Revista CIES – ISSN-e 2216-0167. Volumen 13. Número 1. Año 2022. Páginas 19-41. Dirección de Investigaciones – Institución Universitaria Escolme (Medellín, Colombia)

Análisis del estado actual de la seguridad informática en tiempos de pandemia, entregando un conjunto de buenas prácticas, para fomentar la seguridad informática en las organizaciones de la ciudad de Medellín

Dany Julián Montoya Gómez
Administración de Sistemas Informáticos, Institución Universitaria Escolme, Medellín, Colombia, djmontoyag@escolme.edu.co

Juan Camilo Arias Vargas
Administración de Sistemas Informáticos Institución Universitaria Escolme, Medellín, Colombia, jcariasv@escolme.edu.co

Alex Ávila Quiceno
Docente investigador, Institución Unviersitaria Escolme, Medellín, Colombia, dec.sistemas@escolme.edu.co

Recibido: 26/11/2021 **- Aceptado:** 24/02/2022 **– Publicado:** 05/04/2022

RESUMEN

El presente proyecto pretende analizar el estado actual de la tecnología, especialmente en la seguridad informática a causa de la pandemia por medio de un análisis documental; entregando un conjunto de buenas prácticas para fomentar la seguridad informática en las organizaciones de la ciudad de Medellín. Para el desarrollo del artículo los principales procedimientos serán: analizar el estado de la seguridad informática antes, durante y después de la pandemia, ver el incremento de incidentes en este rango de tiempo, basados en marcos de referencias nacionales e internacionales, se pretende fomentar la seguridad informática en las organizaciones de la ciudad, aportando un paralelo entre el antes y después de la seguridad informática en tiempos de pandemia, también se incluirán algunas recomendaciones para que las empresas mejoren la funcionalidad y la infraestructura de seguridad.

Palabras clave: normativa; delitos informáticos; internet; información; marcos de referencia.

ABSTRACT

This project aims to analyze the current state of technology, especially in computer security due to the pandemic through a documentary analysis security due to the pandemic by means of a documentary analysis; this project aims to provide a set of best practices to promote computer security in the organizations of the city of Medellin. For the development of the article the main procedures will be: to analyze the state of computer security before, during

and after the pandemic, to see the increase of incidents in this range of time, based on national and international reference frameworks, it is intended to promote computer security in the organizations of the city, providing a parallel between the before and after of computer security in times of pandemic, also some recommendations for companies to improve the functionality and security infrastructure will be included.

Keywords: regulation; cybercrime; internet; information; frameworks.

1. INTRODUCCIÓN

La llegada del COVID-19 generó limitantes y amenazas para varios sectores (Mejía-Delgado & Mejía-Delgado, 2022; García-Lirios & Bustos-Aguayo, 2021). En el caso del sector tecnológico se vio afectada la seguridad informática, ya que al pasar de la modalidad presencial a la virtual; muchas empresas de la ciudad perdieron el control sobre el manejo de los activos informáticos. A causa de esto se presentó un incremento en los delitos informáticos.

De acuerdo con lo anterior la siguiente investigación pretende reflejar la evolución que ha tenido la seguridad informática antes y durante la pandemia COVID-19, siendo este un método asertivo para conocer los diferentes puntos de vista del estado de la seguridad en la ciudad de Medellín, permitiendo observar en qué condiciones se encuentra el sector y lo que posiblemente falta por hacer en este, para que el uso de las tecnologías dentro de las empresas sea más seguro.

Por último, se pretende desarrollar un modelo de buenas prácticas basados en algunos marcos de referencias tanto nacionales como internacionales, que impacte de manera positiva a las empresas de la ciudad de Medellín.

A continuación, se detallarán una serie de conceptos que nos permitirán una mejor comprensión sobre los temas propuestos en este artículo, de manera que las expectativas esperadas cumplan con su finalidad, definiendo entonces:

1.1. ¿Qué es delito informático?

Los delitos informáticos son conductas ilícitas susceptibles de ser sancionados por el derecho penal que hacen uso indebido de cualquier medio informático. La necesidad de seguridad informática es alimentada por las amenazas y ciberdelincuentes que buscan comprometer datos importantes y sistemas completos (Mosquera González, Valencia-Arias, Sepulveda, Obando, 2020; Valencia-Arias et al., 2020a). Sin embargo, no todos los ataques son iguales: no provienen de los mismos autores y usualmente no tienen el mismo propósito.

1.2. ¿Características de los delitos informáticos

* Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
* Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos

pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
* Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de estos.

1.3. ¿Cuáles son los delitos informáticos más comunes?

Estafa
Este tipo de delito se comete a través del robo de identidad. Los criminales utilizan técnicas como el spam, webs falsas o softwares ilegales para engañar a las víctimas y robarles las contraseñas o claves personales. De esta manera, acceden a información confidencial. Un ejemplo de ello es el acceso a datos bancarios (Escuela de Ciencias Jurídicas, 2020).

Suplantación de identidad
La suplantación de identidad sucede cuando la estafa tiene éxito y el criminal obtiene acceso a la información personal. Una vez obtenida, el criminal puede realizar compras, llegando a arruinar a la víctima, o hacerse pasar por la persona a quien ha robado los datos (Escuela de Ciencias Jurídicas, 2020).

Extorsión
Este delito sucede cuando alguien utiliza internet para extorsionar dinero a una persona o empresa. La extorsión se comete de distintas formas. Por ejemplo, el criminal puede tener acceso a información personal y amenazar con exponerla a menos que pague cierta cantidad de dinero a cambio. Los delincuentes también pueden llevar a cabo algún tipo de ataque cibernético para luego exigir un pago para detenerlo. Por este motivo, es muy importante tener un antivirus y proteger las cuentas bancarias y personales con contraseñas de alta dificultad (Escuela de Ciencias Jurídicas, 2020).

Hackeo
Este delito se considera muy grave, ya que el hacker intenta obtener acceso a cuentas personales con la ayuda de un ordenador. Con ello consigue robar información confidencial y puede llegar afectar a los negocios de una empresa (Escuela de Ciencias Jurídicas, 2020).

Acoso
Mucha actividad en internet es anónima y uno de los delitos más comunes es el acoso, afectando sobre todo a los adolescentes. Por ejemplo, se recomienda que no acepten a personas desconocidas en sus redes sociales. Si el acoso se vuelve una amenaza, se pueden tomar acciones legales (Academy, s.f.).

Sitios falsos
Existen sitios web que están diseñados para parecer exactamente un sitio web legítimo en el que confiar. Esto lo hacen para engañar y pedir que se dé información personal, como contraseñas de cuentas, direcciones, números de tarjeta de crédito, etc… Estos intentos normalmente se realizan a través de un correo electrónico, una dirección de correo electrónico falsa, imitando a otra persona o compañía (Aldama, 2017).

1.4. ¿Cómo prevenir los delitos informáticos?

Para poder prevenir los delitos informáticos, se debe:

* Cambiar las contraseñas periódicamente, y cuando esto se haga, debe hacerlas más complicadas y para cada cuenta tener una diferente.
* Cierre sesión en todas sus cuentas al terminar de utilizarlas, sobre todo si comparte ordenador con otras personas.
* Instale un antivirus: El antivirus es una herramienta fundamental para su ordenador.
* Utilice un firewall o cortafuegos para tener un acceso seguro a internet.
* No realizar pagos o transferencias, en computadores públicos, debido a que pueden quedar los datos en este ordenador (Tus Abogados & Contadores, 2019).

1.5. ¿Cuáles son las consecuencias de los delitos informáticos?

Las consecuencias de los delitos informáticos para quien los comete son drásticas penas privativas de prisión y multas, por ejemplo, en uno de los delitos informáticos, puede incurrir entre 48 a 96 meses de prisión y 100 a 1000 SMLMV.
Las consecuencias para la víctima, es el detrimento de su patrimonio y la revelación de sus secretos privados (Tus Abogados & Contadores, 2019).

1.6. ¿Cuál ley regula un delito informático?

La ley que regula los delitos Informáticos es el código penal en sus artículos 269- A y siguientes, anexados a este código, mediante la ley 1273 de 2009, mencionando que estos delitos son aquellos que comete un tercero inescrupuloso, escondiéndose detrás de una pantalla, y en la anonimidad. También este tipo de delitos se presta para obstaculizar el buen funcionamiento o el acceso normal a un sistema informático, a los datos informáticos (Tus Abogados & Contadores, 2019).

1.7. ¿Cómo denunciar un delito informático?

Se puede denunciar de manera presencial o escrita, ante la fiscalía o la policía nacional, estos tipos de delitos se pueden denunciar también de forma virtual; por el tipo de delito que es, es considerado como una querella, y quien está legitimado a realizar la denuncia de forma presencial, es la victima directamente (Tus Abogados & Contadores, 2019).

1.8. ¿Qué son marcos referencia de seguridad informática?

Son un sistema de estándares, pautas y buenas prácticas para gestionar los riesgos que surgen en el mundo digital (Gutiérrez, 2020).

1.9. ¿Controles CIS?

Son pautas de mejores prácticas para la seguridad informática. Las pautas constan de 20 acciones clave, denominadas controles de seguridad críticos (CSC), que las organizaciones deben implementar para bloquear o mitigar los ataques conocidos. Los controles están diseñados de manera que se puedan utilizar medios principalmente automatizados para implementarlos, hacerlos cumplir y monitorear. Los controles de seguridad brindan recomendaciones prácticas y sensatas para la seguridad cibernética, escritas en un lenguaje que el personal de TI entienda fácilmente. Los objetivos de las directrices de auditoría de consenso incluyen:

- Aprovechar el ciberdelito para informar la ciberdefensa, centrándose en áreas de alta rentabilidad.
- Garantizar que las inversiones en seguridad se centren en contrarrestar las mayores amenazas.
- Maximizar el uso de la automatización para hacer cumplir los controles de seguridad, negando así los errores humanos.
- Uso del proceso de consenso para recopilar las mejores ideas (Securix, s.f.).

1.10. ¿Controles NIST?

El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad (Comisión Federal de Comercio, s.f.).

El núcleo del marco es un conjunto de funciones y actividades de seguridad cibernética, resultados esperados y referencias informativas que son comunes en todos los sectores y en la infraestructura crítica. El núcleo del marco consta de cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar.

Identificación
Hacer una lista de todos los equipos, programas software y datos que se utilicen, incluyendo ordenadores portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.

Elaborar y compartir una política de ciberseguridad en la empresa que cubra con los siguientes puntos:

- Funciones y responsabilidades de los trabajadores, proveedores y todo el que tenga acceso a datos delicados.
- Pasos para seguir para protegerse contra un ataque y limitar el daño si se produce un ataque.

Protección

- Controlar quiénes acceden a su red y utilizar sus computadores y otros dispositivos.

- Utilizar programas de seguridad para proteger los datos.
- Codificar los datos delicados, tanto cuando estén almacenados o en tránsito.
- Hacer copias de seguridad de los datos con regularidad.
- Actualizar programas de seguridad con regularidad, en lo posible, automatizar las actualizaciones.
- Implementar políticas formales para eliminar de forma segura los archivos electrónicos y dispositivos en desuso.
- Capacitar sobre ciberseguridad a todas las personas que utilizan sus ordenadores, dispositivos y redes. Puede ayudar a sus trabajadores a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.

Detección

- Monitoree sus computadoras para controlar si detecta acceso de personal no autorizado a sus computadoras, dispositivos y software.
- Revisar su red para controlar si detecta usuarios o conexiones no autorizados.
- Investigar cualquier actividad inusual en su red o por parte de su personal.

Respuesta

Implantar un plan para:

- Notificar a los clientes, empleados y otros cuyos datos pueden estar en riesgo.
- Mantener en funcionamiento las operaciones del negocio.
- Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.
- Investigar y contener un ataque.
- Actualizar la política y el plan de ciberseguridad con las lecciones aprendidas.
- Prepararse para eventos inadvertidos que puedan poner en riesgo los datos.
- Poner a prueba su plan de regularidad.

Recuperación

Después de un ataque:

- Reparar y restaurar los equipos y las partes de su red que resultaron afectados.
- Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación (Comisión Federal de Comercio, s.f.).

1.11. ¿Normas ISO 27001: 2013?

Establece buenas prácticas para implementar un sistema de gestión de seguridad de la información. Hacerlo no solo permite proteger los datos de tu organización, que son el activo más importante, sino también generar mayor confianza entre tus clientes, proveedores y empleados

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los requisitos de seguridad,

los procesos empleados y el tamaño y estructura de la organización. Se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un SGSI se ajuste de acuerdo con las necesidades de la organización, por ejemplo, una situación simple requiere una solución de SGSI simple (Cortez, Ortiz & García, 2018).
Esta norma se puede usar para evaluar por las partes interesadas, tanto internas como externas (Norma Técnica Colombiana, 2013).

2. DESARROLLO DEL ARTICULO

A continuación, se desarrollará la investigación planteada en los objetivos específicos, la metodología que se utilizó se desarrolló en 3 fases:
La prima fase es el estado del arte de la seguridad informática. Esta fase fue desarrollada y presentada al interior del marco teórico.
La segunda fase presenta un comparativo sobre la seguridad informática antes y después de la pandemia.
La tercera fase es un manual de buenas prácticas de seguridad informática basados en marcos de referencias internaciones para las organizaciones de Medellín

SEGUNDA FASE
Se presentará un comparativo sobre la seguridad informática antes y un después de la pandemia

2.1. ¿Seguridad informática antes de pandemia?

Pese a la importancia de sus datos, 77% de las corporaciones podían darse el lujo de no tener planes de contingencia contra ciberataques, incluso, de no aplicarlos aun teniéndolos (IBM, durante su más reciente Think Digital), lo que dio oportunidad a los ciberdelincuentes de atacar por varios frentes (dispositivos móviles, redes sociales, etc.) (Naum, 2020).
40% de las empresas latinas entrevistadas en 2017 por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) sospechaban que un día serían objeto de ciberataques; 52% admitió no estar preparado para afrontarlos; y 56% manifestó no tener personal calificado para disminuir invasiones; un panorama alentador que comprobó que "la ocasión hizo al ladrón" (Naum, 2020)

2.1.1. Ransomware

Ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de Ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de Ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito (Seguridad de la Información, 2021).

Ciberseguridad en 2019
En 2019 las autoridades reportaron cerca de 30 mil casos de ciberataques al sector empresarial en Colombia, además alertaron sobre una gran cantidad de empresas que habrían asumido los costos de estos delitos con tal de proteger su imagen corporativa (Holguín, 2020).

“El antivirus ya no es la única forma de blindar a las organizaciones de los ciberataques. De acuerdo con un estudio realizado por el Mintic, la OEA y el Banco Interamericano de Desarrollo, en Colombia, el 60% de las empresas tuvieron gastos por encima de los 500 mil pesos por daños relacionados con ataques cibernéticos y el 5% perdieron más de 4 mil millones de pesos por este delito. Según la fiscalía, Medellín es la tercera ciudad del país con más casos de ciberataques, la mayoría de ellos a compañías de servicios financieros, consumo y transporte” (Holguín, 2020).

La pérdida de información de las empresas por delitos informáticos en la mayoría de los casos se da por intimidaciones a los empleados de la compañía o la suplantación del correo corporativo (Valencia-Arias et al. 2020b).

2.1.2. Ataques delitos informáticos

En la imagen 1, se muestran las cifras de la variación de los ataques de seguridad del año 2019.

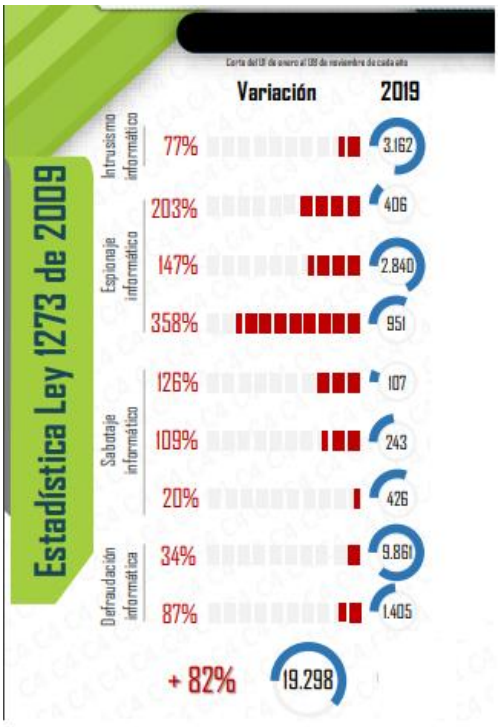

Imagen 1. Variación delitos informáticos 2019. Fuente: Policía Nacional de Colombia (2020).

En la siguiente imagen, se muestran las preocupaciones de seguridad 2019

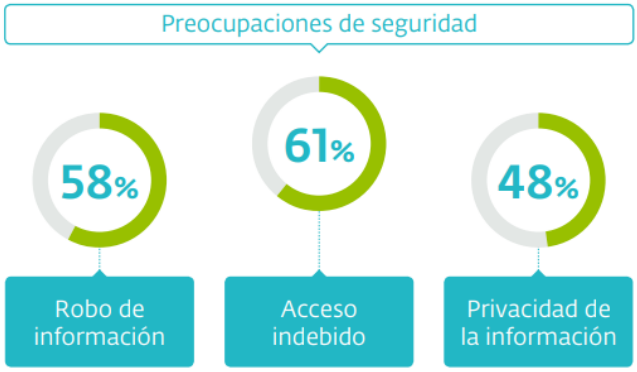

Imagen 2. Preocupaciones de seguridad 2019. Fuente: ESET (2019).

Malware Bancario

En la imagen 3, Malware bancario las soluciones de Kaspersky neutralizaron intentos de ataques de uno o más programas maliciosos diseñados para robar dinero de cuentas bancarias en 766.728 equipos de usuarios.

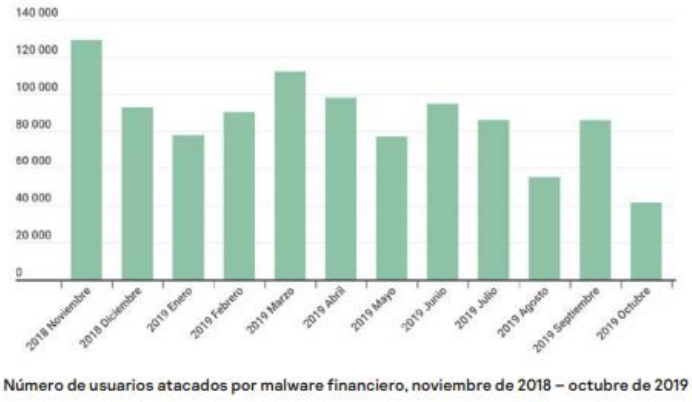

Imagen 3. Malware bancario 2019. Fuente: Kaspersky (2019).

Coin Miners

En el último año, se consolidó como medio de infección la minería de criptomonedas. Las variantes que corresponden a este comportamiento son identificadas por los productos de ESET como CoinMiner y están disponibles para diferentes arquitecturas

El principal riesgo de esta amenaza reside en cómo puede afectar a la reputación de una organización, ya que, si los usuarios notan que los servidores de cualquier empresa que suelen visitar han sido comprometidos, su confianza en ella podría perderse o verse erosionada. Si bien los resultados, en estos casos, no impactan directamente sobre la continuidad del negocio, como sí lo hace el Ransomware, las consecuencias pueden ser graves si la cantidad de usuarios afectados es alta (ESET, 2019).

En la imagen 4, se observa el porcentaje de ataques recibidos en los diferentes sistemas operativos de Coin Miners

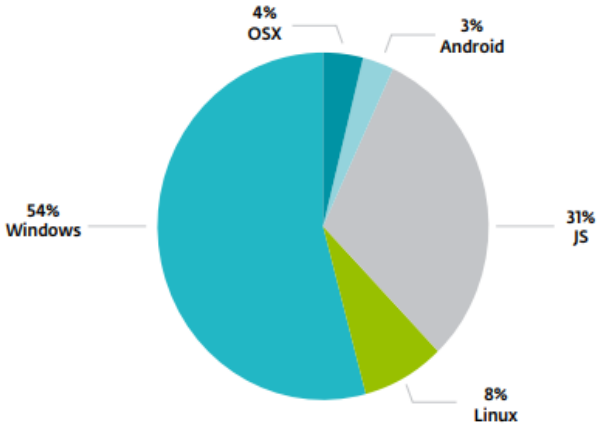

Imagen 4. Plataforma de ataques de Coin Miners. Fuente: ESET (2019).

Phishing

En la siguiente imagen, se puede ver uno de los métodos más utilizados de suplantación de identidad.

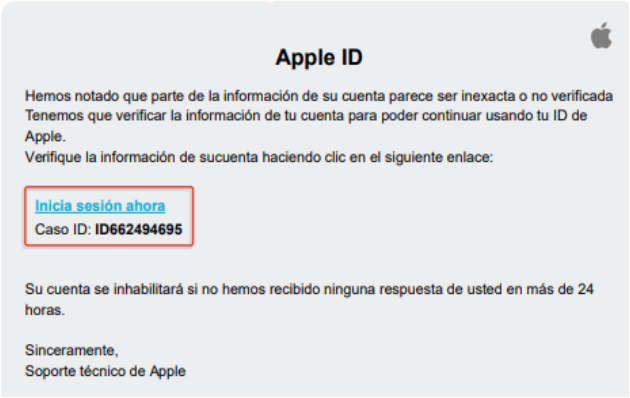

Imagen 5. Phishing Apple. Fuente: ESET (2019).

En esta imagen 6, se muestra el aumento de los delitos informáticos en el año 2019 según el informe de seguridad de ESET.

Imagen 6. Aumento de los delitos informáticos 2019. Fuente: ESET (2019).

2.1.3. ¿Seguridad informática después de la pandemia 2021?

En la actualidad nos hemos visto en la tarea y necesidad de utilizar más los medios digitales como las redes sociales, mediante los equipos personales y celulares para acceso a distintos sitios web. Esto involucra toda la tecnología que se tiene a nuestro alcance y que nos ha permitido estar comunicados en todo momento. Sin embargo, en el afán y día a día en la web, hemos descuidado la seguridad informática, factor de alta relevancia para no ser afectados en nuestra vida personal y financiera.

Es por eso por lo que se hablará del tema de ciberseguridad como factor relevante en nuestro diario vivir. La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos que degradan, alteran y dañan los mismos. También, se conoce como seguridad de tecnología de la información o seguridad de la información electrónica y se aplica en diferentes contextos, desde los negocios hasta la informática móvil personal. Es momento de preguntarse y cuestionarse ¿Cómo estamos utilizando toda esta tecnología y en especial los equipos móviles?

Paralelamente y también muy importante, abarquemos, qué están realizando las empresas. Es un hecho que la tecnología y la especialización en materia de seguridad informática y ciberseguridad marcan tendencias notables que durante 2020 seguirán su rumbo hacia la perfección y profundización. Es por esto que muchas organizaciones buscan actualizar sus estructuras internas para hacer frente a los nuevos desafíos y peligros que nos llegan año a año, no solo con programas y apps especializadas, sino también estableciendo equipos de trabajo y subáreas destinadas a la manutención y cuidado de la estructura de la información (Ortiz, s.f.).

Es ahora cuando la ciberseguridad debe transformarse para apoyar a las organizaciones en diferentes procesos; se deben crear y comprender procesos ágiles que apoyen la seguridad de la información y aportar en ese mundo constante de evolución y transformación.

El mal spam usa ingeniería social para engañar a la gente con el fin de que abra archivos adjuntos o haga clic en vínculos que parecen legítimos, aparentando que proceden de una institución de confianza o de un amigo. Los ciberdelincuentes emplean la ingeniería social en otros tipos de ataques de Ransomware, por ejemplo, presentarse como el FBI para asustar a los usuarios y obligarles a pagar una suma de dinero por desbloquear los archivos.

2.1.4. Violación de datos personales

Es el acceso por partes no autorizadas a datos de acceso restringido. Su peligro existe por la exposición de información y archivos confidenciales a personas no autorizadas sin permiso. Existen diversas modalidades de escape de datos, según si existe intencionalidad, según el alcance del acceso y otro aspecto.

Colombia se ha puesto en la vanguardia en el tratamiento de datos personales como lo están la mayoría de las naciones del mundo, especialmente la Comunidad Europea. Es uno de los

grandes avances legislativos que tuvo el país este año que está por terminar, especialmente si consideramos que somos de los pocos países que penalizan la violación de datos personales.

Como lo menciona Díaz (2013), "en la investigación que realizamos por algo más de diez años, para la redacción de los artículos propuestos en mi proyecto de ley, se dejaron finalmente siete de los diez artículos que originalmente habíamos sugerido, en donde se excluyeron tipos tan importantes como la falsedad informática, espionaje informático y el SPAM, le modificaron el epígrafe a la estafa informática por transferencia no consentida de activos. Por fortuna no se tocó el que nos motiva la atención de esta nota, la violación de datos personales. Si bien es cierto que, en nuestro país, está vigente desde el 31 de diciembre 2008, la ley estatutaria de Hábeas Data, la 1266, no es menos verdad que esta se refiere casi exclusivamente a la protección del dato financiero, sin extender a una protección efectiva a todos los datos personales; de ahí por qué nos preocupamos en la redacción del artículo 269 F, denominado violación de datos personales".

2.1.5. Suplantación de sitios web

También conocido como Web Spoofing consiste en la suplantación de una página web real por otra falsa con el fin de realizar una acción fraudulenta. La web falsa adopta el diseño de la web que se pretende suplantar e incluso una URL similar. Un tipo de ataque más sofisticado consiste en crear una "copia sombra" de toda la página Web para conseguir que el tráfico de la víctima pase por el atacante, de esta manera se obtiene toda la información sensible de la víctima.

Este tipo de ataque consigue redirigir la conexión de una víctima a través de una página falsa hacia otras páginas web con el objetivo de realizar alguna acción fraudulenta asociada con el phishing para obtener información, como usuarios y contraseñas, del tráfico de dicha víctima. Además, es posible que el atacante envíe datos a los servidores de páginas reales en nombre de la víctima o desde cualquier servidor web a la víctima.

Entre las páginas web más susceptibles de ser suplantadas o ser falsificadas en su apariencia, se encuentran las relacionadas con comercio electrónico o e-commerce, que incluyen las páginas de compra y venta, y las páginas de pago online, e incluso paginas estatales o del sector financiero, lo que conlleva la aplicación de circunstancias de agravación punitiva como las del artículo 269H del Codígo Penal. Es de suma importancia que todos los actores de internet se involucren en la seguridad informática, pues es evidente que todos los tipos de tecnología de red pueden ser víctima de suplantación (Sánchez, 2019).

2.1.6. Uso de software malicioso

Es un software diseñado específicamente para obtener acceso a un equipo o dañarlo sin que el usuario tenga conocimiento. Hay distintos tipos de software malicioso, como el spyware, los registradores de pulsaciones, los virus, los gusanos o cualquier tipo de código malicioso que se infiltre en un equipo Norton, s.f.).

Generalmente, para determinar si el software es malicioso, se considera la intención de su creador, más que sus características. La creación de software malicioso está en aumento; esto se debe a que se crean nuevos tipos todos los días y al atractivo del dinero que puede ganarse mediante el crimen organizado en Internet. Originalmente, el software malicioso se creó como un experimento y para realizar bromas, pero luego dio lugar al vandalismo y a la destrucción de equipos. Actualmente, la mayoría del software malicioso se crea para ganar dinero mediante la publicidad forzada (publicidad no deseada), el robo de información confidencial (spyware), la difusión de spam o pornografía por correo electrónico (equipos zombis), o la extorsión (Ransomware) (Norton, s.f.).

2.1.7. Uso de perfiles falsos en redes sociales para difusión de malware

Cuentas falsas en redes sociales como Twitter y Facebook serán usadas para generar contenidos de manera automatizada masificando las cifras de infección de malware (Policía Nacional de Colombia, Dijin, CCIT, Tictac & SAFE, 2019).

Inteligencia artificial y malware

El escaneo automatizado de vulnerabilidades por parte de los Cibercriminales facilitará la detección de víctimas potenciales. El malware podrá detectar si un sistema de seguridad le está analizando (sandbox) y se auto eliminará.

Ataques delitos informáticos

En la imagen 7, se puede observar la variación de los delitos informáticos

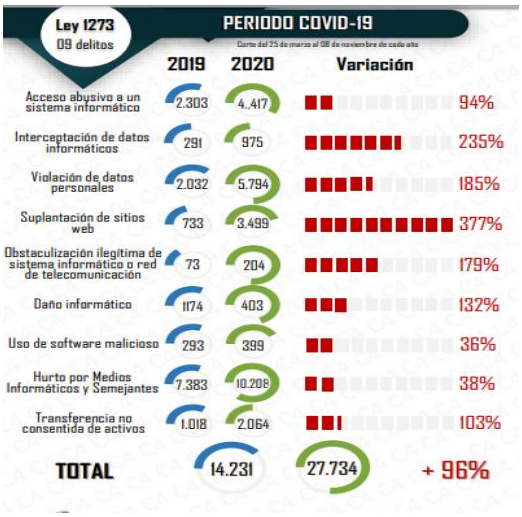

Imagen 7. Delitos informáticos 2020. Fuente: Policía Nacional de Colombia (2020).

2.1.8. Ataques delitos informáticos antes vs después pandemia

En la imagen 8, se observa la variación de delitos informáticos en los periodos de tiempo de 2019 y 2020.

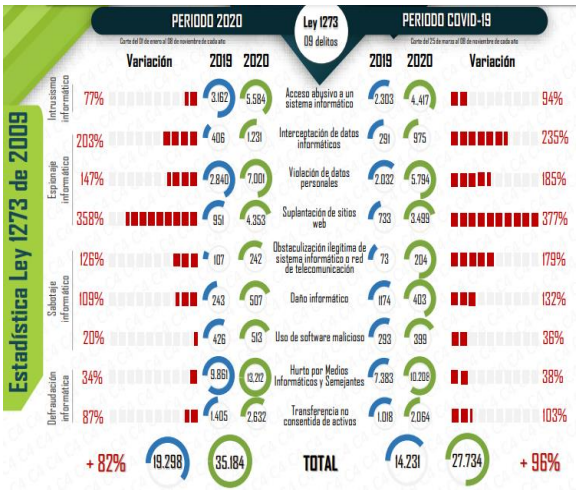

Imagen 8. Variación delitos informáticos año 2019 y 2020. Fuente: Policía Nacional de Colombia (2020).

¿% de crecimiento de los delitos informáticos en Medellín?

En la imagen 9, se ve el crecimiento de los delitos informáticos en la ciudad de Medellín.

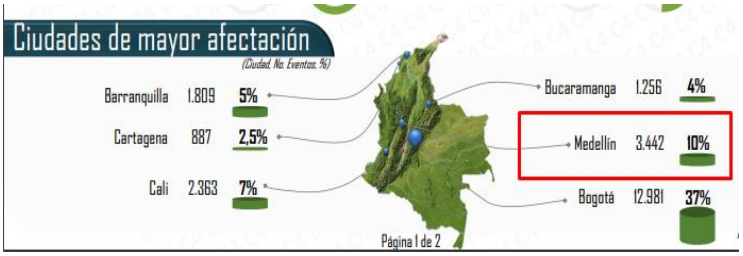

Imagen 9. Crecimiento delitos informáticos. Fuente: Policía Nacional de Colombia (2020).

En la imagen 10, se muestra el aumento de casos delitos informáticos en la ciudad de Medellín.

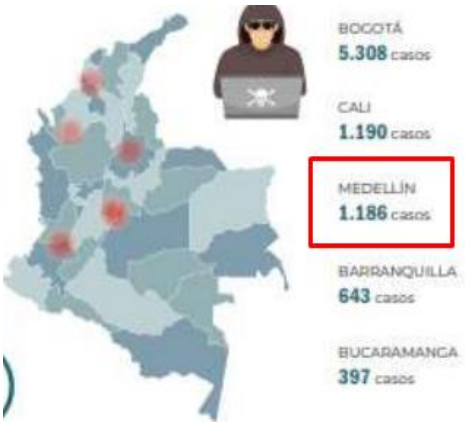

Imagen 10. Casos delitos informáticos Medellín. Fuente: Policía Nacional de Colombia, Dijin, CCIT, Tictac, & SAFE. (2019).

En la siguiente imagen, se puede observar las prácticas de delitos informáticos más comunes después de la pandemia.

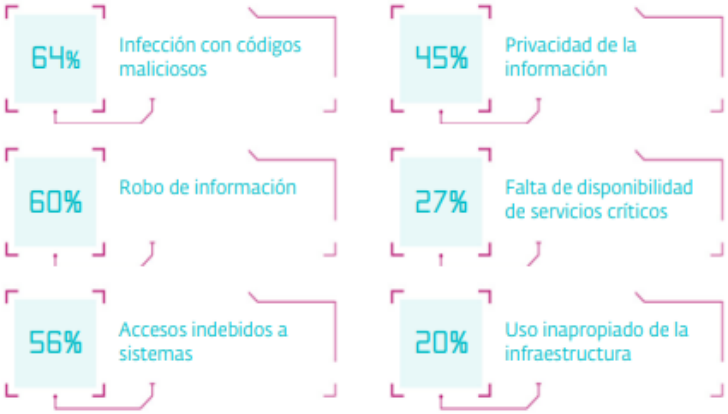

Imagen 11. De las prácticas de gestión de seguridad. Fuente: ESET (2021).

TERCERA FASE

Se presentará un manual de buenas prácticas de seguridad informática basados en marcos de referencias internacionales para las organizaciones de Medellín.

Primero que todo se describiera cada uno de los marcos referencia y estará plasmado en el marco teórico del trabajo y posteriormente se realizara el manual de buenas practicas

Manual de Buenas Practicas

A continuación, presentaremos una serie de controles basados en tres marcos de referencia ISO **27001, CIS y NIST** para este manual se desarrollaron los siguientes controles:

- **Control de Activos**
- **Dispositivos USB**
- **Software antimalware**
- **Redes inalámbricas**
- **Capacitaciones de usuarios**
- **Copias periódicas de seguridad**
- **Contraseñas Seguras**

CONTROL DE ACTIVOS

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se define lo siguiente:

ISO 27001

Control 8.1. La responsabilidad sobre los activos. Con su debido inventario, propiedades y

su respectivo uso, tanto como su devolución.

CIS
Control 1.4. Mantenga un inventario veraz y actualizado de todos los activos tecnológicos capaces de almacenar y/o procesar información. El inventario debe incluir todos los activos de hardware, estén o no conectados a la red de la organización.

NIST
Control ID.AM-1. Los dispositivos y sistemas físicos dentro de la organización deben de estar inventariados.

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se recomienda:

Control 1.1 Utilizar una herramienta de descubrimiento activo
De acuerdo con los controles anteriores se puede concluir que el principal objetivo es la identificación correcta de los activos y las responsabilidades de estos al igual que la correcta evaluación de sus riesgos. Para ello existen diferentes herramientas que pueden ayudar a automatizar dicho control. Entre ellas se encuentra la herramienta GLPI (Gestión Libre del Parque Informático).

DISPOSITIVOS USB
Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se define lo siguiente:

ISO 27001
Control 8.3. El manejo de los soportes de almacenamiento. Como su gestión de soportes extraíbles. La eliminación de estos soportes

CIS
Control 13.7. Se requieren dispositivos de almacenamiento USB, se debe usar software corporativo que pueda configurar sistemas para permitir el uso de dispositivos específicos. Se debe mantener un inventario de tales dispositivos.

NIST
Control PR-PT-2. Habla sobre los medios extraíbles, están protegidos y su uso se encuentra restringido de acuerdo con la política.

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se recomienda:

Control 1.2 Gestionar dispositivos USB
Se debe usar un software corporativo que pueda configurar sistemas para permitir el uso de dispositivos específicos. Se debe mantener un inventario de tales dispositivos permitidos.

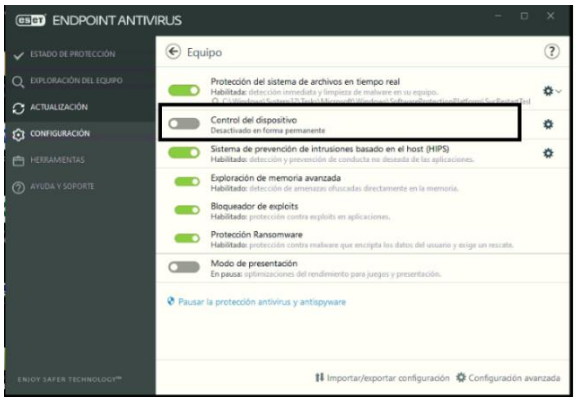

Imagen 12. Control de dispositivos. Fuente: elaboración propia.

SOFTWARE ANTIMALWARE

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se define lo siguiente:

ISO 27001
Control 12.2.1. Protección contra código malicioso.

CIS
Control 8. Utilizar software antimalware gestionado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización**.**

NIST
Control DE.CM-1. El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia.

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se recomienda

Control 1.3 Software antimalware
Se debe implementar un software donde revisemos y controles todo lo que sean software malicioso de todas máquinas de la organización.

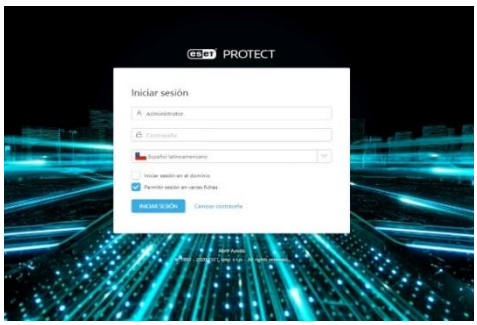

Imagen 13. Software Antimalware. Fuente: elaboración propia.

REDES INALÁMBRICAS

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se define lo siguiente:

ISO 27001
Control 13.1. La gestión de la seguridad en las redes con sus controles y sus mecanismos de seguridad asociados a servicios en red, en los controles.

CIS
Control 15.10. Crear una red inalámbrica separada para dispositivos personales o que no sean de confianza. El acceso de la empresa desde esta red debe tratarse como no confiable y debe filtrarse y auditarse en consecuencia.

NIST
Para este control las NIST no propone ninguna medida.

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se recomienda

Control 1.4. Crear una red inalámbrica separada para dispositivos personales y no confiables
En la imagen 14, se evidencia que se tiene una red inalámbrica llamada INVITADOS para separar los dispositivos personales de los de confianza

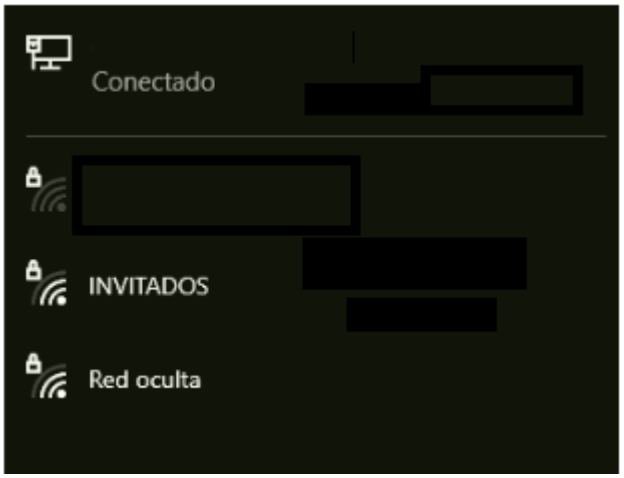

Imagen 14. Redes inalámbricas. Fuente: elaboración propia.

CAPACITACIONES DE USUARIOS

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se define lo siguiente:

ISO 27001
Control 7.2.2. La concienciación, educación y capacitación en seguridad de la información

para los usuarios, en los controles.

CIS
Control 17.2. Realice capacitaciones para abordar el vacío de habilidades identificado para impactar positivamente el comportamiento de seguridad de los miembros de la fuerza laboral.

NIST
Control PR.AT-1. Hablan sobre todos los usuarios, están informados y capacitados.

Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se recomienda

Control 1.5 Capacitación y concientización de la seguridad informática a los usuarios

Se crean campañas semestrales para divulgar temas de seguridad informática, se crean espacios semanales en canales de comunicación para mandar tips de seguridad informática, se crean espacios con preguntas de seguridad, inducciones de seguridad a los empleados nuevos.

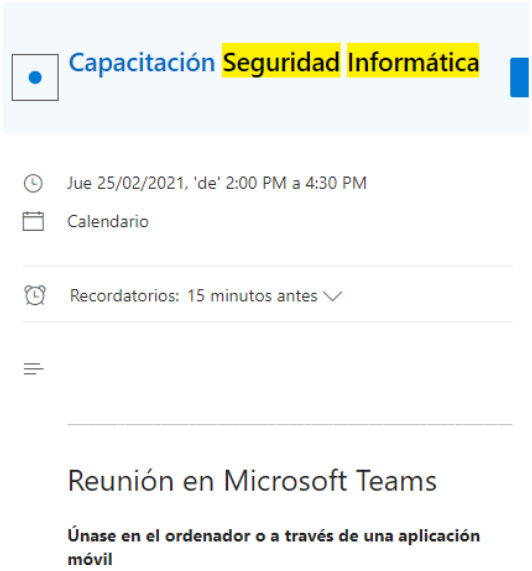

Imagen 15. Capacitaciones seguridad informática. Fuente: elaboración propia.

COPIAS DE SEGURIDAD
Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se define lo siguiente:

ISO 27001
Control 12.3.1. Las copias de seguridad Registrar eventos y generar evidencia, en los controles.

CIS
Control 10.1. Asegurar que se realizan regularmente copias de respaldo de todos los datos de sistemas de manera automatizadas.

NIST
Control PR-IP-4. Se realizan, se mantienen y se prueban copias de seguridad de la información.

Control 1.6. Copias periódicas de seguridad
Contar con copias periódicas de la información según su clasificación.

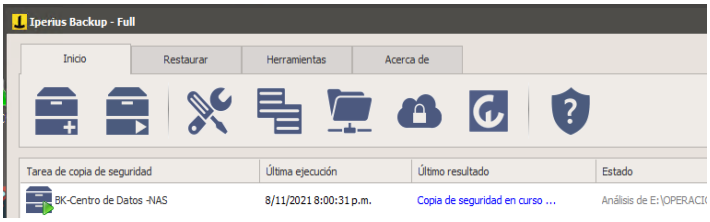

Imagen 16. Copias periódicas de seguridad. Fuente: elaboración propia.

<u>CONTRASEÑAS SEGURAS</u>
Basados en los marcos de referencia ISO **27001, CIS y NIST** sobre el control de activos se define lo siguiente:

ISO 27001
Control 9.4.3. Gestión de contraseñas de usuario. Y la gestión de claves.

CIS
Control 4.4. Se deben usar contraseñas únicas, cuando no está soportada la autenticación multifactor (como el administrador local, root o cuentas de servicio), las cuentas, usarán contraseñas que son únicas de ese sistema.

NIST
Control PR-AC-1. Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

Control 1.7 Contraseñas seguras

Es recomendable implantar un sistema de autenticación de doble en el acceso a servicios que contengan información especialmente sensible o crítica. Se pueden considerar además de la contraseña otro factor como:

- Huella digital
- Tokens de hardware
- 2MFA (Doble factor de autenticación)

3. CONCLUSIONES

El delito informático es el delito del siglo XXI, puede ocasionar grandes pérdidas de dinero en pocos segundos y afectar la privacidad de las personas sin que estas se percaten de ello, entre otras consecuencias, estos delitos van de la mano con los avances tecnológicos.

Debido a las constantes amenazas que se encuentran en los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas, por eso es tan importante tener muy capacitado a los usuarios, son el eslabón más débil y difícil de proteger en las organizaciones.

Las organizaciones deben contar con una política corporativa de trabajo en casa o trabajo remoto con horarios flexibles, con políticas de navegación de internet con el fin de evitar fugas de información y ataques cibernéticos.

La ciberseguridad después de la pandemia se volvió prioridad, más que nunca las empresas tienen que incluir en su estructura la seguridad informática, sin importar el tamaño o el nicho del mercado al que pertenezcan.

Con la elaboración del manual de buenas prácticas se puede concluir que son guías de gran ayuda que nos permite establecer un gobierno de seguridad de la información en las organizaciones. Así mismo con este documento garantizar que las vulnerabilidades y riesgos se minimicen y que los usuarios y toda la estructura organizacional se concienticen en los aspectos de seguridad de la información.

Esta investigación ha demostrado cómo es posible diseñar y crear un manual de seguridad básica, aplicable en empresas partiendo del conocimiento obtenido y la investigación realizada centrándonos en uno de los factores más importantes que es el usuario final.

4. REFERENCIAS

Academy. (s.f.). ¿Qué es ITIL? Descubra una explicación y definición simple de ITIL. Recuperado de https://advisera.com/20000academy/es/que-es-itil/

Aldama, C. (2017). 5 delitos informáticos más comunes de lo que crees. Recuperado de https://informatica-legal.es/delitos-informaticos-comunes-internet-ciberdelito/

Comisión Federal de Comercio. (s.f.). ¿Qué es y cómo funciona el marco de Ciberseguridad del NIST? Recuperado de https://www.ftc.gov/es/tips-advice/business-center/small-businesses/cybersecurity/nist-framework-es

Cortez, N., Ortiz, D., & García, T. (2018). Gestión integrada a la calidad, medio ambiente, seguridad y salud en el trabajo. Recuperado de https://www.academia.edu/37098639/Norma_NTC_Iso_27001_LISTO

Díaz, A. (2013). El delito de violación de datos personales en Colombia. Recuperado de http://oiprodat.com/2013/04/25/el-delito-de-violacion-de-datos-personales-en-colombia/

Escuela de Ciencias Jurídicas. (2020). ¿Cuáles son delitos informáticos más comunes? Recuperado de https://escuelacienciasjuridicas.com/delitos-informaticos-mas-comunes/

ESET. (2019). Eset Security Report Latinoamérica 2019. Recuperado de https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

ESET. (2021). Eset Security Report Latinoamérica 2021. Recuperado de https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

García-Lirios, C., & Bustos-Aguayo, J. M. (2021). Diseño y evaluación de un instrumento para medir el uso de internet en la era COVID-19. *Revista CEA, 7*(14), e1665. https://doi.org/10.22430/24223182.1665

Gutiérrez, N. (2020). Marcos de Ciberseguridad: La Guía Definitiva. Recuperado de https://preyproject.com/blog/es/marcos-de-ciberseguridad-la-guia-definitiva/

Holguín, C. (2020). Medellín es la tercera ciudad del país con más casos de ciberataques. Recuperado de https://telemedellin.tv/medellin-es-la-tercera-ciudad-del-pais-con-mas-casos-de-ciberataques/372725/

Kaspersky. (2019). Boletín de seguridad Kaspersky, 2019 Estadísticas. Recuperado de https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_SP.pdf

Mejía-Delgado, O. A., & Mejía-Delgado, Y. Y. (2022). Madurez tecnológica de la generación Z: reto de la transformación digital en Colombia. Revista CEA, 8(16), e1913-e1913. https://doi.org/10.22430/24223182.1913

Mosquera González, D., Valencia-Arias, A., Sepulveda, J., & Obando Ibarra, C. (2020). Tendencias y evolución investigativa en el campo de la ingeniería en seguridad de sistemas. En: A. Valencia-Arias y M. Hincapie. (Ed). *Evolución y tendencias investigativas e en Ingeniería de Sistemas e Ingeniería Industrial (30-50)*. Sello Editorial Coruniamericana.

Norma Técnica Colombiana -NTS. (2013). Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO 27000). Recuperado de https://docplayer.es/7982301-Norma-tecnica-ntc-iso-iec-colombiana-27001.html

Naum, U. (2020). La ciberseguridad antes, durante y después de la pandemia. Recuperado de https://forbescentroamerica.com/2020/07/14/la-ciberseguridad-antes-durante-y-despues-de-la-pandemia/

Norton. (s.f.). ¿Qué es el software malicioso y cómo puedo evitarlo? Recuperado de https://co.norton.com/internetsecurity-malware.html

Ortiz, F. (s.f.). La ciberseguridad en época de pandemia. Recuperado de https://www.unitec.edu.co/posts/la-ciberseguridad-en-epoca-de-pandemia

Policía Nacional de Colombia, Dijin, CCIT, Tictac, & SAFE. (2019). Informa de las Tendencias del cibercrimen en Colombia 2019-2020. Recuperado de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Policía Nacional de Colombia. (2020). Balance Cibercrimen. Recuperado de https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Sánchez, S. (2019). Web Spoofing: Suplantación de páginas Web y uso indebido de datos personales. Recuperado de https://derinformatico.uexternado.edu.co/web-spoofing-suplantacion-de-paginas-web-y-uso-indebido-de-datos-personales-mediante/

Securix. (s.f.). ¿Su información está protegida? Recuperado de https://securix.com.mx/

Seguridad de la Información. (2021). ¿Qué es ransomware? Recuperado de https://www.pmg-ssi.com/2021/01/que-es-ransomware/

Tus Abogados & Contadores. (2019). Acciones que son consideradas un delito informático en Colombia. Recuperado de https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito-informatico-en-colombia/#Cuales_son_las_consecuencias_de_los_delitos_informaticos

Valencia-Arias, A., Bermeo-Giraldo, M. C., Acevedo-Correa, Y., Garcés-Giraldo, L. F., Quiroz-Fabra, J., Benjumea-Arias, M. L., & Patiño-Vanegas, J. (2020a). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *Revista Ibérica de Sistemas e Tecnologias de Informação, (E29),* 225-239. Recuperado de https://www.proquest.com/docview/2394537804

Valencia-Arias, A., Patiño-Toro, O., Arenas-Fernández, A., Garcés-Giraldo, L. F., Umba-López, A. M., & Benjumea-Arias, M. L. (2020b). Tendencias investigativas en el estudio de la ciberdefensa: un análisis bibliométrico. *Revista Ibérica de Sistemas e Tecnologias de Informação, (E29),* 366-379. Recuperado de https://www.proquest.com/docview/2394538000?pq-origsite=gscholar&fromopenview=true