueados, hay la posibilidad que algunos se dejen engañar de este método porque al dirigirse al enlace este mostrará una página idéntica a la oficial, donde además se solicitaba los datos de la tarjeta de crédito. Eset identifico esta amenaza, realizando pruebas con datos que no eran reales y la página los identificaba como válidos. Además, la página falsa creada por los ciberdelincuentes tenía certificado de seguridad SSL, para dar credibilidad, garantizando que los datos viajan cifrados, el sitio aparecía con el dominio https y esto brindaba mayor confiabilidad para el cliente. Según la investigación el certificado fue conseguido por los intrusos de manera gratuita por la entidad Let`s Encrypt. [92]. En la siguiente imagen se visualiza el correo falso que llegaba a usuarios supuestamente enviado por una entidad bancaria:

[91] Idem

[92] LUBECK Luis. Phishing suplanta identidad de reconocido banco de Colombia y busca robar información financiera {En línea} 2019. Disponible en https://www.welivesecurity.com/la-es/2019/06/05/phishing-activo-reconocido-banco-colombia/

Figura 5. Falso correo que llegaba a usuarios

Fuente: LUBECK Luis. Falso correo que llegaba a usuarios. [Imagen]. Phishing suplanta identidad de reconocido banco de Colombia y busca robar información financiera. 2019. Disponible en https://www.welivesecurity.com/la-es/2019/06/05/phishing-activo-reconocido-banco-colombia/

En la anterior imagen se puede apreciar un correo enviado a los usuarios de una entidad bancaria informando la suspensión de productos y acceso a los canales virtuales, para restablecer la cuenta solicita ingresar a un link en el cual seguramente los intrusos solicitaran datos confidenciales o puede ser un link con contenido maligno.

Otro caso de delito informático se presentó en Pereira y Bogotá donde fueron capturados los integrantes de la banda Wall Street acusados por concierto para delinquir, violación de datos personales, acceso abusivo a un sistema informático, transferencias no consentidas de activos y estuvieron involucrados en 189 casos por hurto a través de fraudes electrónicos. El comandante de la policía de Quindío Luis Benavides responsable de la captura informo sobre perdidas de $2.160.000.000, en cuentas del banco Davivienda realizado con la modalidad SIM

SWAP que bloquea la SIM CARD de los clientes, haciendo reposición ante el operador de esta manera los intrusos se pueden autenticar ante el sistema financiero y pueden modificar claves del portal, para trasferir el dinero a diferentes cuentas y poder retirar el dinero o realizar compras. Entre las víctimas se encuentran usuarios que manejaban altas sumas de dinero como los vicepresidentes del banco. En los últimos meses se está realizando investigaciones para verificar si funcionarios de empresas de telefonía están involucrados en este delito.[93]

El cibercrimen se presenta especialmente como se mencionó anteriormente, por falta de conocimiento de los usuarios, falta de herramientas de seguridad, falta de implementación de mecanismos que ayuden a la recuperación ante los ataques entre otros. Una manera para evitar ser víctimas de los intrusos es aplicar buenas prácticas de seguridad como la norma ISO/IEC 27001 e ISO/IEC 27002, las cuales ayudan a las empresas a estar preparadas ante ataques de malware y contra los ciberdelincuentes; además ayudan a supervisar los sistemas informáticos para defenderse si llegara a existir algún ataque, los recursos de seguridad deben estar actualizados como los sistemas operativos o los antivirus.

La siguiente tabla, es una encuesta realizada por el Instituto Nacional de estadística, donde se observa que un gran riesgo que se presenta tanto para usuarios comunes como para las empresas es el uso de redes sociales, ya que pueden utilizar información compartida y solicitud de datos personales, para el robo de información y otros delitos, es importante tener en cuenta los riesgos a los que se exponen los datos y evitar aceptar solicitudes de personas desconocidas o brindar información confidencial, incluso fotos publicadas pueden ser utilizadas para algún tipo de delito[94].

---

[93] CARACOL RADIO. Wall Street banda que desocupaba cuentas de bancos y empresas {En línea} Quindío. 2019. Disponible en: https://caracol.com.co/emisora/2019/10/22/armenia/1571698682_047504.html

[94] PINTO Alba, CANTON Isabel y SANTOS Yorly. Prácticas de riesgo en redes sociales y whatsapp por estudiantes de educación básica secundaria {En línea} 2019. Disponible en: http://www.revistaespacios.com/a19v40n23/19402307.html

Tabla 1. Conductas de riesgo en internet

Afirmaciones	España		Colombia	
	TA - A	D - TD	TA - A	D - TD
Creo que la información que comparto en las redes sociales es segura	78.1	21.9	60.8	39.2
Prefiero no participar en chats porque algunos contenidos son inadecuados	52.2	47.8	52.9	47.1
Cuando estoy en las redes sociales protejo la reserva de mi identidad	85.1	14.9	72.6	27.4
En las redes sociales puedo ser una persona diferente	35.6	64.4	35.8	64.2
La gente tiende a mentir más en las redes sociales	77.3	22.7	69.2	30.8
Acepto la mayoría de las solicitudes de amistad en redes sociales de desconocidos	24.2	75.8	19.7	80.3
Publico mis fotografías familiares y con mis compañeros de clase sin temor alguno	**57.1**	42.9	**66.1**	**33.9**
En ocasiones he compartido información privada en redes sociales	**32.9**	67.1	12.7	87.3
Me han enviado información inadecuada a través de Internet	**38.2**	61.8	**19.5**	80.5
He recibido solicitudes para compartir información personal a través de Internet	23.0	77.0	21.4	78.6
He facilitado mi usuario y contraseña en redes sociales a amigos o novio(a)	**10.5**	89.5	**16.8**	83.2

Fuente: PINTO Alba, CANTON Isabel y SANTOS Yorly. Prácticas de riesgo en redes sociales y whatsapp por estudiantes de educación básica secundaria {En línea} 2019. Disponible en: http://www.revistaespacios.com/a19v40n23/19402307.html

Se destaca de las preguntas realizadas la que mayor porcentaje representa es: Cuando estoy en redes sociales protejo la reserva de mi identidad con un 85% para España que están de acuerdo y 72% en Colombia están de acuerdo, sin embargo un porcentaje considerable manifiesta compartir información en estos medios, por lo tanto se evidencia que la información no está completamente

segura y que cualquier dato que se comparte puede ser utilizado por intrusos que comprometen la privacidad e integridad de la misma.

7 ESTADÍSTICAS DE CIBERDELITOS DEL AÑO 2020 EN COMPARACIÓN CON LOS AÑOS ANTERIORES

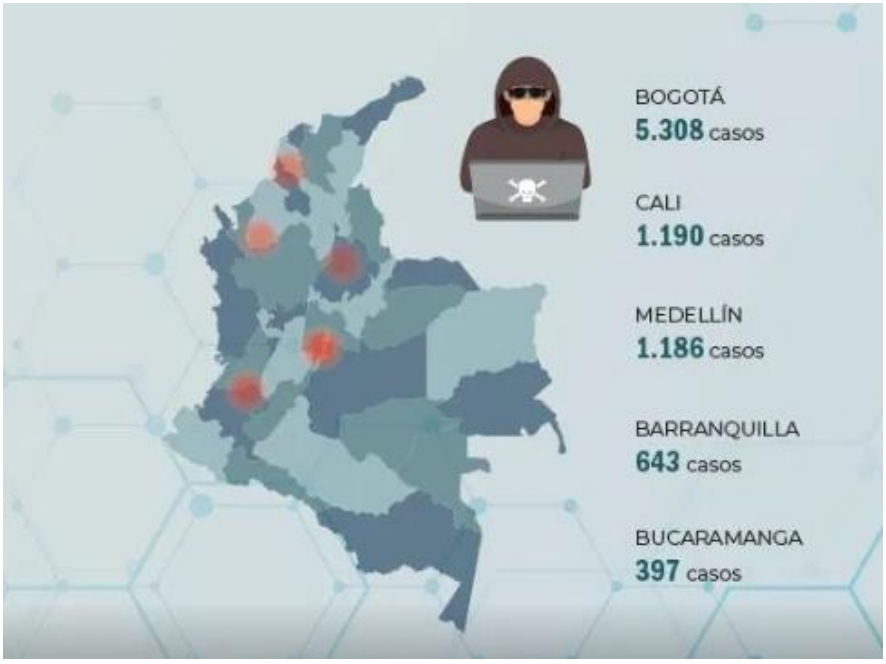
La seguridad de la información se ha convertido en un reto para las empresas colombianas. Según el estudio de “Tendencias del cibercrimen en Colombia 2019-2020” realizado por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), el Centro de Capacidades para la Ciberseguridad de la Policía Nacional del Colombia (C4), el Programa de Seguridad Aplicada al Fortalecimiento Empresarial (Safe) y el Tanque de Análisis y Creatividad de las TIC (TicTac), el desarrollo de los delitos informáticos facilita la detección de víctimas potenciales, ya que los ciberdelincuentes encuentran nuevas formas de identificar vulnerabilidades además de aplicar nuevas técnicas de ingeniería social.[95] En algunos casos es posible que el malware detecte si un sistema de seguridad lo está analizando y se autoelimina. Por lo tanto, esta clase de acciones representan un mayor desafío para los investigadores, deberán avanzar de igual manera que los delitos informáticos por que las técnicas antiforense eliminarán las evidencias digitales de los equipos y sistemas que se infecten. La ingeniería social es la mayor técnica que utilizan los ciberdelincuentes para atacar, más del 90% de los ciberataques se realizan mediante este método sin embargo los ciberdelincuentes utilizaran cada vez herramientas más avanzadas como el deepfake, basada en inteligencia artificial la cual permite superponer imágenes o videos en otros o imitar voces reales para que la víctima no sospeche si un contenido es falso.[96] Es un problema para las empresas colombianas ya que podrían recibir audios o videos donde suplantan la identidad de ejecutivos, clientes o proveedores para recibir dinero o productos. En el estudio realizado sobre las Tendencias del cibercrimen también se menciona los riesgos por el uso de botnet utilizado para

[95] MUÑOZ Fernando. Cibercrimen: su computador o Smartphone van a ser atacados. {En línea} IMPACTOTIC. 2019. Disponible en: https://impactotic.co/cibercrimen-su-computador-va-a-ser-atacado-en-5-4-3/

[96] Idem

enviar mensajes de extorsión, uso de foros para venta de datos bancarios y cuentas falsas en redes para la propagación de malware. [97] A continuación, se puede observar los delitos informáticos que más han afectado a Colombia, los datos corresponden al año 2019:

Figura 6. Ciudades colombianas más afectadas en Colombia en 2019



Fuente: IMPACTOTIC. Ciudades colombiana más afectadas en Colombia en 2019. . [Imagen]. Tendencias del cibercrimen en Colombia 2019-2020. Disponible en: https://impactotic.co/cibercrimen-su-computador-va-a-ser-atacado-en-5-4-3/

En la anterior imagen, se observa que la mayor cantidad de delitos informáticos en las ciudades de Colombia corresponde a Bogotá con 5.308 casos registrados.[98] Es alarmante que en el presente año 2020, por la situación de la pandemia los casos de ciberdelito han aumentado, los delincuentes informáticos han aprovechado que

[97] Idem

[98] Idem

por temas de aislamiento preventivo la comunicación y las actividades que se realizaban presencialmente se deben hacer a través de internet y medios informáticos, de esta manera los ataques pueden llegar por mensajes falsos o correos electrónicos donde engañan a las víctimas para obtener sus datos o enviar malware. Entre los delitos informáticos que más han afectado a los colombianos se encuentran hurtos por medios informáticos, violación de datos personales, acceso abusivo a un sistema informático, transferencia no consentida de activos y uso de software malicioso. [99]

Según Luis Fernando Atuesta jefe del centro cibernético de la policía nacional "El delito que más se produce es el hurto a través de medios informáticos, es decir, la gente es víctima de que le roben la plata de sus bancos por medio de internet. Lo que más se ha incrementado es el uso de software malicioso y hay una propagación de virus impresionante a través de internet, lo que hace que se apoderen de nuestras claves bancarias" [100]

En este tiempo de pandemia los ciberdelitos se han incrementado más del 150% y han identificado cerca de 200 páginas con contenido malicioso. Menciono el coronel. [101]

A continuación, se presenta una tabla donde se aprecia los delitos informáticos en el primer trimestre del año 2019, resultados obtenidos según estadísticas del cai virtual.

[99] Idem

[100] ATUESTA Luis, Delitos informáticos aumentaron en Colombia durante la cuarentena. Citado por: Semana. {En línea} 2020. Disponible en: https://www.semana.com/on-line/tecnologia/articulo/delitos-informaticos-aumentaron-en-colombia-durante-la-cuarentena/662686

[101] Idem

Tabla 2. Delitos informáticos reportados en el CAI Virtual de la Policía durante los meses enero, febrero y marzo de 2019

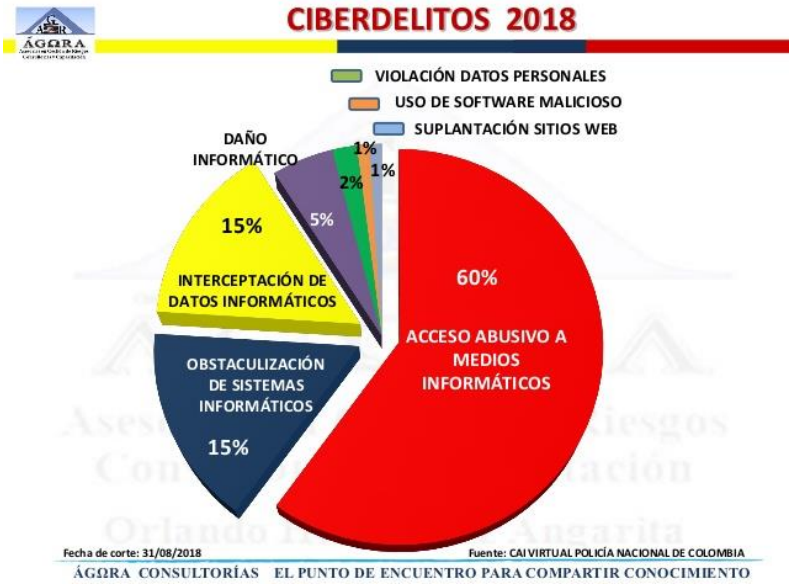
Delito	Artículo	ene-19	feb-19	mar-19	Total
Uso software malicioso	269E	518	477	366	1361
Violación datos personales	269F	148	180	182	510
Acceso abusivo sistema informático	269A	115	86	128	329
Obstaculizar sistema informático	269B	53	20	35	108
Interceptación datos informáticos	269C	49	31	35	115
Daño informático	269D	30	75	35	140
Transferencia no consentida activos	269J	30	36	35	101
Estafa	246	166	614	491	1271
Extorsión	244	78	37	99	214
Hurto	269I	129	104	117	350
Pornografía infantil	218	71	20	72	163
Injuria	220	188	20	138	346
Calumnia	221	30	20	60	110
Amenazas	347	30	56	52	138
Total delitos ->		**1635**	**1776**	**1845**	**5256**

Fuente: HURTADO, María y SIERRA, Christian. Aseguramiento de la seguridad de la información desde el análisis de vulnerabilidades en la infraestructura cibernética de la empresa NOSTRADAMUS. [En línea]. Bogotá. 2020. p.13. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/34783/cdsierrab.pdf?sequence=1&isAllowed=y

En este año 2020 la mayor cantidad de casos de delitos reportados corresponden al hurto a través de medios informáticos como lo menciona anteriormente Luis Atuesta jefe del centro cibernético de la policía nacional, mientras que en el primer trimestre del año 2019 la mayor cantidad de casos corresponden al uso de software malicioso con 1.361 casos en total. Con lo cual se puede concluir que se debe prestar atención al uso de los datos confidenciales, en lo posible utilizar la información confidencial de manera encriptada, con clave y evitar proporcionar datos a extraños, ya que la información está expuesta a ataques cibernéticos sobre todo en la actualidad donde la mayor parte del tiempo se permanece se hace uso de la tecnología.

Se puede observar en la siguiente figura que en el año 2018 en Colombia el delito que más se realizó fue el acceso abusivo por medios informáticos, referente al ingreso de intrusos a un sistema sin autorización de quien tiene el derecho legítimo de hacer uso del mismo. Este delito muchas veces puede ser cometido por jóvenes hacker con el objetivo de consultar el nivel de seguridad de un sistema informático o para practicar las habilidades que pueden tener para pasar por alto las medidas de seguridad, pero estas acciones son consideradas un delito grave, ya que vulneran la integridad, intimidad y disponibilidad de los datos y sistemas informáticos. [102]

Figura 7. Ciberdelitos en Colombia, año 2018



Fuente: HERNANDEZ Orlando. Estadísticas delitos informáticos de 2010 a 2018. [Imagen]. Boletín ágora consultorías. 2018. p.3. Disponible en: https://www.slideshare.net/donorlan/boletin-agora-consultorias-estadistica-ciberdelitos-2010-a-agosto-2018

[102] HERNANDEZ Orlando. Estadísticas delitos informáticos de 2010 a 2018. {En línea} Boletin agora consultorias. 2018. Disponible en: https://www.slideshare.net/donorlan/boletin-agora-consultorias-estadistica-ciberdelitos-2010-a-agosto-2018

En la siguiente figura, se observa que en el año 2015 a 2017 el mayor delito presentado fue la estafa y compras por internet con un 41%, donde los delincuentes informáticos utilizaban mecanismos de engaño para obtener la información de sus víctimas, troyanos y gusanos para obtener contraseñas, roban tarjetas de crédito o débito o a través de correos pueden recibir alguna notificación referente a algún premio o algún producto que desea comprar o servicio que ofrecen por internet, la victima deposita el dinero pero no recibe la solicitud. Las estafas que más se presentan son por la compra de artículos económicos, trabajos bien remunerados, alquiler de vivienda entre otros[103].

Figura 8. Ciberdelitos en Colombia desde 2015 a 2017

Fuente: HERNANDEZ Orlando. Estadísticas delitos informáticos de 2010 a 2018. [Imagen]. Boletín ágora consultorías. 2018. p.4. Disponible en: https://www.slideshare.net/donorlan/boletin-agora-consultorias-estadistica-ciberdelitos-2010-a-agosto-2018

[103] Abogado defensor. Victimas de estafas por internet {En línea} 2018. Disponible en: https://www.tuabogadodefensor.com/victimas-estafas-internet/

8 RECOMENDACIONES PARA PREVENIR, CONTROLAR Y REGULAR LAS VULNERABILIDADES EN LOS SISTEMAS INFORMÁTICOS

Las **vulnerabilidades** se refieren a una falla de seguridad que puede presentar el software o hardware y puede ser utilizada por un intruso para comprometer la integridad, disponibilidad o confidencialidad de la información o del sistema en el que se encuentre. Estas fallas se pueden presentar en el diseño, configuración o en los procedimientos que realiza el sistema. La acción que explota una vulnerabilidad y compromete al sistema informático es una **amenaza,** esta puede ser interna o externa y la probabilidad que una vulnerabilidad sea explotada por una amenaza generando pérdidas o daños se convierte en un **riesgo**.[104]
Entre las vulnerabilidades más comunes que se pueden presentar en un sistema informático se encuentran:

- **Vulnerabilidades del día cero:** existen cuando hay un agujero o falla en un programa de software en el cual no existe un parche o solución, se presenta por que el proveedor del software no conoce donde se encuentra la vulnerabilidad. Cuando la vulnerabilidad se descubre el programador deberá tomar medidas preventivas lo más pronto ya que si la vulnerabilidad es explotada por un delincuente informático se produce un ataque. [105]
- **Vulnerabilidades de diseño:** se pueden presentar por fallos en el diseño tanto de protocolos de la red como a fallas en las políticas de seguridad [106]
- **Vulnerabilidades de implementación:** se presentan cuando existen errores en la programación o por algún descuido del fabricante. [107]

---

104 MEDIACLOUD. vulnerabilidad informática. {En línea} disponible en: https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

[105] Idem

[106] Idem

[107] Idem

- **Vulnerabilidades por mantenimiento:** la falta de mantenimiento puede presentar sistemas que no están actualizados y que presentan problemas de seguridad.[108]
- **Vulnerabilidades por el factor humano:** pueden ser las que afecten más a los sistemas ya que suceden por falta de concientización y conocimiento de los usuarios sobre prácticas de seguridad[109]

La mayoría de las actividades que desarrollan las empresas están centralizadas en la utilización de sistemas informáticos y dependen completamente de estas para el normal funcionamiento, sin embargo, las vulnerabilidades debilitan la seguridad de la información el cual es el activo más importante para las empresas y si llegaran a afectar sus datos probablemente causaría daños económicos, productivos y su prestigio también puede afectarse.

Es necesario organizar la seguridad de la información asignando roles y responsabilidades a los integrantes de la empresa. También se debe definir políticas de la seguridad de la información que deben estar orientadas a los integrantes de la empresa comunicando sobre el uso adecuado de los recursos de la información. Debe ser un documento que fortalezca la gestión de las tecnologías de la información y la seguridad informática, con una duración extensa que evite realizar cambios frecuentes, deberá ser clara y no generar confusiones y la información será clasificada de uso confidencial, interno o público. [110]

Para minimizar los riesgos es recomendable tener en cuenta las medidas preventivas que sean necesarias como prácticas de seguridad, actualizaciones, tener herramientas de seguridad como antivirus, evitar ingresar a sitios web o correos de procedencia desconocida, realizar inventario de los activos, realizar

[108] Idem

[109] Idem

[110]MINTIC. Guía para la implementación de Seguridad de la información en una MIPYME. {En línea} 2016. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

pruebas de penetración e implementar medidas correctivas para reducir las amenazas.[111]

A continuación, se realiza una explicación de las recomendaciones más importantes: [112]

- **Establecer políticas de seguridad:** se refiere a un plan creado según las funciones y necesidades de la empresa, para proteger la información, salvaguardar la confidencialidad y establecer el uso apropiado del sistema que se utiliza en la empresa con el objetivo de reducir los riesgos, daños o el ingreso no autorizado en el cual se debe incluir a los empleados, hardware y software. Para su desarrollo es necesario identificar las vulnerabilidades, amenazas internas y externas e implementar medidas de protección y planes de contingencia si se llega a presentar un ataque o falla. Los empleados deben conocer las políticas de seguridad de la empresa y las compañías deben capacitarlos para que sean utilizadas además de convertirse en un hábito donde puedan actuar de la mejor manera cuando identifican una sospecha que genere una amenaza para la empresa. En las políticas de seguridad se debe tener en cuenta prohibir el acceso a páginas web sospechosas, utilizar las conexiones HTTPS y evitar introducir memorias USB externas sin autorización.[113]
- **Respaldar información y recuperarla:** las compañías que realizan copias de seguridad frecuentemente, reducen el impacto que genera un ataque informático, ya que pueden recuperarse más rápido. Los respaldos de información se pueden realizar en medios físicos, en la nube o en las dos, según las necesidades de la empresa, lo importante es realizarlas de manera

[111] Idem

[112] PORTAFOLIO Siete consejos para proteger los sistemas informáticos de las compañías. {En línea} 2017. Disponible en: https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755

[113] Idem

periódica y automática. En el caso de información confidencial es importante que se guarde para mayor seguridad con el encriptado de los backups y con contraseñas.[114]

- **Cifrar las comunicaciones de la empresa:** el cifrado impide que personas no autorizadas lean o roben la información además de garantizar la autenticidad de los datos. La información que se envía es cifrada mediante algoritmos que solo se puede decodificar con la clave correcta por lo tanto solo puede ingresar a la información quien tiene la clave. Para las empresas debe ser una prioridad corporativa las comunicaciones donde se envían datos confidenciales como contraseñas, datos personales o financieros, llamadas, listas de contactos, mensajes confidenciales a través de whatsapp entre otros. [115]
- **Utilizar antivirus:** toda empresa debe tener instalado antivirus en sus equipos ya que están expuestas a virus informáticos ya sea por la información financiera que manejan o sus datos confidenciales. Los antivirus deben estar actualizados, si los empleados utilizan otros dispositivos como tablets o celulares también deben tener instalado el antivirus para evitar los ataques.[116]
- **Proteger los equipos conectados a la red:** se debe considerar la protección tanto de equipos de cómputo como impresoras o televisores inteligentes, dado que también pueden recibir ataques. Para estos dispositivos no existen antivirus, pero se debe tener precauciones para su cuidado, en el caso de las impresoras lo ideal es ubicarlas atrás del cortafuego y sin conexión abierta a internet, el software debe estar actualizado, cifrar el disco duro y tener control de su uso por medio de contraseñas. Para los televisores inteligentes se debe ingresar únicamente en sitios seguros, descargar únicamente aplicaciones oficiales y el software debe estar actualizado. [117]

---

[114] Idem

[115] Idem

[116] Idem

[117] Idem

- **Precaución sobre dispositivos móviles:** con el avance de la tecnología también han aumentado los delitos informáticos los cuales se han dirigido en los últimos años a los dispositivos móviles, los ataques se realizan a través de aplicaciones de juegos o entretenimiento que aparentemente no son una amenaza, pero que intrusos utilizan para obtener información y datos confidenciales de los usuarios, también están dirigiendo ataques a los celulares por medio de ransomware, por lo tanto se debe tener en los dispositivos la instalación de antivirus, no ingresar a páginas o aplicaciones con contenido inseguro y tener copias de seguridad. [118]
- **Utilizar herramientas de seguridad:** es recomendable utilizar firewalls o cortafuegos los cuales ayudan a prevenir ataques exteriores en las redes locales, aunque los computadores cuentan con estas opciones, para mayor seguridad se puede adquirir dispositivos hardware o software que ayudan a analizar y filtrar el tráfico en la red y detectar posibles amenazas. El cortafuego que se adquiere como dispositivo hardware analizara amenazas en todos los dispositivos y el cortafuego software es una aplicación instalada en el computador que solo analizara amenazas donde se encuentre instalado. [119]
- **Protección de la red WIFI:** frecuentemente los intrusos utilizan la red WIFI para ingresar a la red de las empresas, por lo tanto, se debe cambiar la clave que esta por defecto en el router por una más segura y el nombre de la red, se recomienda utilizar el nivel de seguridad WPA2, reducir los rangos de las direcciones IP permitidas y autenticar a todos los usuarios que se conectan a la red. [120]
- **Utilizar contraseñas complejas:** existen aplicaciones, cuentas o sistemas operativos que solicitan una contraseña para su ingreso, es importante que sean creadas con un nivel de complejidad que no sean fáciles de descifrar por los intrusos. Se recomienda realizar combinación de números y letras además

[118] Idem

[119] Idem

[120] Idem

de caracteres que no sean comunes como un asterisco un punto un espacio etc. [121]

- **Ignorar correos sospechosos:** evitar ingresar o responder correos sospechosos, si contienen enlaces no se deben abrir ni descargar archivos adjuntos, ya que pueden tener contenido malicioso o pueden robar la información. Los correos electrónicos de phishing aparentemente son de entidades con la cual el usuario tiene alguna relación de una cuenta o negocio, en estos casos aprovechan los intrusos para engañar al usuario suplantando a la entidad solicitando datos confidenciales como números de cuenta o contraseñas, se recomienda cambiar la contraseña de las cuentas periódicamente.[122]

Para mejorar la seguridad de la información en las empresas se debe tener en cuenta tres tipos de medidas de seguridad. La seguridad perimetral referente a elementos y dispositivos electrónicos que garanticen la protección física de los sistemas. Medidas de seguridad externa basados en la protección de los sistemas informáticos de ataques externos como los hackeos, denegación de servicio entre otros, para proteger a los sistemas de amenazas externas es necesario contar con herramientas de seguridad como firewall, antivirus o routers con protección DDoS y las medidas de seguridad interna referentes a la protección de la información y la red de acciones locales o acciones incorrectas que realicen los usuarios de manera involuntaria como intencional.[123] La seguridad informática en las empresas como se menciona anteriormente depende de varios factores, es importante que todos los funcionarios que realizan sus actividades a través de medios tecnológicos se comprometan a aplicar las herramientas, normas y recomendaciones de seguridad para evitar ataques informáticos. Además, las

[121] ARATECNIA. Medidas de seguridad informática que deben tener las empresas. {En línea} Zaragoza. Disponible en: http://www.aratecnia.es/medidas-de-seguridad-informatica/

[122] Idem

[123] SISTERNAS Pau. Medidas de seguridad informática para las empresas. {En línea} Emprende Pyme. 2018. Disponible en: https://www.emprendepyme.net/medidas-de-seguridad-informatica-para-las-empresas.html

empresas deben fomentar el desarrollo de la cultura de seguridad de la información realizando capacitaciones y concientizando al personal sobre ciberseguridad de acuerdo a las políticas, normas y procedimientos de la organización y realizar controles para verificar que se cumplan las prácticas de seguridad establecidas e implementando acciones de sensibilización respecto a la seguridad informática. [124]

[124] CIC. La importancia de la seguridad informática en la empresa. {En línea} 2019. Disponible en: https://www.cic.es/seguridad-informatica-empresa/

9 MECANISMOS DE CONCIENTIZACIÓN A LOS USUARIOS Y EMPRESAS DE LA IMPORTANCIA DE APLICAR HERRAMIENTAS Y NORMAS DE SEGURIDAD

Aunque las empresas inviertan en infraestructura, tecnología y herramientas de seguridad para protegerse de ataques cibernéticos, el personal representa la mayor vulnerabilidad en cuanto al riesgo que se expone la información, por lo tanto, es necesario concientizar a los empleados sobre la seguridad de sus datos. A pesar de ser el factor humano el más crítico es el más descuidado, desafortunadamente las empresas se enfocan más por la seguridad en cuanto a infraestructura; sin embargo la mayoría de los ataques que se presentan se generan por personal desinformado y que no dimensionan la problemática que ocasionan las conductas incorrectas en el manejo de la red, representando para las empresas una vulnerabilidad, ya que los intrusos se enfocan inicialmente en la debilidad de la mayoría de las empresas referente a un usuario no capacitado [125] Por lo tanto, es indispensable para las empresas realizar campañas de capacitación a los empleados sobre los riesgos de la seguridad informática.

9.1 CONCIENTIZAR A LOS EMPLEADOS

Para las empresas no es suficiente la inversión que realizan en infraestructura, los esfuerzos técnicos y mecanismos de seguridad, es necesario enfrentar un mayor desafío referente a crear conciencia en los empleados sobre la seguridad de la información. A demás de comunicar a los empleados sobre los riesgos es necesario implementar herramientas y métodos educativos para que los empleados se acostumbren a utilizar hábitos para el cuidado de la información.

[125] IMPACTOTIC. Seguridad de la información un tema de tecnología y conciencia. {En línea} 2018. Disponible en: https://impactotic.co/seguridad-de-la-informacion-educacion-en-toda-la-organizacion/

Las estrategias que se pueden utilizar para concientizar a los empleados en el manejo de la privacidad de la información son realizar capacitaciones, campañas internas o demostraciones con gráficas y casos reales para que tengan una visualización global de la problemática.[126]

Es importante que las empresas consideren efectuar un programa de Concientización de la Seguridad de la información que fortalezca el conocimiento de los empleados y que conozcan las políticas, procedimientos y prácticas de seguridad de la empresa que se deben tener en cuenta tanto personal como al intervenir personas externas. Muchos de los empleados no se preocupan por la información que se utiliza de manera corporativa por lo tanto las empresas deben aportar estrategias de concientización de la información como una herramienta para que los empleados comprendan su rol en la organización y se puedan apropiar de las responsabilidades que tienen dentro de la empresa para preservar la seguridad de los datos y su confidencialidad.[127]

9.2 CUIDAR Y PROTEGER LA INFORMACIÓN:

Las ventajas de realizar un programa de Concientización de la información pueden aumentar el nivel de seguridad y profundizar en la importancia de cuidar y proteger la información. Además, reduce el riesgo que los empleados puedan realizar malas prácticas por falta de conocimiento y que puedan estar preparados o realizar un plan estratégico o de contingencia en el momento de presentarse un incidente por alguna falla de seguridad.128 Las empresas pueden tener un grado elevado de inseguridad cuando no cuentan con herramientas o procedimientos de seguridad y sobre todo cuando no existe educación del personal para minimizar los riesgos que se presenten. Se debe tener en cuenta para cuidar y proteger la información, realizar pruebas de ingeniería social, campañas de motivación a los

[126] Idem

[127] Idem

[128] Idem

empleados para la protección de los datos, realizar cambios donde se puedan detectar vulnerabilidades y realizar reuniones periódicamente informando al personal sobre el estado actual de la seguridad de la información con base en esto realizar medidas preventivas y talleres en beneficio del mejoramiento de la seguridad. [129]

Para que el programa de Concientización sea efectivo se requiere compromiso de todo el personal con el objetivo de cumplir las estrategias y de manera gradual practicar los hábitos de protección de la información. El programa además debe estar en continuo desarrollo, encaminado a las necesidades de cada organización y presentar un cronograma que especifique las capacitaciones que se realizaran[130].

La Concientización de la seguridad de la información ayuda a que el personal este mejor capacitado en cuanto a identificar las amenazas de seguridad y pueda realizar medidas preventivas que reduzcan los riesgos de la privacidad de la información.

9.3 ESTRATEGIAS PARA LA CREACIÓN DE CAPACITACIONES DE CONCIENTIZACIÓN PARA LOS EMPLEADOS DE LA ORGANIZACIÓN

De acuerdo a la publicación 800-50 del Programa de concientización y capacitación sobre seguridad de la tecnología de la información del Instituto de estándares y tecnología existen 4 fases para la concientización sobre seguridad informática referentes al diseño, desarrollo, difusión, evaluación y monitoreo del cumplimiento:[131]

---

[129] Idem

[130] Idem

[131] VARGAS SALCEDO Julio. Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa {En línea} Fundación Universidad Piloto de Colombia. Disponible en: http://polux.unipiloto.edu.co:8080/00004663.pdf

9.3.1 Etapa de diseño: se debe tener en cuenta para iniciar la concientización del personal, las necesidades de la organización y estar encaminada a la cultura y arquitectura de la tecnología de la información. En esta etapa se tiene en cuenta:

- **Propósito:** para formar sensibilización y concientización en los integrantes de la organización las empresas deben enseñar la importancia de la seguridad de la información, esto ayudara a la compañía a mejorar la seguridad e identificar los riesgos sobre la información confidencial. No es un proceso fácil el entrenamiento y la capacitación del personal cuando se cambian los procesos internos que se han realizado siempre y que requieren ser reemplazados por otros procedimientos más seguros, ya que a veces las personas no se adaptan a cambiar las acciones que han realizado durando mucho tiempo y están acostumbradas a realizar las tareas de la misma manera, por lo tanto es importante que el mensaje y propósito de las capacitaciones sean llamativas, centradas y fáciles de entender además deben convencer de ser adecuadas e impulsar a realizar cambios en el comportamiento que ha realizado anteriormente el personal y que genera riesgos, con las capacitaciones se necesita demostrar que las nuevas prácticas que se realizaran serán más seguras y protegerán a la información.[132]

- **Personal al cual se transmite el mensaje:** todos los integrantes de la organización deben comprometerse para crear un ambiente de seguridad informática. El mensaje que se transmita debe ser claro y unificado, para esto se debe acordar con la gerencia y administrativos el objetivo que desean transmitir y que deberá conocerse por todas las áreas e integrantes de la organización. Es importante que en las capacitaciones participen los integrantes de las áreas de la organización, ya que al estar en constante relación con los

[132] Ibid., p. 8.

sistemas pueden ayudar a identificar los riesgos y socializar con todo el grupo las necesidades de la organización, se debe tener en cuenta los aportes de los integrantes, priorizar las amenazas más relevantes y los temas de seguridad que necesitan profundizar[133].

- **Alcance:** se refiere a los requisitos necesarios para diseñar, desarrollar, implementar y conservar el programa de educación de seguridad informática, se tiene en cuenta las necesidades de la concientización y capacitación de todo el personal, áreas y procesos, desde los niveles más bajos a los más altos como la gerencia. Los objetivos principales en las capacitaciones son[134]:
  - **Cambiar las acciones habituales:** el personal debe ser accesible al cambio es decir si existen acciones que dejan en riesgo la seguridad de la información y se han realizado cambios para el mejoramiento, el personal debe estar disponible y aplicar las nuevas normas de seguridad.
  - **Conocer los riesgos:** el personal debe tener la capacidad de identificar los riesgos a los que este expuesta la información y realizar las acciones correctas para evitarlos.
  - **Apoyar el proceso de la capacitación:** el personal debe ser considerado como un apoyo para el mejoramiento de la seguridad, ya que conoce los procesos que se realizan y cuales están en mayor riesgo, de esta manera también puede colaborar y guiar a los demás integrantes a comprender la importancia de la seguridad y de las capacitaciones.

- **Política:** las políticas de concientización de seguridad de la información deben ser claras y debe conocerlas todo el personal, la empresa deberá garantizar que todos los integrantes están debidamente capacitados para cumplir con las responsabilidades delegadas, ejecutando acciones seguras para salvaguardar

[133] Ibid., p. 8.

[134] Ibid., p. 8.

la información confidencial. Las políticas contienen una serie de actividades que deberá cumplir el personal para alcanzar los objetivos determinados por la organización para la seguridad de la información. En las políticas del programa de concientización se debe incluir los requisitos que necesita la organización para el desarrollo del programa, roles y responsabilidades de los integrantes de la organización, la estrategia, el plan de educación y mantenimiento del programa.[135]

- **Funciones y responsabilidades:** el encargado del desarrollo del programa de comunicación deberá comunicarse con los administradores, ejecutivos y gerencia de la empresa para identificar los resultados que pretenden obtener del programa y como pueden contribuir para su desarrollo. Se deberá determinar los siguientes roles con sus respectivas funciones y responsabilidades: [136]
  - **Líderes de la organización:** los gerentes de la empresa deben darle importancia a la seguridad de la información así como al programa de concientización y sensibilización del personal por eso es importante crear una área adecuada donde los encargados de las capacitaciones desarrollen la creación del programa enfatizando en los temas de seguridad de los datos y un entrenamiento constante, deberá existir una persona que lidere y comunique los temas de comunicación sobre las políticas y el camino que seguirá las campañas de concientización. Se debe realizar un cronograma de las reuniones donde se comunique el avance y notifique las novedades respecto a la mejora de la seguridad, verificar que el presupuesto y recursos sean acordes a los objetivos que se establecen y contar con el personal capacitado para la seguridad de la información.[137]

[135] Ibid., p. 8.

[136] Ibid., p. 8.

[137] Ibid., p. 9.

- **Líderes de gestión estratégica:** será el encargado de gestionar el entrenamiento, supervisar al personal y brindar aportes significativos para la seguridad de la información. Tiene gran responsabilidad ya que entre sus tareas le corresponde establecer una estrategia global, garantizar que los integrantes de la organización comprendan los nuevos alineamientos e informar el avance de las capacitaciones para que tengan claro sus responsabilidades. [138]
- **Jefe de seguridad TI:** tiene la responsabilidad de verificar que el contenido de la capacitación sea apropiado, oportuno y sea utilizado de manera correcta y efectiva, verificar que los usuarios y gerentes estén comunicando de manera clara lo aprendido en las capacitaciones, garantizar que el contenido del programa de concientización sea actualizado y revisado periódicamente.[139]
- **Jefes de área:** deben cumplir con los requisitos que se determinan en las capacitaciones e informar a los colaboradores. [140]
- **Usuarios:** son el objetivo de las campañas de concientización a quienes se debe priorizar la transmisión del mensaje para reducir las vulnerabilidades. Los usuarios pueden ser los empleados, contratistas, proveedores o visitantes. [141]

9.3.2 Etapa de desarrollo: la gerencia será un ejemplo para los funcionarios de la empresa, es necesario que aplique las normas y prácticas de seguridad de la información correctamente además de motivar a los empleados a seguir estas acciones. Deberá la empresa establecer un objetivo claro, que sea alcanzable dirigido los integrantes de la organización. Es importante que todos cumplan correctamente las sugerencias del plan de concientización para reflejar un cambio

[138] Ibid., p. 9.
[139] Ibid., p. 9
[140] Ibid., p. 9
[141] Ibid., p. 9

positivo, el programa de concientización ayuda a informar a los empleados sobre la mejor manera de utilizar controles de seguridad para proteger la información, pueden conocer las políticas y procedimientos que se aplican además de conocer las sanciones ante el incumplimiento.[142] En esta etapa se tiene en cuenta:

- **Aprendizaje continuo:** el aprendizaje dirigido a los funcionarios debe contener información concreta sobre los riesgos a los que está expuesta la información ya sea en el correo electrónico corporativo, redes sociales, mensajes enviados a través de diferentes medios entre otros, para que el aprendizaje se asimile más fácil también se puede realizar en las capacitaciones juegos o dinámicas donde puedan participar todos los integrantes. [143]
- **Concientización:** las campañas de concientización sirven para cambiar las acciones incorrectas realizadas por los integrantes de la organización y aplicar buenas prácticas de seguridad. Los profesionales de seguridad deberán identificar los temas principales que se deben tratar en el programa de concientización y conocer los retos a los cuales se enfrenta la organización para aplicar las acciones correctas que minimicen los riesgos generados por el personal con el fin de crear cultura con respecto a la seguridad informática. [144]
- **Capacitaciones:** las capacitaciones ayudan al personal a ampliar sus conocimientos, habilidades y aptitudes, de manera que puedan tener un mejor desempeño de sus actividades, adaptándose a los cambios que sugiere la empresa. Es un proceso educativo en el cual el personal obtiene el conocimiento necesario y las habilidades para demostrar la eficacia adquirida para realizar las actividades que ayuden a cumplir con los objetivos de la empresa. [145]
- **Educación:** los usuarios adquieren un nivel de educación considerable cuando tienen la capacidad de utilizar sus habilidades de seguridad y su conocimiento

[142] Ibid., p. 9

[143] Ibid., p. 9

[144] Ibid., p. 9

[145] Ibid., p. 10

para identificar los riesgos a los que se encuentra expuesta la información brindando una solución o actuando de la mejor manera para evitar un ataque. Los encargados de las capacitaciones deben transmitir el mensaje de los objetivos del programa de concientización concretamente. Según la disponibilidad y actitud del personal deberán utilizar métodos para el aprendizaje de las normas, prácticas y recomendaciones que serán aplicadas continuamente. [146]

- **Desarrollo profesional:** el nivel de conocimiento sobre seguridad informática del personal de la empresa dependerá del cargo que desempeñen, se recomienda realizar actividades o recompensas para motivar a los empleados cuando desarrollan adecuadamente las actividades teniendo en cuenta las medidas de seguridad de la información que se sugieren en las capacitaciones. [147]

9.3.3 Etapa de difusión: para trasmitir el mensaje y los objetivos que se desean alcanzar con el programa de concientización, existen diferentes maneras como la publicación de carteles ubicados en puntos estratégicos dentro de la empresa, colocar mensajes en los fondos de pantalla de los computadores, realizar dinámicas o preguntas con respecto a los temas que se están tratando en las capacitaciones, mensajes en objetos que utilizan a diarios los empleados como esferos, libretas, llaveros entre otros, también se puede enviar mensajes a los correos de los empleados, realizar teleconferencias o reuniones con personas especializadas en el tema y que presenten casos reales para comprender la gravedad de una empresa que no cuente con la seguridad de la información, esto dependerá de la complejidad del mensaje y los recursos que proporciona la empresa.[148]

---

[146] Ibid., p. 10

[147] Ibid., p. 10

[148] Ibid., p. 10

9.3.4 Etapa de evaluación: después de haber realizado las respectivas capacitaciones, los encargados de transmitir y desarrollar las campañas del programa de concientización deberán realizar seguimiento, ya que los funcionarios de la empresa suelen olvidar los conocimientos aprendidos, la empresa crea nuevos procesos, existen cambios de infraestructura, cambios de cargo, nuevos empleados etc, por lo tanto es importante que realicen evaluaciones periódicamente y actualicen el contenido de las capacitaciones cuando sea necesario, deberán contar con estrategias que ayuden a que el programa de las capacitaciones siga desarrollándose y aplicándose las medidas de seguridad de la información ya que el objetivo de las campañas de concientización es que la empresa demuestre una mejora continua en los procesos que realizan los empleados en beneficio de la seguridad de los datos.[149]

9.3.5 Monitoreo de cumplimiento: cuando las campañas finalizan los encargados del programa deben realizar seguimiento a través de procesos que ayuden a monitorear el cumplimiento y eficacia de los temas tratados en las campañas de concientización. Deberán recolectar datos de la empresa para analizar y realizar informes del estudio de toda la compañía referente a iniciativas de sensibilización, capacitación y educación. Esta información se puede recolectar a través de encuestas, reuniones con todo el grupo de trabajo o entrevistas. [150]

La creación de un programa de concientización es fundamental para las empresas ya que genera en los funcionarios un cambio de cultura enfocada a proteger la información y realizar procesos donde puedan participar todos los integrantes de los cuales se espera la mejor disponibilidad y apoyo en el proceso de aprendizaje de las normas, políticas y medidas de seguridad de la información, para mitigar los riesgos a los que se exponen los datos confidenciales. Es importante fortalecer en

[149] Ibid., p. 10.

[150] Ibid., p. 10.

los integrantes de la empresa la capacidad de identificar las vulnerabilidades o ataques que se puedan presentar y la manera de actuar correctamente cuando se presentan estos casos. Se espera que el cambio empiece por la motivación de la alta gerencia la cual deberá ser ejemplo para los colaboradores en transmitir adecuadamente el mensaje de seguridad de la información. Para el desarrollo de las campañas de concientización es necesario que el personal encargado de brindar las capacitaciones sea altamente calificado y que la compañía cuente con los recursos para cumplir con las estrategias que plantea el equipo encargado de desarrollar el programa.

10 CONCLUSIONES

Los medios tecnológicos benefician a la sociedad, facilitando muchas de las actividades que realizan las personas y se han convertido en una necesidad y prioridad para el funcionamiento de muchas empresas; no obstante, también han sido utilizados para fines incorrectos. A medida que avanza la tecnología los delitos informáticos también van desarrollándose ya que los intrusos encuentran nuevas formas para ingresar a los sistemas, por esta razón se debe optar por implementar herramientas, mecanismos, prácticas y normas que ayuden a proteger la información. Para las personas que hacen uso de los medios tecnológicos es importante estar actualizados sobre el tema del cibercrimen y conocer los delitos más frecuentes y las técnicas que utilizan los intrusos. Los delitos informáticos especialmente se están realizando hacia las entidades bancarias, según investigaciones pocas empresas utilizan herramientas para prevenir los riesgos, o no invierten lo suficiente en la seguridad de sus datos, esto puede afectar considerablemente la información incluso pueden perderla completamente, lo cual representa para las empresas una gran desventaja y genera desconfianza en sus clientes.

La mayoría de los ataques se han generado por fallas de programación donde existen vulnerabilidades, falta de inversión en herramientas de seguridad y principalmente por falta de cultura informática el cual es un factor crítico para las organizaciones. Es importante que las personas se concienticen sobre la utilización de los servicios tecnológicos para que implementen mecanismos que permitan prevenir los ciberataques. Cualquier persona puede llegar a ser víctima de un delito informático y con mayor razón las empresas, la mejor manera de minimizar los riesgos es conocer los casos frecuentes que se están presentando, que afectan la seguridad informática, es necesario contar con aplicaciones que ayuden a identificar las amenazas, tener estrategias y medidas de seguridad que permita a las empresas estar preparadas ante las acciones de los

ciberdelincuentes y si en algún momento se llegara a realizar un ataque el impacto no sea tan grave o por lo menos tener respaldo de la información.

La criminalidad informática representa un desafío tanto para los usuarios, empresas, entidades policiales y judiciales que investigan la procedencia de los delitos, se deben afrontar con el conocimiento para comprender que consecuencias pueden generar, cada persona que esté en relación con los medios tecnológicos debe tener la capacidad de identificar una amenaza y afrontar de la mejor manera estas situaciones.

Con la creación de los decretos y leyes sobre la seguridad informática es posible penalizar las acciones incorrectas a través de los medios tecnológicos, dado que muchas veces las empresas por temor a afectar su prestigio o perdida de sus clientes muchos de los delitos no son denunciados. El tema del cibercrimen es bastante amplio y está en constante cambio ya que los intrusos encuentran nuevas formas de realizar delitos.

La presente monografía está enfocada en las vulnerabilidades más comunes que los criminales informáticos utilizan para cumplir sus objetivos. En este documento también se presentó el análisis sobre algunos casos reales ocurridos en Colombia y que han afectado a empresas, así como a los usuarios de las mismas. Por lo tanto, es necesario estudiar esta problemática y tener un panorama global de los riesgos a los que se expone la información en las empresas colombianas y la manera de prevenirlos. Finalmente se realiza las recomendaciones ante los delitos informáticos que más se generan.

11 RECOMENDACIONES

Teniendo en cuenta las vulnerabilidades que se presentan en los sistemas de las empresas, se menciona a continuación las recomendaciones más importantes: [151]

Establecer políticas de seguridad: plan creado según las funciones y necesidades de la empresa, para proteger la información, salvaguardar la confidencialidad y establecer el uso apropiado del sistema que se utiliza en la empresa con el objetivo de reducir los riesgos, daños o el ingreso no autorizado en el cual se debe incluir a los empleados, hardware y software.[152]

Respaldar información y recuperarla: las compañías que realizan copias de seguridad frecuentemente, reducen el impacto que genera un ataque informático, ya que pueden recuperarse más rápido.[153]

Cifrar las comunicaciones de la empresa: el cifrado impide que personas no autorizadas lean o roben la información además de garantizar la autenticidad de los datos. [154]

Utilizar antivirus: toda empresa debe tener instalado antivirus en sus equipos ya que están expuestas a virus informáticos ya sea por la información financiera que manejan o sus datos confidenciales. Los antivirus deben estar actualizados, si los empleados utilizan otros dispositivos como tablets o celulares también deben tener instalado el antivirus para evitar los ataques.[155]

---

[151] PORTAFOLIO Siete consejos para proteger los sistemas informáticos de las compañías. {En línea} 2017. Disponible en: https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755

[152] Idem

[153] Idem

[154] Idem

[155] Idem

Proteger los equipos conectados a la red: se debe considerar la protección tanto de equipos de cómputo como impresoras o televisores inteligentes, dado que también pueden recibir ataques. [156]

Utilizar herramientas de seguridad: es recomendable utilizar firewalls o cortafuegos los cuales ayudan a prevenir ataques exteriores en las redes locales.[157]

Protección de la red WIFI: frecuentemente los intrusos utilizan la red WIFI para ingresar a la red de las empresas, por lo tanto, se debe cambiar la clave que esta por defecto en el router por una más segura y el nombre de la red. [158]

Utilizar contraseñas complejas: existen aplicaciones, cuentas o sistemas operativos que solicitan una contraseña para su ingreso, es importante que sean creadas con un nivel de complejidad que no sean fáciles de descifrar por los intrusos.[159]

Ignorar correos sospechosos: evitar ingresar o responder correos sospechosos, si contienen enlaces no se deben abrir ni descargar archivos adjuntos, ya que pueden tener contenido malicioso o pueden robar la información. .[160]

---

[156] Idem

[157] Idem

[158] Idem

[159] ARATECNIA. Medidas de seguridad informática que deben tener las empresas. {En línea} Zaragoza. Disponible en: http://www.aratecnia.es/medidas-de-seguridad-informatica/

[160] Idem

BIBLIOGRAFÍA

ABC Sociedad. Mulas de dinero {En línea} 2018. Disponible en: https://www.abc.es/sociedad/abci-mulas-dinero-nuevo-fraude-puedes-participar-sin-querer-201812311104_video.html

Abogado defensor. Victimas de estafas por internet {En línea} 2018. Disponible en: https://www.tuabogadodefensor.com/victimas-estafas-internet/

ABUSHIHAB Amir. Cibercrimen una aproximación a la delincuencia informática {En línea} Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/1995/Abushihabamir2016.pdf?sequence=1&isAllowed=y

ACTUALICESE. Aspectos que regula el Decreto 1377 de 2013 {En línea} 2014. Disponible en: https://actualicese.com/aspectos-que-regula-el-decreto-1377-de-2013-en-el-contrato-para-el-tratamiento-de-datos-personales/

ACTUALICESE. El ciberdelito es una industria en crecimiento. Las compañías necesitan compañías que las apoye {En línea} 2019. Disponible en: https://actualicese.com/el-ciberdelito-es-una-industria-en-crecimiento-las-companias-necesitan-una-guia-que-las-apoye/

ACUÑA Luisa y VILLA Sandra. “Estado actual del cibercrimen en Colombia con respecto a Latinoamérica” {En línea} 2018. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/25619/%20lfacunal.pdf?sequence=1

AMCHAM COLOMBIA. ¿Cómo pueden afrontar las empresas colombianas los riesgos cibernéticos? {En línea} Bogotá. 2019. Disponible en: https://www.amchamcolombia.co/es/comunicaciones/noticias-afiliados/2907-como-pueden-afrontar-las-empresas-colombianas-los-riesgos-ciberneticos

ARATECNIA. Medidas de seguridad informática que deben tener las empresas. {En línea} Zaragoza. Disponible en: http://www.aratecnia.es/medidas-de-seguridad-informatica/

ARIAS Diana. Colombia el país con más ransomware en Latinoamérica en 2018. {En línea} 2019 Disponible en: https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/

ATUESTA Luis, Delitos informáticos aumentaron en Colombia durante la cuarentena. Citado por: Semana. {En línea} 2020. Disponible en: https://www.semana.com/on-line/tecnologia/articulo/delitos-informaticos-aumentaron-en-colombia-durante-la-cuarentena/662686

AVAST. Exploits. {En línea}. 2020. Disponible en: https://www.avast.com/es-es/c-exploits

BAUTISTA Fredy. Colombia el país con más ransomware en Latinoamérica en 2018. Citado por: ARIAS Diana. {En línea} 2019. Disponible en: https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/

BAUTISTA Fredy. Tendencias del cibercrimen en Colombia 2019-2020. Citado por TicTac. {En línea} 2019. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

BECK. Que es el forjacking. {En línea} 2019. Disponible en: https://abdc.es/blog/formjacking-que-es-como-evitarlo/

Cancillería. Concejo de Europa invito a Colombia a adherir a la convención sobre Delito Cibernético. {En línea} Bogotá. 2013. Disponible en: https://www.cancilleria.gov.co/newsroom/news/consejo-europa-invito-colombia-adherir-la-convencion-sobre-delito-cibernetico

CARACOL RADIO. Wall Street banda que desocupaba cuentas de bancos y empresas {En línea} Quindío. 2019. Disponible en: https://caracol.com.co/emisora/2019/10/22/armenia/1571698682_047504.html

CARRASQUILLA Claudia, Cada día se presentan 138 denuncias por estafa en Colombia. Citado por: EL TIEMPO. Documento de la fiscalía señala que en los primeros 8 meses del 2019 se reportaron 33986 delitos. {En línea} 2019 Disponible en: https://www.eltiempo.com/justicia/delitos/denuncias-por-estafa-en-colombia-411020

Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Compilado por Ricardo Antonio Parada; José Daniel Errecaborde. - 1a Ed {En línea} Ciudad Autónoma de Buenos Aires. Erreius, 2018. Disponible en: http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

CIC. La importancia de la seguridad informática en la empresa. {En línea} 2019. Disponible en: https://www.cic.es/seguridad-informatica-empresa/

COMPUCHANNEL. ¿Qué es un ataque de denegación de servicio? {En línea}. 2018 Disponible en: https://www.internetya.co/ataques-de-denegacion-de-servicio-ddos-un-riesgo-real/

DECIDEO. 90% de los colombianos está seriamente preocupado por el fraude de tarjetas bancarias" {En línea} 2019. Disponible en: https://www.decideo.com/90-de-los-colombianos-esta-seriamente-preocupado-por-el-fraude-con-tarjetas-bancarias-Nuevo-Indice-de-Seguridad_a2311.html

Diario oficial. Ley 1273 de 2009. {En línea} 2009. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

DIAZ Juan. Cuidado el smishing está al acecho. {En línea} LAS 2ORILLAS. 2019 Disponible en: https://www.las2orillas.co/cuidado-el-smishing-esta-al-acecho/

DINERO. 90% de los colombianos preocupados por fraude de tarjetas. {En línea} 2019 Disponible en: https://www.dinero.com/economia/articulo/transacciones-digitales-como-evitar-el-fraude-online/279725

DINERO. Suplantando a Bancolombia para estafar clientes. {En línea} 2017. Disponible en: https://www.dinero.com/empresas/articulo/campana-de-phishing-afecta-a-miles-de-clientes-de-bancolombia/242871

ECURED. Ataque informático. {En línea} Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

ECURED. Ciberespacio. {En línea} 2020. Disponible en: https://www.ecured.cu/Ciberespacio

EL ECONOMISTA. Caso de vishing con pretexto de reembolso. {En línea} 2018. Disponible en: https://www.eleconomista.com.mx/finanzaspersonales/Nuevo-caso-de-vishing-opera-con-el-pretexto-de-rembolsos-20180826-0062.html

EL ESPECTADOR. En 2019 se registraron 48 billones de intentos de ciberataques en Colombia {En línea} 2020. Disponible en: https://www.elespectador.com/tecnologia/en-2019-se-registraron-48-billones-de-intentos-de-ciberataques-en-colombia-articulo-908787

EL TIEMPO. Cada día se presentan 138 denuncias por estafa. {En línea} 2019 Disponible en: https://www.eltiempo.com/justicia/delitos/denuncias-por-estafa-en-colombia-411020

EL TIEMPO. Cibercrimen le cuesta a Colombia 190.000 millones de pesos al año. {En línea} 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesos-al-ano-380830

EL TIEMPO. Colombia el país de Latinoamérica más afectado por ransomware en el 2018. {En línea} 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/los-paises-mas-afectados-por-ransomware-en-2018-313224

Forbes Staff. ¿Cómo combatir la ciberseguridad en este 2020? {En línea} 2020. Disponible en: https://forbes.co/2020/01/25/tecnologia/como-combatir-la-ciberseguridad-en-este-2020/

GARCIA Jay, Cibercimen le cuesta a Colombia más de $190 mil millones de pesos al año. Citado por: EL TIEMPO. Distintos ataques afectan a empresas y agencias gubernamentales en Colombia. {En línea} 2019 Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesos-al-ano-380830

Germannube. Ley 1281 de 2012, Protección de datos Colombia {En línea} YouTube. 2013. 1:20 minutos. Disponible en: https://www.youtube.com/watch?v=9ypqfqlu-kw

HERNANDEZ Orlando. Estadísticas delitos informáticos de 2010 a 2018. {En línea} Boletín ágora consultorías. 2018. Disponible en: https://www.slideshare.net/donorlan/boletin-agora-consultorias-estadistica-ciberdelitos-2010-a-agosto-2018

HERRERO Miguel. El cibercrimen también te afecta. {En línea} INCIBE. 2015. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/economia-cibercrimen

HOYOS Víctor. ¿Qué tal está Colombia en cuestión de ciberseguridad? {En línea} 2015. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/7794/Qu%E9?sequence=1

INCIBE. Amenaza vs Vulnerabilidad {En línea}. 2017. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

INFOLAFT. Lo que debe saber sobre el cibercrimen en Colombia {En línea} 2014. Disponible en https://www.infolaft.com/lo-que-debe-saber-sobre-el-cibercrimen-en-colombia/

JULIA Samuel. 5 riesgos de seguridad informática en tu empresa que podrías evitar. {En línea} GADAE. 2020. Disponible en: https://www.gadae.com/blog/riesgos-de-seguridad-informatica/

Kaspersky. ¿Qué es un botnet? {En línea}. 2013. Disponible en: https://www.kaspersky.es/blog/que-es-un-botnet/755/

Kaspersky. ¿Qué es un virus troyano? {En línea} Disponible en: https://www.kaspersky.es/resource-center/threats/trojans

LA CRONICA DEL QUINDIO. El malware se disfraza de COVID-19. {En línea} Quindío. 2020. Disponible en: https://www.cronicadelquindio.com/noticia-completa-titulo-el-malware-se-disfraza-de-covid-19-nota-138164

LUBECK Luis. Phishing suplanta identidad de reconocido banco de Colombia y busca robar información financiera {En línea} 2019. Disponible en https://www.welivesecurity.com/la-es/2019/06/05/phishing-activo-reconocido-banco-colombia/

MALWAREBYTES. Ransomware. {En línea} 2019. Disponible en: https://es.malwarebytes.com/ransomware/

MARTINEZ FERREL, Ernesto. Las diferentes amenazas de seguridad informática. {En línea}. 2018. Disponible en: https://sites.google.com/site/lasamenazaslainformatica/

MEDIACLOUD. vulnerabilidad informática. {En línea} disponible en: https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

MEJIA Mariana. El phishing es el ciberataque más común en medio del confinamiento. {En línea} 2020. Disponible en: https://caracol.com.co/radio/2020/05/07/tecnologia/1588814967_884881.html

MINTIC. Guía para la implementación de Seguridad de la información en una MIPYME. {En línea} 2016. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MORALES Juan David. Ciberestafas en tiempos de coronavirus ¿Cómo no caer en ellas? {En línea} EL TIEMPO. 2020. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/estafas-en-internet-han-aumentado-durante-la-pandemia-del-coronavirus-486284

MOSQUERA Darío. Perspectiva global para la aplicación de la seguridad informática. {En línea} Universidad Piloto de Colombia. 2016. Disponible en: http://35.227.45.16/bitstream/handle/20.500.12277/2662/00003815.pdf?sequence=1&isAllowed=y

IMPACTOTIC. Seguridad de la información un tema de tecnología y conciencia. {En línea} 2018. Disponible en: https://impactotic.co/seguridad-de-la-informacion-educacion-en-toda-la-organizacion/

MUÑOZ Fernando. Cibercrimen: su computador o Smartphone van a ser atacados. {En línea} IMPACTOTIC. 2019. Disponible en: https://impactotic.co/cibercrimen-su-computador-va-a-ser-atacado-en-5-4-3/

OSI. Fraudes online {En línea} 2013. Disponible en: https://www.osi.es/es/actualidad/blog/2013/06/28/fraudes-online-vi-has-ganado-un-premio

PEÑA Juliana. Legislación aplicable a las conductas delictivas en internet {En línea} Disponible en http://bibliotecadigital.usbcali.edu.co/bitstream/10819/737/1/Legislacion_Aplicable_Conductas_Pena_2009.pdf

PINTO Alba, CANTON Isabel y SANTOS Yorly. Prácticas de riesgo en redes sociales y whatsapp por estudiantes de educación básica secundaria {En línea} 2019. Disponible en: http://www.revistaespacios.com/a19v40n23/19402307.html

PORTAFOLIO Siete consejos para proteger los sistemas informáticos de las compañías. {En línea} 2017. Disponible en: https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755

PORTAFOLIO. Colombia es el segundo país latinoamericano con mayor riesgo de conducta negativa en internet. {En línea} 2018. Disponible en: https://www.portafolio.co/tendencias/trucos-con-los-que-buscan-hacerle-el-quite-al-reconocimiento-facial-536538

PORTAFOLIO. El secuestro de información desangra a las empresas del país {En línea} 2019. Disponible en: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

PUENTES Juan. Aumenta el cibercrimen en Colombia en el contexto de COVID-19. Citado por: ACIS. COVID 19 La tormenta perfecta para ciberdelincuentes {En línea} Bogotá. 2020. Disponible en: https://acis.org.co/portal/content/noticiasdelsector/aumenta-el-cibercrimen-en-colombia-en-el-contexto-de-covid-19

RADIO SANTA FE. Compañías colombianas son más reactivas que preventivas en materia de cibercrimen {En línea} Bogotá. 2019. Disponible en: http://www.radiosantafe.com/2019/08/13/companias-colombianas-son-mas-reactivas-que-preventivas-en-materia-de-cibercrimen/

Redacción atmosfera. Colombia sufrió 42 billones de intentos de ciberataque en 3 meses. {En línea} EL TIEMPO. 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666

Redacción profesional Líder. Casi 50% de las empresas han sido víctimas de delitos financieros {En línea} EL ESPECTADOR. 2018. Disponible en: https://www.elespectador.com/economia/casi-el-50-de-las-empresas-han-sido-victimas-de-delitos-financieros-articulo-798201

Save the children. Grooming que es, como detectarlo y prevenirlo. {En línea} Disponible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

SEGUIN Patrick. Spyware. {En línea} AVAST.2020. Disponible en: https://www.avast.com/es-es/c-spyware

SEMANA. Así esta Colombia en el ranking de ciberseguridad mundial. {En línea} 2019. Disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

Significados.com. Ciber. {En línea} 2015. Disponible en: https://www.significados.com/ciber/

SISTERNAS Pau. Medidas de seguridad informática para las empresas. {En línea} Emprende Pyme. 2018. Disponible en: https://www.emprendepyme.net/medidas-de-seguridad-informatica-para-las-empresas.html

SoftwareLab ¿Qué es el SPAM? {En línea} 2020. Disponible en: https://softwarelab.org/es/que-es-spam/

TECNOSFERA. En 2019 se reportaron más de 28000 casos de ciberataques en Colombia {En línea} EL TIEMPO. 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

TicTac. Tendencias del cibercrimen en Colombia 2019-2020 {En línea} CCIT. 2019. Disponible en: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

TOLEDO Edgar. Metodología para la forensia Informática. {En línea} 2008. Disponible en: http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/bitstream/handle/231104/319/Metodologia%20para%20la%20forensia%20informatica.pdf?sequence=1

TORRES Gonzalo. ¿Qué es un virus informático? {En línea} AVG. 2017. Disponible en: https://www.avg.com/es/signal/what-is-a-computer-virus

UID. Delitos informáticos en Colombia. {En línea} 2020. Disponible en: http://uid.org.co/delitos-informaticos-en-colombia/

UNIVERSIDAD LIBRE. Seguridad de la información {En línea}. Bogotá. 2015 Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

VALBUENA Sindy. Bancos en Colombia pueden recibir hasta 10 ataques cibernéticos al mes {En línea} 2018. Disponible en: https://www.rcnradio.com/tecnologia/bancos-en-colombia-pueden-recibir-hasta-10-ataques-ciberneticos-al-mes

VARGAS SALCEDO Julio. Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa {En línea} Fundación Universidad Piloto de Colombia. Disponible en: http://polux.unipiloto.edu.co:8080/00004663.pdf

YOHAI Alberto. Tendencias cibercrimen Colombia 2019-2020 {En línea} Bogotá. 2019. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

ANEXO 1. RESUMEN ANALÍTICO ESPECIALIZADO –RAE

Fecha de Realización:	22/05/2020
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de sistemas
Título:	Casos de estudio de cibercrimen en Colombia
Autor(es):	González Solarte Nancy Adriana
Palabras Claves:	Cibercrimen, amenazas, ataques, riesgos, seguridad informática
Descripción:	Con la presente monografía se pretende identificar las vulnerabilidades que existen en las empresas colombianas con respecto a la seguridad informática, conocer el estado actual del cibercrimen en las empresas colombianas en comparación con años anteriores y brindar las mejores recomendaciones para minimizar los riesgos. Para las empresas colombianas el cibercrimen representa una gran problemática ya que con el aumento de la tecnología gran parte de la información que utilizan se encuentra en la red o los sistemas informáticos por tal razón una amenaza a la seguridad de los datos que manejan genera grandes pérdidas y puede incluso bloquear el normal funcionamiento de las actividades que realizan, generalmente las organizaciones tienen en cuenta la seguridad en cuanto a la infraestructura y olvidan el impacto que puede generar cuando no se tiene una correcta seguridad de la información, es

	importante conocer los mecanismos de defensa que están utilizando las empresas y que necesitan para mejorar la seguridad, además de concientizar a los usuarios para realizar un adecuado uso de los recursos tecnológicos y la manera de reducir el desarrollo del cibercrimen.

Fuentes bibliográficas destacadas:

Acuña, Luisa. Villa, Sandra. “Estado actual del cibercrimen en Colombia con respecto a Latinoamérica”(2018) {en línea} disponible en: (https://repository.unad.edu.co/bitstream/handle/10596/25619/%20lfacunal.pdf?sequence=1)

Toledo Edgar “Metodología para la forensia Informática” (2008). {en línea} disponible en: http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/bitstream/handle/231104/319/Metodologia%20para%20la%20forensia%20informatica.pdf?sequence=1

Yohai Alberto “Tendencias cibercrimen Colombia 2019-2020”–{en línea} (https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf)

PORTAFOLIO “El secuestro de información desangra a las empresas del país” {en línea} disponible en: (https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729”)

El ciberdelito es una industria en crecimiento. Las compañías necesitan compañías que las apoyen” (2019) {en línea} disponible en: (https://actualicese.com/el-ciberdelito-es-una-industria-en-crecimiento-las-

<table>
<tr><td colspan="2">companias-necesitan-una-guia-que-las-apoye/)

EL TIEMPO “Colombia sufrió 42 billones de intentos de ciberataque en 3 meses” {en línea} disponible en: (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666)</td></tr>
<tr><td>Contenido del documento:</td><td>INTRODUCCIÓN
1. DEFINICIÓN DEL PROBLEMA
1.1 PLANTEAMIENTO DEL PROBLEMA
1.2 FORMULACIÓN DEL PROBLEMA
2. JUSTIFICACIÓN
3. OBJETIVOS
3.1 OBJETIVO GENERAL
3.2 OBJETIVOS ESPECÍFICOS
4. MARCOS DE REFERENCIA
4.1 MARCO TEÓRICO
4.2 MARCO CONCEPTUAL
4.2.1 Ataques más comunes en el ciberespacio Colombiano
4.2.1.1 Ataques bancarios
4.2.1.2 Cibercrimen
4.2.1.3 Ciberespacio
4.2.1.4 Estafa Nigeriana
4.2.1.5 Estafas electrónicas
4.2.1.6 Forjacking
4.2.1.7 Impacto del cibercrimen
4.2.1.8 Malware
4.2.1.9 Phishing
4.2.1.10 Ransomware</td></tr>
</table>

	4.2.1.11 Riesgos del cibercrimen 4.2.1.12 Smishing 4.2.1.13 Vishing 4.3 ANTECEDENTES 4.4 MARCO LEGAL 4.4.1 CONPES 3701 de 2011 4.4.2 Ley 1273 de 2009 4.4.3 Ley 1581 de 2012 4.4.4 Decreto 1377 de 2013 5. ESTADO ACTUAL DEL CIBERCRIMEN EN COLOMBIA 6. ANÁLISIS DEL IMPACTO NEGATIVO DEL CIBERCRIMEN PARA LAS EMPRESAS COLOMBIANAS 6.1 CASOS REALES QUE HAN AFECTADO A EMPRESAS COLOMBIANAS 7. ESTADÍSTICAS DE CIBERDELITOS DEL AÑO 2020 EN COMPARACIÓN CON LOS AÑOS ANTERIORES 8. RECOMENDACIONES PARA PREVENIR, CONTROLAR Y REGULAR LAS VULNERABILIDADES EN LOS SISTEMAS INFORMÁTICOS 9. MECANISMOS DE CONCIENTIZACIÓN A LOS USUARIOS Y EMPRESAS DE LA IMPORTANCIA DE APLICAR HERRAMIENTAS Y NORMAS DE SEGURIDAD 9.1 CONCIENTIZAR A LOS EMPLEADOS 9.2 CUIDAR Y PROTEGER LA INFORMACIÓN 9.3 ESTRATEGIAS PARA LA CREACIÓN DE

	CAPACITACIONES DE CONCIENTIZACIÓN PARA LOS EMPLEADOS DE LA ORGANIZACIÓN 9.3.1 Etapa de diseño 9.3.2 Etapa de desarrollo 9.3.3 Etapa de difusión 9.3.4 Etapa de evaluación 9.3.5 Monitoreo de cumplimiento 10. CONCLUSIONES 11. RECOMENDACIONES BIBLIOGRAFÍA Anexo 1. Resumen Analítico Especializado – RAE101
Conceptos adquiridos :	Con la investigación realizada se puede comprender la importancia de implementar mecanismos, herramientas, políticas y normas de seguridad de la información en las empresas. Se verifica la falta de conocimiento de los empleados que representan un factor crítico ya que pueden cometer errores al utilizar los recursos tecnológicos y por lo tanto generar problemas de seguridad que los afecta de manera productiva y financiera. La seguridad de una organización depende de varios factores, no se debe tener en cuenta solo la infraestructura sino también la seguridad de los activos y el factor humano en el cual se debe enfatizar en su formación con capacitaciones y prácticas para realizar un uso adecuado de la

	tecnología en las actividades que realizan ya que pueden existir vulnerabilidades que deben saber identificar para minimizar los riesgos.
Conclusiones:	Los medios tecnológicos benefician a la sociedad, facilitando muchas de las actividades que realizan y se han convertido en una necesidad y prioridad para el funcionamiento de muchas empresas, sin embargo, también han sido utilizados para fines incorrectos. A medida que avanza la tecnología los delitos informáticos también van desarrollándose ya que los intrusos encuentran nuevas formas para ingresar a los sistemas, por esta razón se debe optar por implementar herramientas, mecanismos, prácticas y normas que ayuden a proteger la información. La mayoría de los ataques se han generado por fallas de programación donde existen vulnerabilidades, falta de inversión en herramientas de seguridad y principalmente por falta de cultura informática el cual es un factor crítico para las organizaciones. Es importante concientizar a las personas que están constantemente utilizando los servicios tecnológicos para que implementen mecanismos que permitan prevenir los ciberataques.