ATAQUES CIBERNÉTICOS MÁS FRECUENTES EN LAS MIPYMES DE COLOMBIA DURANTE EL PERIODO 2020 - 2021 DE LA PANDEMIA COVID-19

DERLY PAULINA MARTINEZ VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO
2022

ATAQUES CIBERNÉTICOS MÁS FRECUENTES EN LAS MIPYMES DE COLOMBIA DURANTE EL PERIODO 2020 - 2021 DE LA PANDEMIA COVID-19

DERLY PAULINA MARTINEZ VARGAS

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Msc. Katerine Marceles Villalba
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO
2022

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este proyecto a Dios porque en su inmenso amor por sus hijos ha permitido el desarrollo de todas mis actividades propuestas dándome cada día todas las herramientas para salir adelante, a mi esposo e hija quienes siempre me han apoyado en cada decisión, con mucho amor y paciencia dieron espacios para que pudiera emprender y desarrollar todas las actividades para este reto, a mi hermosa madre Yolanda que ha hecho suyos mis triunfos y me ha acompañado siempre.

AGRADECIMIENTOS

A Dios por permitir el desarrollo del todas las actividades diarias, porque a pesar de todas las adversidades me ha fortalecido en su fe y me ha dado la sabiduría para sortear todos los obstáculos para salir adelante, a mi familia, mi esposo e hija por su comprensión y apoyo, a mi mamá Yolanda, quien me ha alentado siempre para no desfallecer, a los tutores de la Unad de quienes he recibido apoyo y todos mis compañeros de grupo, con quienes me he apoyado para fortalecer mis conocimientos y han aportado al cumplimiento de las metas propuestas.

CONTENIDO

INTRODUCCIÓN 18

1 DEFINICIÓN DEL PROBLEMA 20

1.1 ANTECEDENTES DEL PROBLEMA 20

1.2 FORMULACIÓN DEL PROBLEMA 21

2 JUSTIFICACIÓN 22

3 OBJETIVOS 24

3.1 OBJETIVOS GENERAL 24

3.2 OBJETIVOS ESPECÍFICOS 24

4 MARCO REFEReNCIAL 25

4.1 MARCO TEÓRICO 25

4.2 MARCO CONCEPTUAL 34

4.3 MARCO HISTÓRICO 38

4.4 ANTECDENTES 39

4.5 MARCO LEGAL 41

5 DESARROLLO DE LOS OBJETIVOS 44

5.1 Caracterización los delitos informáticos más relevantes en Colombia que afectan las Mipymes 44

5.1.1 Acceso abusivo a un sistema informático 48

5.1.2 Interceptación de datos informáticos 49

5.1.3 Violación de datos personales 50

5.1.4 Suplantación de sitios Web.” 51

5.1.5 Obstaculización ilegítima de sistema informático o red de telecomunicación 52

5.1.6 Daño informático 52

5.1.7 Uso de software malicioso.”. 53

5.1.8 Hurto por Medios Informáticos y Semejantes 54

5.1.9 Transferencia no consentida de activos 55

5.2 Causas por las cuales las Mipymes están siendo vulnerables a los ataques informáticos e identificacion de vulnerabilidades y amenazas 55

5.2.1 Política de protección para acceso remoto a la información personal 59

5.2.2 Mecanismos de monitoreo de consulta de las bases de datos 60

5.2.3 Auditoría de los sistemas de información 61

5.2.4 Sistemas de gestión de seguridad o un programa integral de gestión de datos 62

5.2.5 Medidas especiales para proteger datos sensibles 63

5.2.6 Política de seguridad para el intercambio físico o electrónico de datos 64

5.2.7 Política de auditoría de seguridad de la información 65

5.2.8 Controles de seguridad en la tercerización de servicios para el tratamiento de datos 66

5.2.9 Medidas apropiadas y efectivas de seguridad 68

5.2.10 Herramientas de gestión de datos 69

5.2.11 Políticas y procedimientos de gestión de incidentes de seguridad 70
5.2.12 Vulnerabilidades informáticas y amenazas que afectan las Mipymes 72
5.3 HERRAMIENTAS OPEN SOURCE PARA LA SEGURIDAD INFORMATICA 75
5.3.1 Herramientas Open Source para la seguridad informática en Mipymes 78
5.3.2 Manual de buenas prácticas para Mipymes 92
6 CONCLUSIONES 94
7 RECOMENDACIONES 96
8 BIBLIOGRAFÍA 97
ANEXOS 104

LISTA DE TABLAS

pág.

Tabla 1. Estadística de delitos 2019 – 2020. 28
Tabla 2. Resultados Estudio de medidas de seguridad en el tratamiento de datos personales 2020 31
Tabla 3. Rangos para la Definición del Tamaño Empresarial 36
Tabla 4. Delitos, penas y multas 41
Tabla 5. Tipificación de los Delitos Informáticos 45

LISTA DE FIGURAS

pág.

Figura 1. Crecimiento de incidentes de seguridad con más presencia en 2020 en Colombia 46
Figura 2. Principales modalidades de ciberdelitos 1er trimestre 2020 47
Figura 3. Ciudades de mayor afectación con ciberdelitos 47
Figura 4. Ejemplos observados de relajación de controles de ciberseguridad 57

LISTA DE GRAFICAS

pág.

Gráfica 1. Empresas analizadas estudio Superintendencia de Industria y Comercio ..59
Gráfica 2. Empresas que carecen de una política de protección para acceso remoto a la información personal 60
Gráfica 3. Empresas que carecen de un sistema de control de acceso a bases de datos 61
Gráfica 4. Empresas que carecen de sistemas de auditoria informática 62
Gráfica 5. Empresas de carecen de Sistema de Gestión de la Seguridad de la Información 63
Gráfica 6. Empresas que carecen de política específica que normalice el acceso a las bases de datos sensibles 64
Gráfica 7. Empresas que carecen de Política de Seguridad para intercambio físico o electrónico de datos 65
Gráfica 8. Empresas que carecen de Política de auditoría de la información.....66
Gráfica 9. Empresas que carecen de controles de seguridad en la tercerización de servicios para el tratamiento de datos 67
Gráfica 10. Empresas que carecen de medidas apropiadas y efectivas de seguridad 68
Gráfica 11. Empresas que carecen de herramientas de gestión de datos 69
Gráfica 12. Empresas que carecen de políticas y procedimientos de gestión de incidentes de gestión de incidentes de seguridad 70

LISTA DE ANEXOS

ANEXO 1. Manual de Buenas Practicas de Seguridad Informatica para Las Mipyes en Colombia 102
ANEXO 2. Resumen Analitico Especializado 110

GLOSARIO

AMENAZA: Probabilidad de ocurrencia de eventos que pueden afectar la disponibilidad de recursos y sistemas de información.

CIBERATAQUE: Conjunto de procesos y acciones ejecutadas de manera no autorizada ingresan a un sistema informático con el fin de alterar su funcionamiento y causar daño en su estructura.

CIBERDELITO: Son operaciones delictivas cometidas a través de medios electrónicos en las cuales se ven afectados los usuarios y sus sistemas informáticos.

CIBERSEGURIDAD: Corresponde al grupo de procesos, herramientas físicas y tecnológicas que conjugados entre si buscan la seguridad informática en una organización.

CONFIDENCIALIDAD: Característica de la información que garantiza que ésta sea accedida solo por quienes están autorizados para su consulta, difusión y/o transformación.

DISPONIBILIDAD: Característica de la información que permite su acceso de manera oportuna.

FIREWALL: Conocido también como cortafuegos, es un sistema compuesto por dispositivos hardware, software y/o ambos, los cuales se relacionan bajo unas condiciones y limitantes establecidos por una organización buscando tener un control frente a la información que ingresa y sale en el proceso comunicativo entre dos o más redes.

HACKER: Persona que posee altos conocimientos y habilidades informáticas.

HACKING: Son todas las técnicas, medios y procesos utilizados para acceder de manera no autorizada a un sistema informático.

IDS: "Sistema de detección de intrusos"[1], Definido como son un conjunto de herramientas informáticas usadas para la detección de intrusiones y realización de monitoreo a través del tráfico saliente y entrante de equipos o redes en los SI de una empresa.

INTEGRIDAD: Característica de la información que determina su conservación y coherencia.

MALWARE: Programa con código malicioso el cual al ser ejecutado en un sistema o equipo informático causa daño.

METODOLOGÍA: Grupo de procesos y secuencias organizadas de un determinado tema o área que al ser implementadas logran alcanzar un objetivo.

SOFTWARE OPEN SOURCE: Programas informáticos de código abierto, su licencia permite a las organizaciones que los implementan tener la posibilidad de ajustarlos a sus necesidades.

PENTEST: Pruebas realizadas a organizaciones a través de ataques a su sistema informático que buscan conocer las vulnerabilidades presentes y las amenazas que estás pueden generar.

[1] GOMEZ, Roberto. Seguridad Informática. Detección de Intrusos [en línea]. [Consultado el 30 de julio de 2021]. Disponible en Internet: http://www.cryptomex.org/SlidesSeguridad/IDS.pdf

REDES INFORMATICAS: Agrupación de dispositivos conectados entre sí sobre los cuales existe un flujo de información que comparten y transfieren.

RIESGOS INFORMATICOS: Son la probabilidad de materialización de un evento que afecta un sistema informático.

SEGURIDAD INFORMATICA: Conjunto de procedimientos que buscan proteger la información ante la presencia de accesos no autorizados, ataques y condiciones físicas desfavorables.

VULNERABILIDAD: Es la debilidad que presenta un sistema ante la presencia de riesgos y que permite que este sea atacado.

RESUMEN

El desarrollo de este proyecto busca identificar los ataques informáticos que están afectando las Micro, pequeñas y medias empresas en Colombia dentro del marco de la actual pandemia Covid-19, la cual inició en el país en el mes de marzo del año 2020, se tomará como principal insumo los informes presentados por organismos judiciales quienes de manera conjunta trabajan con entes no gubernamentales cuyo objetivo está en la promoción y fomento de acciones tendientes a la seguridad informática de las organizaciones, con base en los datos aportados los cuales tienen su origen en las denuncias realizadas por las víctimas sobre casos reales se pueden establecer los niveles de aumento de estas modalidades delictivas, el tipo de organizaciones sobre las cuales se están presentando y las causas de vulnerabilidad existentes por medio de las cuales se están materializando los eventos delictivos.

Con el fin de proponer un aporte a la solución de la problemática antes mencionada se realiza la presentación y caracterización de herramientas Open Source a las cuales pueden acceder las organizaciones para ser implementadas buscando generar un esquema de seguridad informática integral que permita mitigar la presencia de los ciberataques.

Palabras Claves: Amenazas informáticas, Ataques Informáticos, Mipymes, normatividad, Open Source, seguridad informática, vulnerabilidad.

ABSTRACT

The development of this project seeks to identify the computer attacks that are affecting Micro, small and medium companies in Colombia within the framework of the current Covid-19 pandemic which began in the country in March 2020, it will be taken as The main input is the reports presented by judicial bodies who jointly work with non-governmental entities whose objective is to promote and encourage actions aimed at the information security of organizations, based on the data provided, which originate from the complaints. carried out by the victims on real cases, it is possible to establish the levels of increase of these criminal modalities, the type of organizations on which they are presenting themselves and the existing causes of vulnerability through which the criminal events are materializing.

In order to propose a contribution to the solution of the aforementioned problem, the presentation and characterization of Open Source tools are made to which organizations can access to be implemented, seeking to generate a comprehensive computer security scheme that allows mitigating the presence of cyberattacks.

Keywords: IT threats, IT attacks, Mipymes, regulations, Open Source, IT security, vulnerability.

INTRODUCCIÓN

El auge de la conexión a través de redes, la sistematización de varios procesos y su evolución de manera acelerada en el mundo ha llevado a que hoy en día muchas organizaciones concentren gran parte de sus operaciones en la tecnología digital, comprometiendo la conservación, disponibilidad y seguridad de numerosa información en la gran red mundial que es el internet**.**

La información hace parte importante dentro de una organización ha pasado de ser almacenada en archivos físicos para ser contenida en forma digital, con ello obligando a sus propietarios a implementar sistemas de gestión y seguridad informática para garantizar su custodia, disponibilidad, confidencialidad e integridad. Esta evolución informática ha generado múltiples beneficios en general y también ha beneficiado a usuarios, clientes, empresas, entes y organizaciones que han podido acceder a servicios sin salir de casa, reducción del tiempo y costo en trámites, acceso a la educación, comunicación, entre otros; al mismo ritmo con que estos avances han crecido también lo ha hecho la delincuencia, que busca sacar provecho de la exposición de la información y la presencia de sistemas vulnerables a través de los cuales ejecutan su actuar con fines económicos y también de desprestigio a las organizaciones.

Colombia no es indiferente a esta situación, los últimos años la ciberdelincuencia ha crecido de manera alarmante, de acuerdo con el informe “Tendencias del Cibercrimen en Colombia 2019-2020”[2] en el año 2019 se incrementaron en un 54% los incidentes cibernéticos respecto a los presentados en el 2018, en estos eventos se han visto comprometidas empresas privadas, del estado y personas naturales, sus sistemas Informáticos han sido atacados poniendo en riesgo su capacidad, prestigio y bienes de clientes y usuarios.

[2] COLOMBIA. POLICÍA NACIONAL. Informe Tendencias del Cibercrimen Colombia 2019-2020. 2019. [Consultado el 19 de julio de 2021]. Disponible en Internet: https://caivirtual.policia.gov.co/#observatorio

Para finales del año 2019 e inicios del 2020 en el mundo se presenta una situación que cambió y afectó la vida de toda la población, el cual fue la pandemia Covid-19, en Colombia el primer caso fue confirmado el 6 de marzo de 2020. Con la llegada de este virus y debido a su alta velocidad de contagio la Organización Mundial para la Salud determinó una serie de medidas a tomar por parte de las naciones para afrontar la situación con miras a evitar el contagio y minimizar su propagación, tomando decisiones como los aislamientos obligatorios de las personas contagiadas, confinamientos obligatorios, cierres temporales de empresas, distanciamiento social y restricción en las movilizaciones; muchas empresas debieron parar sus producciones y servicios, buscar opciones de actividades virtuales para sus empleados con el fin de salvaguardar su salud y bienestar, afectando en mayor proporción a las Mipymes, las cuales son empresas con estructuras organizacionales pequeñas que tienen sistemas de seguridad informática débiles o en el peor de los casos no tiene ninguno.

Las medidas tomadas por el gobierno nacional de manera obligatoria para todos los sectores motivó la creación de alternativas para mitigar las consecuencias económicas críticas a las cuales se vieron expuestas las Mipymes, las empresas forzadas a tener a sus empleados en distanciamiento social empezaron a implementar sistemas a distancia, trabajo en casa, comercio electrónico, dando como consecuencia la ampliación de la estructura tecnológica y de redes con una mayor exposición a los delincuentes cibernéticos, quienes logran acceder a sus víctimas debido a las vulnerabilidades que éstas presentan por tener sistemas de seguridad informática frágiles y desactualizados o no contar con ningún sistema que permita administrar y gestionar sus riegos.

Con el propósito mitigar los riesgos a los cuales estas organizaciones están expuestas se presenta una caracterización de herramientas disponibles, de fácil implementación y sobre todo con costos mínimos, como lo son las open source para pentesting, con el fin de ofrecer alternativas exequibles que permitan su fortalecimiento empresarial a partir de la seguridad informática.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Las organizaciones hoy en día han implementado en sus herramientas de trabajo técnicas que anteriormente eran poco comunes, la tecnología ha permitido la optimización de muchos procesos y servicios, logrando que las empresas sean más eficientes y competitivas.

El uso de las TIC (tecnologías de la información y comunicación) en las empresas determinan un factor importante en su desarrollo económico, para el mes de septiembre de 2019, “En el marco del “1er Congreso de Seguridad y Salud en el Trabajo de la Pequeña y Mediana Empresa – MiPymes”, la ministra del Trabajo, Alicia Arango Olmos, recordó la importancia que tienen las MiPymes en el país, debido a que, según cifras del DANE, éstas representan más de 90% del sector productivo nacional y generan el 35% del PIB y el 80% del empleo de toda Colombia”[3]; sin embargo, esta participación dentro del sector económico se ha visto fuertemente afectada por la presencia de la pandemia covid-19, las empresas de manera urgente han debido implementar estrategias para mantener su productividad y de esta misma forma garantizar el empleo y sobre todo preservar el bienestar de sus trabajadores con el aislamiento preventivo obligatorio.

Dentro de las estrategias acogidas está el teletrabajo, esta modalidad tuvo su origen sobre el año 2018 y a pesar que desde entonces se ha venido desarrollando con el fin de promover el uso de las TIC, fue en la Pandemia cuando realmente su uso se disparó, el comercio electrónico y el marketing digital también se han posicionado, el desarrollo de estas prácticas que sin duda alguna han realizado un gran aporte al sector económico, pero paralelamente al avance de la pandemia, han traído consigo el

[3] COLOMBIA. MINISTERIO DEL TRABAJO. Prensa. Comunicados 2019. [sitio web]. Bogotá. [[Consultado el 15 de octubre de 2021]]. Disponible en Internet: https://www.mintrabajo.gov.co/prensa/comunicados/2019/septiembre/mipymes-representan-mas-de-90-del-sector-productivo-nacional-y-generan-el-80-del-empleo-en-colombia-ministra-alicia-arango

aumento de los delitos cibernéticos, poniendo al descubierto la debilidad que muchas organizaciones tienen en sus sistemas de seguridad informática.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles han sido los sectores empresariales más afectados por los ataques cibernéticos en Colombia y cuáles pueden ser los orígenes de estos eventos durante el periodo de la pandemia Covid-19, marzo 2020 – junio 2021?

2 JUSTIFICACIÓN

A raíz del surgimiento de la pandemia Covid-19 se han presentado muchos cambios en la vida de las personas en diversos aspectos, el entorno social, desarrollo educativo, economía, finanzas, tecnología, el medio ambiente, sin duda alguna el transcurrir cotidiano para todos ahora es diferente. Con más de un año de avance de esta pandemia se han implementado mecanismos y estrategias para contrarrestar las consecuencias que ésta ha venido dejando desde que se presentó el primer caso en Colombia, marzo 6 de 2020.

Las Mipymes consideradas eje fundamental en la economía nacional en medio de su afectación directa han emprendido alternativas que les permitan su continuidad en el negocio, la tecnología ha jugado un papel fundamental en este emprendimiento, con sus herramientas las empresas han implementado el comercio electrónico, el teletrabajo y procesos y servicios de manera remota. El aumento en el uso de los sistemas informáticos para el desarrollo de estas alternativas y la interacción que se ha dado entre los diferentes actores, empresas, clientes, usuarios, ha atraído la atención de los delincuentes quienes han fijado sus objetivos en la red informática.

La falta de educación en seguridad de medios electrónicos e informáticos por parte de las organizaciones hacia sus empleados, clientes y usuarios y la carencia de sistemas seguros ha dado un espacio propicio para que las Mipymes sean vulneradas y atacadas poniendo en riesgo su estabilidad económica, financiera y reputacional.

Si bien el estado por medio de programas de apoyo financiero como el PAEF (Programa de Apoyo al empleo formal), el cual define el Banco Agrario de Colombia como: “El PAEF es un programa social del Estado que otorgará a los beneficiarios del mismo, con cargo a los recursos del Fondo de Mitigación de Emergencias (FOME), un aporte monetario mensual de naturaleza estatal, y hasta por once veces conforme lo dispuso el artículo 1 de la Ley 2060 de 2020, con el objeto de apoyar y proteger el empleo formal

del país, para que con este se propenda por salvaguardar el empleo formal del país”[4]; ha permitido a las Mipymes sostener sus nóminas, el programa SofisTICa a través del cual dan soporte en la productividad y actualización de procesos, bienes y servicios a través de la implementación de soluciones tecnológicas se hace necesario conocer el estado actual de las empresas en cuanto a las vulnerabilidades bajo las cuales están siendo atacadas y ofrecer a ellas herramientas de fácil implementación y uso para fortalecer sus sistemas de seguridad informática.

[4] COLOMBIA. BANCO AGRARIO DE COLOMBIA, Conoce más sobre los programas de Apoyo al Empleo Formal PAEF y Pago de la Prima de Servicios PAP [en línea]. [Consultado el 19 de octubre de 2021]. Disponible en Internet: https://www.bancoagrario.gov.co/Paginas/apoyo_empleo_formal_paef.aspx

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los ataques cibernéticos más frecuentes a los que han estado expuestas las Mipymes de Colombia durante el periodo 2020 - 2021 de la Pandemia Covid-19, mediante la revisión de informes técnicos y judiciales para promover su mitigación por medio de uso de herramientas Open Source de fácil acceso.

3.2 OBJETIVOS ESPECÍFICOS

- Caracterizar los ataques cibernéticos más frecuentes a los que han estado expuestas las Mipymes de Colombia durante el periodo 2020 - 2021 de la Pandemia Covid-19, con el fin mitigar los riesgos informáticos a los cuales están expuestas.

- Determinar mediante el análisis de informes técnicos y judiciales las causas por las cuales las Mipymes están siendo vulnerables a ataques informáticos para la identificación de las vulnerabilidades sobre las cuales se están presentando las amenazas y su materialización.

- Proponer herramientas Open Source de las cuales pueden hacer uso las Mipymes y un manual de buenas prácticas con base a lineamientos y/o directrices que permitan fortalecer su sistema de seguridad de la información.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La comunicación en el mundo ha evolucionado de manera significativa buscando ser cada día más rápida y asequible dada la necesidad de comunicación que por naturaleza tiene el hombre, su origen se remonta a los años A.C cuando aparecieron las pinturas rupestres y los jeroglíficos, los antepasados buscaban comunicarse a través de imágenes y escrituras en piedra, más adelante aparecen lo correos los cuales se realizaban a través de personas que se desplazan de un lugar a otro en caballos llevando consigo la información. Con el invento del papel en China sobre el año 105 D.C[5] y la imprenta en el año 1440[6] permitió un gran adelanto que permitía a muchas personas tener noticias y poder acceder al conocimiento a través de textos, en 1794 se inventó el telégrafo óptico[7], dando paso a la comunicación electrónica con el telégrafo eléctrico y el código Morse en 1837[8]; en 1876 es inventado el teléfono[9] convirtiéndose en la herramienta más importante de comunicación, en 1901[10] la radio y en 1927[11] el televisor, permitiendo la transmisión de voz e imagen, en 1968 aparece la computadora

[5] SANTOS. Abraham. Archivo General del Estado de Oaxaca: La evolución del papel. [en línea]. [Consultado el 20 de octubre de 2021]. Disponible en Internet: https://www.oaxaca.gob.mx/ageo/la-evolucion-del-papel/

[6] VELDUQUE, María. El origen de la imprenta: la xilografía. La imprenta de Gutenberg. [en línea]. España: 2011. p. 5). [Consultado el 20 de octubre de 2021]. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=5169198

[7] ROMEO. José. El Telégrafo Óptico 1790 – 19850: Estudio Critico comparativo de los diferentes sistemas de transmisión utilizados. [en línea]. Madrid. España. [Consultado el 20 de octubre de 2021]. Disponible en internet: https://dialnet.unirioja.es/servlet/articulo?codigo=574200

[8] LUMBRERAS. Juan. El Telégrafo Morse y La Electricidad. La física de los descubrimientos científicos. Propuesta de intervención en Primaria. [en línea]. Valladolid. España. 2015-2016. [Consultado el 20 de octubre de 2021]. Disponible en Internet: https://uvadoc.uva.es/bitstream/handle/10324/20012/TFG-G1993.pdf;jsessionid=3925D65211FA55F9173C7568116CE2D9?sequence=1

[9] NATIONAL GEOGRAPHIC. Historia: Una Invención Conflictiva - Alexander Graham Bell y la polémica del teléfono. [sitio web]. 2020. [Consultado el 20 de octubre de 2021]. Disponible en Internet: https://historia.nationalgeographic.com.es/a/alexander-graham-bell-y-polemica-telefono_15118

[10] GARCIA CAMARGO. Jimmy. La Radio por Dentro y por Fuera. Primera Edición. [en línea]. Ciespal. Agosto de 1980. p. 443. [Consultado el 20 de octubre de 2021]. Disponible en Internet: https://biblio.flacsoandes.edu.ec/libros/digital/53840.pdf

[11] GARCÍA, María y ESTUPIÑÁN, Óscar. Historia y Trasformación de La Televisión de Pago en España. un Recorrido Tecnológico desde el Vídeo Comunitario hasta el Vídeo Online. p. 91-110. [Consultado el 22 de octubre de 2021]. Disponible en Internet: https://www.redalyc.org/articulo.oa?id=525752957006

moderna y el primer dispositivo de almacenamiento electrónico, “el disquete”[12]; para 1969 surge la gran novedad que dio origen a la internet, la ARPANET[13], esta una red de computadores creada por el departamento de seguridad de Estados Unidos con fines militares; con la aparición de internet se abre la puerta a una revolución al sistema de comunicaciones que en su momento existía, esta red internacional permitía mediante protocolos la conexión lógica de redes físicas, dentro de los servicios de internet está la WWW (World Wide Web - red informática mundial) sistema que permite la transmisión y consulta de diferentes tipos de datos utilizando protocolos de transferencia de hipertexto (HTTP), también existen otros servicios como el correo electrónico, la mensajería instantánea y las conversaciones en línea.

Desde entonces al internet ha crecido a pasos agigantados, Rubén Cañedo en su artículo Aproximaciones para una historia de Internet[14], describe como a partir de 1990 surgen las participaciones comerciales en el uso de internet, con ello la vinculación de un sin número de usuarios a hoy en día.

El sistema de comunicación y conexión en red, internet, ha dado paso a la aparición de muchas herramientas digitales que permiten la comunicación inmediata con cualquier persona en el mundo a través de la telefonía IP, el correo electrónico, las redes sociales, la telefonía; si bien todo este auge tecnológico ha traído grandes ventajas para el hombre con lo cual ha podido estar informado en tiempo real con cualquier suceso mundial, acceder a información global para fines educativos, culturales, comerciales, financieros, deportivos, etc.…sin contar con toda la información que a su vez puede ser transmitida y almacenada en la red; también ha conllevado de manera paralela a desarrollarse la contraparte a todos los beneficios que ha traído, hurtos informáticos, accesos no autorizados, publicación de información no veraz, inconvenientes de privacidad.

---

[12] LOPATEGUI. Edgar. Historia de las Computadoras. [en línea]. Guatemala. 28. p.6. [Consultado el 20 de octubre de 2021]. Disponible en Internet: http://biblio3.url.edu.gt/Libros/provinciales/computadoras.pdf

[13] CAÑEDO, Rubén. (2004). Aproximaciones para una historia de Internet. [Consultado el 23 de octubre de 2021]. Disponible en Internet: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000100005&lng=es&tlng=es.

[14] Ibid.

Así como desde sus inicios existieron hombres capaces de transformar la historia con sus invenciones y avances, lo han hecho igualmente para alterar estos sistemas.
La información y los datos se han constituido como uno de los activos más preciados tanto para las personas como para las organizaciones y éste a medida del crecimiento de la tecnología informática ha venido siendo compartido en la red, quedando también expuesto a ser accedida, compartida, modificada y eliminada de manera no autorizada[15].

En la medida que la tecnología ha evolucionado y está siendo cada vez más accesible a las personas también está avanzando la ciberdelincuencia, convirtiéndose según la Interpol en uno de los delitos transnacionales de más rápido crecimiento a los que se enfrentan los países miembros de este organismo[16], los objetivos de ataques están siendo enfocados en las micro, pequeñas y medianas empresas, los ciberdelincuentes han visto en ellas un amplio campo de acción, debido a que muchas de ellas carecen de sistemas seguros que permitan el manejo y gestión adecuado de la seguridad de la información.

La Policía Nacional de Colombia define los delitos informáticos como conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc.…[17], estos ciberdelitos son considerados actos ilícitos cometidos a una persona u organización sin previa autorización y consentimiento cuyo fin es el

[15] BORRERO, Paul. Identificación de Activos de Información, Riesgos y Controles Asociados para La Empresa Estrategias Empresariales de Colombia Bajo la Norma Iso 27001 e ISO 31000. [en línea] Cali-Colombia. 100. [Consultado el 20 de octubre de 2021]. Disponible en Internet: http: https://repository.unad.edu.co/bitstream/handle/10596/35641/pcborreroo.pdf?sequence=3&isAllowed=y
[16] INTERPOL. Estrategia Mundial Contra la Ciberdelincuencia. Resumen. [en línea]. Febrero 2017. Consultado: el 20 de octubre de 2021]. Disponible en Internet: file:///C:/Users/Jose%20ferney/Downloads/Summary_CYBER_Strategy_2017_01_SP%20LR%20(4).pdf
[17] POLICIA NACIONAL DE COLOMBIA. Denunciar delitos informáticos. [sitio web]. Bogotá. [Consultado el 21 de octubre de 2021]. Disponible en Internet: https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

acceso, uso, destrucción de información a través de las TIC.

En Colombia de manera frecuente se presenta esta clase de delitos, según el informe Tendencias del Cibercrimen en Colombia, primer trimestre de 2020 emitido por El Tanque de Análisis y Creatividad de las Tic (Tic-Tac) hubo un incremento del 37% de ciberataques comparado con este mismo periodo en el año 2019, en el aumento de estos índices ha tenido gran incidencia la situación por la que atraviesa actualmente el mundo con la pandemia Covid-19.[18]

Dentro de los delitos con mayor crecimiento el informe señala el phishing con una variación del 240% en el incremento de casos, Violación de datos personales 13.5%, Transferencia No Consentida de Activos 8.2%, a su vez el centro cibernético de la Policía Nacional través del balance cibercrimen 2020 – semana 45, presenta un comparativo periodo 2020 vs periodo covid-19 de la relación y comportamiento en cifras de 9 delitos evaluados en el periodo comprendido entre el 1 enero a 8 de noviembre para los años 2019 y 2020, como se muestra en el siguiente cuadro.

Cuadro 1. Estadística de delitos 2019 – 2020.

PERIODO 2020 Corte del 01 de enero al 08 de noviembre de cada año			**Ley 1273 9 delitos**	**PERIODO COVID** Corte del 25 de marzo al 08 de noviembre de cada año		
No casos 2019	**No casos 2020**	**Variación %**		**No casos 2019**	**No casos 2020**	**Variación %**
3.162	5584	77%	Acceso abusivo a un sistema informático	2.303	4.417	94%

[18] COLOMBIA. CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES-CCIT. Tendencias del Cibercrimen en Colombia (primer trimestre de 2020). [en línea]. Bogotá. Abril 2020. 14. Segunda Edición. [Consultado el 14 de julio de 2021]. Disponible en Internet: https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/

406	1.231	203%	Interceptación de datos informáticos	291	975	235%
2.840	7.001	147%	Violación de datos personales	2.032	5.794	185%
951	4.353	358%	Suplantación de sitios Web	733	3499	377%
107	242	126%	Obstaculización ilegítima de sistema informático o red de telecomunicación	73	204	179%
243	507	109%	Daño informático	1174	403	132%
426	513	20%	Uso de software malicioso	293	399	36%
9.865	13.212	34%	Hurto por Medios Informáticos y Semejantes	7.383	10.208	38%
1405	2.632	87%	Transferencia no consentida de activos	1.018	2.064	103%
19.298	**35.184**	**82%**	Total	**14.231**	**27.734**	**96%**

Fuente: POLICIA NACIONAL DE COLOMBIA. Centro Cibernético Policial. Balance Cibercrimen 2020 – Semana 45. [en línea]. Bogotá. Abril 2020. 2. [Consultado: 14 de julio de 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Los resultados del informe permiten observar el incremento de los delitos cibernéticos durante el tiempo de pandemia, según Jürgen Stock, secretario general de INTERPOL “Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la

inestabilidad de la situación socioeconómica generada por la COVID-19”[19]

En el contexto de la Pandemia Covid-19 el sector económico se ha visto muy afectado, para Colombia de manera específica en las Mipymes, debido a la presencia del primer caso de contagio en marzo 6 de 2020[20] y basados en las recomendaciones de la Organización Mundial de la Salud (OMS)[21] el gobierno determinó una serie de medidas a fin de garantizar la preservación de la vida y el fortalecimiento del sector salud.
Inicialmente se dan medidas de confinamiento obligatorio, restricciones de movilidad, distanciamiento social y también el cierre de empresas, con el objetivo de frenar el contagio y de alguna manera mejorar la infraestructura de atención en salud para el país.

Numerosas empresas debieron parar su operación, el verse afectados en el empleo de muchas personas como también la producción de bienes y servicios, otras tomaron la decisión de hacer uso de las herramientas tecnológicas con el fin de garantizar su continuidad y preservar el bienestar de sus empleados, de mismo modo las personas han visto en la tecnología un aliado que permite la realización de diversos trámites en línea sin salir de casa.
Dentro de las estrategias implementadas por las empresas están el teletrabajo, comercio electrónico, el marketing digital, estas medidas han abierto la posibilidad de mantenerse en el mercado, mediante la oferta de servicios en línea han dado opciones para atraer clientes y ampliar su comercio, han podido garantizar el trabajo a sus empleados a través del desarrollo de éste en sus casas, según Estudio de Penetración

[19] STOCK, Jürgen. Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. [en línea]. Agosto 2020. [Consultado el 14 de julio de 2021]. Disponible en Internet: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19
[20] COLOMBIA. MINISTERIO DE SALUD Y PROTECCION SOCIAL. Boletín de Prensa No 050 de 2020. [en línea]. 2020. [Consultado el 14 de julio de 2021]. Disponible en Internet: https://www.minsalud.gov.co/Paginas/Colombia-confirma-su-primer-caso-de-COVID-19.aspx
[21]ORGANIZACIÓN MUNDIAL DE LA SALUD. Actualización de Estrategia frente a la Covid-19. [en línea]. Ginebra. 2020. [Consultado el 23 de julio de 2021]. Disponible en Internet: https://www.who.int/docs/default-source/coronaviruse/covid-strategy-update-14april2020_es.pdf?sfvrsn=86c0929d_10

y Percepción del Teletrabajo presentado por Iván Durán funcionario del Ministerio de las TIC´S informa que tras la llegada del covid-19 y dadas las restricciones de movilidad, se incrementó la modalidad del teletrabajo en 2020, arrojando que 209.173 empleados se convirtieran en teletrabajadores, presentando un incremento de 71 % comparado con 2018, cuando solo había 122.278.[22]; si bien estas medidas ofrecen ventajas también está la otra parte de la balanza, debido al tiempo de adaptación a la situación actual de pandemia los cambios que realizaron las Mipymes orientados en garantizar sus negocios se dieron sobre la inmediatez, entonces se adaptaron los servicios, equipos y las redes, dejando a un lado la parte más importante sobre la cual se soportan, la seguridad informática.

La Superintendencia de Industria y Comercio (SIC) en su estudio de medidas de seguridad en el tratamiento de datos personales 2020, registra el informe de los datos encontrados en la encuesta realizada a 33.596 empresas, de las cuales el 93.3% (31.333) son privadas y 6.7% (2.263) son públicas, arrojando los siguientes porcentajes de cumplimiento de estas frente a la seguridad de la información.[23]

Cuadro 2. Resultados Estudio de medidas de seguridad en el tratamiento de datos personales 2020

Ítems Evaluados / **Organizaciones evaluadas**	**2019**	**2020**
	32.763	33.596
No tienen una política de protección para acceso remoto a la información personal	88%	72.7%

[22] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Quinto Estudio de Percepción y Penetración en Empresas Colombianas 2020. [en línea]. Bogotá. [Consultado el 23 de octubre de 2021]. Disponible en Internet: https://mintic.gov.co/portal/715/articles-179742_recurso_1.pdf

[23] COLOMBIA. SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. [en línea]. 2020. 41. Consultado: 23 de octubre de 2021]. Disponible en Internet: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

No cuenta con mecanismos de monitoreo de consulta de las bases de datos	84%	69.3%
No ha implementado un procedimiento de auditoría de los sistemas de información	83%	71.3%
No tiene implementado un sistema de gestión de seguridad o un programa integral de gestión de datos	82%	67.5%
No ha implementado medidas especiales para proteger datos sensibles	79%	61.3%
No ha implementado una política de seguridad para el intercambio físico o electrónico de datos	76%	66.1%
No tiene política de auditoría de seguridad de la información	72%	63.6%
No tiene controles de seguridad en la tercerización de servicios para el tratamiento de datos	71%	61%
No implementa medidas apropiadas y efectivas de seguridad	66%	50.7%
No cuenta con herramientas de gestión de datos	63%	49.9%
No tiene políticas y procedimientos de gestión de incidentes de seguridad	62%	52.6%
Promedio de incumplimiento respecto de los ítems evaluados	**75.09%**	**62.36%**

Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [en línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

De acuerdo con los resultados del cuadro anterior, se puede observar que hay un porcentaje alto de incumplimiento de medidas de seguridad por parte de las empresas para el 2020, además es menor en comparación con los resultados 2019, es decir se ha desmejorado.

Entre los valores más altos están y que se evidenció en la tabla anterior, que el 72.7% no tienen establecida una política de protección para acceso remoto a la información personal, el 71.3% No ha implementado un procedimiento de auditoría de los sistemas de información, 69.3% No cuenta con mecanismos de monitoreo de consulta de las

bases de datos, 67.5% No tiene implementado un sistema de gestión de seguridad o un programa integral de gestión de datos[24]; haciendo una relación de los índices de ciberdelitos con el estado de los sistemas de seguridad de las empresas para el 2020 dentro del marco de la pandemia Covid-19, se determina la gran necesidad que estás tienen en la implementación y mejora de sistemas de seguridad que permitan identificar y gestionar sus riesgos de manera eficiente y oportuna, más cuando de manera constante aumentan los servicios digitales y las organizaciones hacen uso de ellos.

El gobierno nacional y las organizaciones que agrupan las Mipymes como las Cámaras de Comercio, realizan programas de promoción y control frente a la ciberseguridad, recientemente el Ministerio de Tecnologías de la Información y las Comunicaciones abrió convocatoria para capacitar en seguridad informática a 540 personas naturales con establecimientos comerciales legalmente constituidos del sector económico privado[25], también cuentan con SofisTICa, programa que se desarrolla en convenio entre el Ministerio de Tecnologías de la Información y las Comunicaciones y Colombia Productiva, entidad adscrita al Ministerio de Comercio, Industria y Turismo, creado como estrategia para elevar la productividad y la sofisticación de Mipymes, grandes empresas, gremios y entidades de sectores tradicionales, por medio de la implementación de soluciones tecnológicas, además de ayudar al mejoramiento de la competitividad de las empresas de Software y TI, y el fortalecimiento del comercio electrónico en Colombia.[26]

Si bien es importante el apoyo que se ofrece a las Mipymes por parte del gobierno y las diferentes organizaciones, las empresas con el fin de implementar las estrategias hacia las cuales son orientados con estos programas de ciberseguridad requieren el disponibilidad y uso de herramientas sencillas y a bajo costo, debido a su estructura

[24] Ibid., p. 2.
[25] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Convocatoria de Habilidades Digitales – Formación en Ciberseguridad. [en línea]. Bogotá. 2021. [[Consultado el 23 de octubre de 2021]. Disponible en Internet: https://talentodigital.mintic.gov.co/734/w3-propertyvalue-179871.html#data=%7B%22filter%22:%22%22,%22page%22:0%7D
[26] COLOMBIA PRODUCTIVA. SofisTICa. [en línea]. Bogotá. [Consultado el 23 de octubre de 2021]. Disponible en Internet: https://www.colombiaproductiva.com/sofistica

financiera estas empresas tienen limitantes en la destinación y uso de recursos para tecnología, motivo por el cual en gran parte carecen de sistemas de seguridad informática.

El mercado de herramientas informáticas y tecnológicas ofrece una gama amplia de sistemas que pueden ser implementados y gestionados por las organizaciones para su ciberseguridad con ello podrán ser más competentes y eficientes en el uso de sus recursos además de ofrecer a sus clientes la seguridad de sus datos, dentro de estas se encuentran los sistemas Open Source, sistemas de código abierto que dan la posibilidad de ajuste de acuerdo con la necesidad del usuario.
Dentro de estas tecnologías las más sobresalientes en la actualidad se encuentran:

- LAMP (Linux, Apache, MySQL, PHP)
- sistema operativo móvil Android
- explorador web Mozilla Firefox
- sistema de control de versiones ampliamente utilizado Git

El software open source ofrece grandes ventajas a las empresas, además de tener la posibilidad de ser ajustado a sus necesidades, pueden tener soporte de diversos sectores y personas debido a que su desarrollo no se encuentra centralizado.

4.2 MARCO CONCEPTUAL

La problemática abordada en el presente documento está enmarcada en las siguientes definiciones.

- Seguridad Informática

La seguridad informática es un grupo de técnicas y buenas prácticas que desarrollan las personas y las organizaciones con el fin de salvaguardar sus sistemas de información tanto físico como digitales bajo los siguientes principios.

- Integridad

Característica de la información que está determinada por la conservación de esta y la protección de accesos no autorizados.

- Confidencialidad

Característica de la información y sus recursos que está determinada por el control de acceso y modificación que puede tener a partir del personal autorizado.

- Disponibilidad

Característica que establece que la información pueda ser accedida en el momento necesario como también su capacidad de recuperación ante un evento adverso.

- Autenticación

Característica que define la veracidad de la información.

- Pentesting

El término pentesting ha sido compuesto por la unión de dos abreviaturas en ingles testing y pentetration, pruebas de penetración, estas pruebas están orientadas en descubrir las vulnerabilidades de un sistema a partir de ataques simulados y autorizados. “Una prueba de penetración o pentest es un ataque simulado y autorizado contra un sistema informático con el objetivo de evaluar la seguridad del sistema. Durante la prueba, se identifican las vulnerabilidades presentes en el sistema y se explotan tal como haría un atacante con fines maliciosos. Esto permite al pentester realizar una evaluación de riesgos en la actividad comercial del cliente basándose en los resultados de la prueba y sugerir un plan de medidas correctivas”[27]

Existen dos clases de pentest o auditorias como también pueden llamarse:

[27] GUILLEN, Jose. Introducción al Pentetesting. 2017. [Consultado el 23 de octubre de 2021]. Disponible en Internet: http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf.

- Internos

Conocidos como auditorias de caja blanca y auditorias de caja gris, se desarrollan al interior de la organización y disponen de la información y acceso a su información.

- Externos

Auditorias de caja negra, las pruebas se realizan de manera externa con ataques por parte del profesional encargado quien identifica a través de estos las vulnerabilidades que hay en la organización objeto de prueba.

- Mipymes

Término que agrupa las micro, pequeñas y medianas empresas, fue definido por decreto 957 del 5 de junio de 2009[28] en medio de la clasificación de las empresas de acuerdo con los ingresos por actividades ordinarias anuales de las empresas, como se relaciona en el cuadro siguiente.

Cuadro 3. Rangos para la Definición del Tamaño Empresarial

Sector	Micro	Pequeña	Mediana
Manufacturero	Inferior o igual a 23.563 UVT.	Superior a 23.563 UVT e inferior o igual a 204.995 UVT.	Superior a 204.995 UVT e inferior o igual a 1’736.565 UVT.
Servicios	Inferior o igual a 32.988 UVT.	Superior a 32.988 UVT e inferior o igual a 131.951 UVT.	Superior a 131.951 UVT e inferior o igual a 483.034 UVT.

28 COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 957 (5, junio de 2019). Por el cual se adiciona el capítulo 13 al Título 1 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único del Sector Comercio, Industria y Turismo y se reglamenta el artículo 2° de la Ley 590 de 2000, modificado por el artículo 43 de la Ley 1450 de 2011. [en línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 2019. nro. 50975. p. 1-7. [Consultado el 16 de julio de 2021]. Disponible en Internet: https://www.mincit.gov.co/normatividad/decretos/2019/decreto-957-por-el-cual-se-adiciona-el-capitulo-13

Comercio	Inferior o igual a 44.769 UVT.	Superior a 44.769 e inferior o igual a 431.196 UVT.	Superior a 431.196 UVT e inferior o igual a 2’160.692 UVT.

Fuente: Ministerio de Comercio, Industria y Turismo. Definición de tamaño empresarial. [en línea]. Disponible en: https://www.mipymes.gov.co/temas-de-interes/definicion-tamano-empresarial-micro-pequena-median

- Delitos Informáticos

Son acciones no consentidas contra cualquier medio físico y/o digital el cual contiene datos que son usados de manera ilegal para beneficio de quien las ejecuta.

Parker define a los delitos informáticos como “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”[29].

En Colombia los delitos informáticos están enmarcados dentro de la Ley 1273 de 2009 – “De la protección de la información y de los datos”.

- Riesgos Informáticos

Es la probabilidad de ocurrencia de un evento dañino en un sistema informático o tecnológico.

La Organización Internacional de Normalización (ISO) los define como: “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños”.

- Amenaza informática

Están determinadas por las acciones delictivas que pueden ocurrir ante la presencia de una vulnerabilidad dentro de un entorno informático ya sea en su estructura física o digital.

[29] PARKER, D.B, Citado por Romeo Casabona Carlos M. Poder Informático y Seguridad Jurídica.

- Vulnerabilidad

Condición de debilidad que tiene un sistema sobre el cual pueden ocurrir eventos que afectan su funcionamiento, las vulnerabilidades al igual que las amenazas se presentan en entornos físicos y digitales, a través de estas se materializan las amenazas.

- Software Open Source

Programas de código abierto, los cuales han sido creados con el objetivo de ser utilizados por cualquier persona u organismo y este pueda utilizarlo y modificarlo de acuerdo con su necesidad, contiene dos características especiales, la primera es que carece de costo y la segunda es que puede ser aplicado en la creación de software nuevo.

4.3 MARCO HISTÓRICO

El desarrollo del presente documento está enmarcado en el origen y desarrollo de la actual Pandemia Covid-19, su origen se presentó en Wuhan (China) el 31 de diciembre de 2019, el primer contagio para Colombia se presentó el 6 de marzo de 2020, desde entonces se han decretado diversos mecanismos de prevención que han afectado de manera significativa la vida de las personas, en su entorno social, laboral, familiar, financiero y personal.

Dentro de las medidas tomadas por las empresas sustentadas en las recomendaciones de organizaciones mundiales de salud como la OMS[30] se ha establecido el distanciamiento social, el uso de mascarilla, el lavado de manos, el aforo máximo de personas en cualquier establecimiento comercial, entre otras. Estas disposiciones llevadas a entornos empresariales han afectado de manera significativa el sector económico. Las empresas ante las consecuencias que ha causado la pandemia y con el fin de restablecer su economía han venido desarrollando estrategias que permitan el

[30] ORGANIZACIÓN MUNDIAL DE LA SALUD. Brote de enfermedad por coronavirus (COVID-19): orientaciones para el público. [Consultado el 16 de julio de 2021]. Disponible en Internet: https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019/advice-for-public

cumplimiento de las normas de salud para preservar la vida de sus empleados, pero también ayuden a su desarrollo financiero; la migración de operaciones y servicios a la red ha sido una ventana que se ha abierto permitiendo el restablecimiento de los sectores.

El uso de la tecnología en las empresas con objetivos comerciales ha venido desarrollándose de manera acelerada en la misma medida que lo ha hecho el internet, el origen del comercio electrónico está alineado sobre el año 1990 con auge del internet[31], desde entonces se han desarrollado diversos sistemas que soportan estas operaciones y que proveen otro tipo de servicios digitales, entonces de manera paralela la tecnología y los servicios a través de la red se han desarrollado, quizá hace algunos años estos servicios estaban limitados por situaciones técnicas, de conocimiento inclusive por falta de recursos, hoy en día con la masificación del uso de los teléfonos celulares y el fácil acceso a dispositivos portátiles son muchas las personas que tienen la posibilidad de interactuar comercialmente a través de la red. Se ha dado tanta transcendencia a todo aquello que se puede hacer para estar conectado y consumir contenido electrónico que la seguridad de todos estos procesos se ha dejado a merced de quienes si saben cómo dar uso de ella.

4.4 ANTECDENTES

Actualmente el mundo se ve enfrentado a una batalla cibernética todos los días, a medida que se contrarresta un ataque cibernético, sale otro con mejores características, con la aparición de la pandemia y el aumento del uso de las herramientas tecnológicas por parte de las empresas se ha puesto al descubierto los bajos niveles de seguridad que tienen.

[31] OCDE. Panorama del comercio electrónico. Políticas, Tendencias y Modelos de Negocio. Publicado originalmente por la OCDE en inglés con el título: Unpacking E-Commerce: Business Models, Trends and Policies. París. 2019. [Consultado el 17 de julio de 2021]. Disponible en Internet: https://www.oecd.org/sti/Panorama-del-comercio-electro%CC%81nico.pdf

Es inútil tener un sistema tecnológico con tantos beneficios si este carece de seguridad o es débil frente a la delincuencia.

Las actividades delictivas cibernéticas han aumentado de manera considerable desde que inicio la pandemia, según el informe de la Interpol del 4 de agosto de 2020[32] "…la ciberdelincuencia ha puesto de manifiesto un cambio sustancial en los objetivos de los ataques, que antes eran particulares y pequeñas empresas y ahora tienden a ser grandes multinacionales, administraciones estatales e infraestructuras esenciales". Dentro de su informe presenta las principales ciberamenazas detectadas a través de la información aportada por los países miembros.

- Phishing 59%
- Malware/Ransomware 36%
- Dominios maliciosos 22%
- Noticias falsas 14%

En Colombia la situación se asemeja a la que vive el resto del mundo, actualmente las personas y empresas están expuestas a diversos ataques, la policía Nacional a través del Centro Cibernético Policial en el balance cibercrimen 2020[33] define las principales modalidades delictivas que actualmente se presentan las cuales han sido reportadas por medio del CAI Virtual:

- Estafa por compra y/o venta de productos
- Phishing
- Suplantación de identidad
- Vishing (Voice phishing)
- Malware
- Amenazas a través de redes sociales

[32] INTERPOL. Aumento alarmante de los ciberataques durante la epidemia de COVID-19. Agosto. 2020. [Consultado el 17 de julio de 2021]. Disponible en Internet: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

[33] COLOMBIA. POLICIA NACIONAL. Centro Cibernético Policial. Balance Cibercrimen 2020. [Consultado el 17 de julio de 2021]. Disponible en Internet: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

- Injuria y/o calumnia a través de redes sociales

4.5 MARCO LEGAL

Las Mipymes en Colombia están siendo afectadas por los ciberdelitos, existe una normatividad legal que regula estos actos, en necesario que las empresas conozcan su alcance como también la aplicación de todas las medidas para salvaguardar los datos de sus clientes y evitar su incumplimiento**.**

- Ley 1273 de 2009[34] (Ley de delitos informáticos)

Mediante esta ley se modifica el código penal colombiano adicionando los siguientes delitos los cuales atentan contra el principio básico de la información, la disponibilidad, integridad y confidencialidad como también los atentados informáticos y otras disposiciones, además se determina el tiempo de la pena de prisión y multas, como se muestra en el cuadro 4.

Cuadro 4. Delitos, penas y multas

Articulo	**Prisión (meses)**	**Multa (smlmv)**
Artículo 269A: Acceso abusivo a un sistema informático.	48 - 96	100 - 1000
Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.		
Artículo 269C: Interceptación de datos informáticos.	36-72 meses	
Artículo 269D: Daño Informático.		
Artículo 269E: Uso de software malicioso.		

[34] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 (5, enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [En línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 2009. nro. 47223. p. 1-4. [Consultado el 17 de julio de 2021]. Disponible en Internet: https://www.mintic.gov.co/portal/inicio/Normatividad/Leyes/

Artículo 269F: Violación de datos personales.	48 - 96	100 - 1000
Artículo 269G: Suplantación de sitios web para capturar datos personales.		
Artículo 269H: Circunstancias de agravación punitiva: (Afectación de sistemas informáticos del estado, oficiales, financieros, delitos cometidos por funcionarios públicos, perjudicando a otros con el delito informático, delitos con fines terroristas, para provecho propio o de terceros)	Las penas impuestas pueden aumentar desde la mitad hasta las ¾ de acuerdo al agravante	
Artículo 269I: Hurto por medios informáticos y semejantes.	6 -14 años	
Artículo 269J: Transferencia no consentida de activos.	48 -120	200 - 1500
Para los últimos dos artículos, si la cuantía supera los 200 smlmv la sanción aumenta la mitad		

Fuente: Ley 1273 de 2009.

- Ley 527 de 1999[35]

Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones

- Ley 1266 de 2008[36]

“La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías

[35] COLOMBIA. SECRETARIA SENADO. Documentos - Estructura Temática. Ley 527 (21, agosto de 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [En línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 1999. nro. 43673. p. 1-9. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

[36] COLOMBIA. SECRETARIA SENADO. Documentos - Estructura Temática. Ley 1266 (31, diciembre de 2008). por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [En línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 2008. nro. 47219. p. 1-16. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países".

- Ley 1581 de 2012[37]

"La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."

[37] COLOMBIA. SECRETARIA SENADO. Documentos - Estructura Temática**.** Ley 1581(17, octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. [En línea]. Santa Fe de Bogotá, D.C.: Diario Oficial. 2012. nro. 48587. p. 1-11. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

5 DESARROLLO DE LOS OBJETIVOS

De acuerdo con el objetivo general el cual tiene como fin analizar los ataques cibernéticos más frecuentes a los que han estado expuestas las Mipymes de Colombia durante el periodo 2020 - 2021 de la Pandemia Covid-19, mediante el análisis de informes técnicos y judiciales para promover su mitigación por medio de uso de herramientas Open Source de fácil acceso, a continuación, se realiza la caracterización de estos y se determinan las causas por las cuales las empresas son vulnerables a estos ataques.

A fin de dar un apoyo al sector de las micro, pequeñas y medianas empresas en Colombia dentro del componente de la seguridad de la información y frente al incremento de los ciberdelitos dentro del marco de la pandemia se proponen las herramientas Open Source de las cuales pueden hacer estas organizaciones y un manual de buenas prácticas para fortalecer sus sistemas de seguridad de la información.

5.1 CARACTERIZACIÓN LOS DELITOS INFORMÁTICOS MÁS RELEVANTES EN COLOMBIA QUE AFECTAN LAS MIPYMES

Según el informe del Balance Cibercrimen 2020 emitido por el Centro Cibernético Policial de la Policía Nacional[38] los delitos más representativos durante el tiempo que ha transcurrido desde que dio inicio la pandemia Covid-19 son los siguientes que se relacionan en el cuadro 5:

[38] POLICIA NACIONAL., Op. cit., p. 1.

Cuadro 5. Tipificación de los Delitos Informáticos

Tipificación de los Delitos Informáticos		
Delito	**Definición**	**Modalidades**
Acceso abusivo a un sistema informático	Acceso no autorizado a cualquier sistema de información por medio de vulnerabilidades presentes.	Ingeniería social, trashing, botnet, Ransomware
Interceptación de datos informáticos	Captura de datos privados sin autorización ya sea en el origen o destino para ser procesados y/o difundidos	Técnica interceptación, Fishing, spyware
Violación de datos personales	Es la destrucción, eliminación, modificación, divulgación de información personal de manera no consentida por sus propietarios	Técnica interceptación, Hoax, Ransomware, spyware
Suplantación de sitios Web	Creación de una versión falsa de un sitio web con el fin de capturar información la cual es utilizada para cometer actos ilícitos,	Fishing
Obstaculización ilegítima de sistema informático o red de telecomunicación	Bloqueo ilegal de un sistema o red informático impidiendo su acceso	Data leakage, Ransomware, botnets
Daño informático	Alteración de la información o dispositivos que la contienen causando su indisponibilidad y uso	Gusanos informáticos, bomba lógica, Fishing, Ransomware, gusanos
Uso de software malicioso	Utilización de programas informáticos creados con fines delictivos para causar daños a los sistemas informáticos, hurto y/o secuestro de información.	Virus, snifer, botnet, Keylogger, spyware, Ransomware, gusanos, troyanos
Hurto por Medios Informáticos y Semejantes	Operaciones bancarias, financieras y comerciales realizadas desde dispositivos electrónicos que son vulneradas generando la exposición de los datos con los cuales se realiza el hurto a las victimas	Skimming, Smishing, técnica del salami, Round Down, Clonación de tarjetas débito y/o crédito, modalidad cambiazo en cajeros automáticos

Transferencia no consentida de activos	Con la manipulación de los sistemas informáticos se realiza la transferencia de activos sin consentimiento de sus propietarios	Ingeniería social, phishing, programa maligno

Fuente: Propia del autor

Con estudios realizados para el primer trimestre 2021 como el programa SAFE-Seguridad aplicada al fortalecimiento de las empresas, denominado “Comportamiento del Cibercrimen en el Contexto de la Reactivación”[39] y el CSOC -Centro de Operaciones de Ciberseguridad de Claro con su informe “La Ciberseguridad, haciendo frente a las Amenazas” dentro del estudio Ciberseguridad en Entornos Cotidianos[40], permite determinar que la tendencia acerca de los ciberdelitos se mantiene frente al mismo periodo del año 2020 y comparado con el 2019 se ha incrementado en un 115%, la siguiente figura muestra el crecimiento porcentual presente a corte del mes de diciembre del año 2020 acerca de los incidentes de seguridad con mayor presencia en Colombia.

Figura 1. Crecimiento de incidentes de seguridad con más presencia en 2020 en Colombia

Fuente: GONZALES, Juan y VARGAS, Cristian. La Ciberseguridad, haciendo frente a las amenazas. Claro. Consultado el 22 de julio de 2021 [imagen]. Disponible en: https://www.ccit.org.co/autor-estudio/tictac/

[39] COLOMBIA. CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES-CCIT. Comportamiento del Cibercrimen en el contexto de la reactivación. [En línea]. 2021. Disponible en Internet: https://www.ccit.org.co/estudios/comportamiento-del-cibercrimen-en-el-contexto-de-la-reactivacion/

[40] COLOMBIA. CAMARA COLOMBIANA DE INFORMATICA Y TELECMUNICACIONES. Tanque de Análisis y Creatividad de las TIC Tanque de Análisis y Creatividad de las TIC. Ciberseguridad en entornos cotidianos. Diciembre 2020. [En línea]. Disponible en Internet: https://www.ccit.org.co/estudios/ciberseguridad-en-entornos-cotidianos-estudio-del-cibercrimen-2020/

El CAI virtual del Centro Cibernético de la Policía Nacional presenta las principales modalidades de delitos cibernéticos como también las ciudades que han presentado mayor afectación, en su informe Balance Cibercrimen 2020[41] los cuales están determinados en las siguientes figuras, en la numero 2 se observan las 7 modalidades de ciberdelitos más sobresalientes para el primer trimestre del año 2020 teniendo en cuenta los incidentes que han sido reportados en el CAI Virtual, sobresalen la estafa por compra y/o venta de productos con 2.391 casos reportaos seguida de la suplantación de identidad con 1.776 casos; en la figura 3 se puede apreciar las 6 ciudades que han presentado mayor afectación, presentando mayor porcentaje Bogotá con 37%, Medellín 10% y Cali 7%.

Figura 2. Principales modalidades de ciberdelitos 1er trimestre 2020

Figura 3. Ciudades de mayor afectación con ciberdelitos

Fuente: El CAI virtual del Centro Cibernético de la Policía Nacional. Informe Balance Cibercrimen 2020. [Imagen]. Disponible en:

[41] COLOMBIA. POLICIA NACIONAL. Op. cit., p. 39.

https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

5.1.1 Acceso abusivo a un sistema informático. Definido en el Artículo 269A de la Ley 1273 de 2009[42], "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes" Este delito se presenta a través de técnicas como el Trashing e ingeniería social, en el primero usa información que ha sido eliminada por los usuarios para buscar datos confidenciales que le sirvan para acceder a los sistemas informáticos, el segundo mediante acciones persuasivas los delincuentes logran acceder a información importante ganando la confianza de las victimas haciendo que estas la suministren.

El informe tendencias Cibercrimen Colombia 2019 – 2020 posiciona este delito en el tercer lugar dentro de los cinco delitos informáticos que afectan a los colombianos con un total de 7994 casos denunciados para el año 2019[43], en este mismo informe se evidencia un porcentaje importante de ataques Ransomware para Colombia del 30% del total de casos presentados en Latinoamérica, siendo las PYMES el principal objetivo, los principales medios de propagación que se han identificado están dados por phishing con correos electrónicos con asuntos "importantes y urgentes" como sanciones, multas, citaciones de entidades estatales con los cual las víctimas se ven motivadas a abrir y ejecutar los correos y documentos adjuntos que contienen malware, de esta manera logran instalarse de manera silenciosa durante un determinado tiempo, con relación al primer trimestre 2021, la Cámara Colombiana de Informática y Telecomunicaciones – a través del TicTac, presenta estudio denominado Comportamiento del Cibercrimen en el Contexto de la Reactivación[44] en el cual se evidencia un incremento del 21% con 5477

[42] COLOMBIA. SECRETARIA SENADO. Ley 527. Op. cit., p. #.41.
[43] COLOMBIA. POLICÍA NACIONAL. Op. cit., p. #17.
[44] CAMARA COLOMBIANA DE INFORMATICA Y TELECMUNICACIONES. Op. cit., p. #45.

casos frente al año 2020. Debido a que en la actualidad se presenta un uso masivo de los teléfonos inteligentes y que son utilizados para almacenar información importante, están siendo objetivo de ataques cibernéticos, después de lograr ingresar al sistema celular por medio de malware, pueden tener acceso a datos privados como cuentas, tarjetas bancarias, claves, entonces esta información es utilizada para realizar otros tipos de delitos cibernéticos.

5.1.2 Interceptación de datos informáticos. El código penal en su Artículo 269C.[45] Interceptación de datos informáticos, lo define, "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

El delito de interceptación datos hoy en día está ligado a todos los medios de comunicación digital como lo son las redes sociales, el teléfono móvil celular, los correos electrónicos como también a los medios de comunicación empresarial, del 100% de incidentes informáticos reportados en Colombia para el año 2019, 14% corresponden al envío de malware, datos reportados en el estudio Tendencias del Cibercrimen 2019-2020[46], 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.

[45]COLOMBIA. SECRETARIA SENADO. Ley 599 (24, julio de 2000). Por la cual se expide el Código Penal. [En línea] Santa Fe de Bogotá, D.C.: Diario Oficial. 2008. nro. 44097. p. 1-64. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

[46] COLOMBIA. POLICÍA NACIONAL. Op. cit., p. #17.

5.1.3 Violación de datos personales. El delito de Violación de datos personales está contenido en la Ley 1273 de2009 en su Artículo 269F[47] sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes,

incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. La legislación colombiana en la Ley 1581 de 2012[48] dicta disposiciones especiales para la protección de datos personales.

Este delito está determinado por las acciones realizadas para acceder a información personal de manera ilícita y esta es usada por un delincuente para obtener beneficio económico, ha sido catalogado por parte de estudio de cibercriminalidad [49]realizado por el TicTac[50] de la CCIT[51] y el CECIP[52] como el segundo delito más denunciado en Colombia con 8037 casos, este índice posiciona al robo de identidad como una de las principales amenazas a las cuales se está expuesto, en reciente informe presentado por el programa SAFE (Seguridad aplicada al fortalecimiento de las empresas) del TicTac de la CCIT en el mes de octubre 2021, se presenta un 67% de incremento de este tipo de ciberataques.[53].

[47] COLOMBIA. CONGRESO DE LA REPUBLICA. Op. cit., p. #40.
[48] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Arquitectura TI. [En línea]. Disponible en https://www.mintic.gov.co/arquitecturati/630/articles-9011_documento.pdf
[49] COLOMBIA. POLICÍA NACIONAL. Op. cit., p. #17.
[50] Tanque de Análisis y Creatividad de las TIC - primer tanque de análisis y creatividad del sector TIC en Colombia, establecido por la CCIT con el fin de proponer iniciativas de política pública orientadas a la transformación digital del país, con base en la sostenibilidad y competitividad económica, la inclusión social, y la eficiencia gubernamental. https://www.ccit.org.co/tictac/
[51] La Cámara Colombiana de Informática y Telecomunicaciones, es la entidad gremial que agrupa a las empresas más importantes del Sector de Telecomunicaciones e Informática en Colombia. https://www.ccit.org.co/la-ccit/
[52] Policía Nacional - Centro Cibernético Policial. https://caivirtual.policia.gov.co/
[53]CAMARA COLOMBIANA DE INFORMATICA Y TELECMUNICACIONES. Op. cit., p. #45.

5.1.4 Suplantación de sitios Web. Artículo 269G.[54] Ley 12173 de 2009.” El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito”.

También conocido como Web Spoofing, consiste en suplantar un sitio web a través del direccionamiento de la víctima hacia sitios web falsos y en ellos obtener su información. El estudio Ciberseguridad en entornos Cotidianos presenta para el año 2020 que la suplantación de sitios web para captura de datos personales tuvo un incremento del 303% comparado con los casos denunciados para el 2019[55].

[54] COLOMBIA. CONGRESO DE LA REPUBLICA. Op. cit., p. #40.
[55] CAMARA COLOMBIANA DE INFORMATICA Y TELECMUNICACIONES. Op. cit., p. #45.

5.1.5 Obstaculización ilegítima de sistema informático o red de telecomunicación. Articulo 269B[56] Ley 12173 de 2009. “El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor”.

Este delito ataca los sistemas informáticos generando indisponibilidad de la información, a partir de este se pueden presentar otros delitos ya que su acción da paso a que los datos afectados pueden ser manipulados.

5.1.6 Daño informático. Articulo 269D Ley 1273 de 2009[57]. Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Este delito también es conocido como sabotaje informático dentro de las consecuencias que estos causan a un sistema informático están la eliminación de información, inaccesibilidad de datos, inclusive a la infraestructura tecnológica que los contiene.

[56] COLOMBIA. CONGRESO DE LA REPUBLICA. Op. cit., p. #40.
[57] Ibíd., p. 1.

5.1.7 Uso de software malicioso. El software malicioso también conocido como malware, su uso está definido dentro la Ley 1273. De 2009 en su Art 269E[58] como "El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes".

La presencia de este delito está determinada por el uso de programas que han sido diseñados para causar daños en los sistemas informáticos, ya sea para hurto o destrucción de la información como también para la propagación de estos. Entre los programas más comunes están: virus informático, gusano informático, troyanos, spyware, ransomware.

Para el año 2019 según cifras del Centro Cibernético de la Policía se incrementó a 612% la presencia de ataques de malware en Colombia siendo las MIPYMES las organizaciones más afectadas, los correos con notificaciones de suplantación de sitios de entidades oficiales 63%, el redireccionamiento a sitios web 32% y la descarga de aplicaciones maliciosas 5%, son los métodos a través de los cuales se ha presentado este delito, información revelada por el mismo ente en su informe Tendencias Cibercrimen 2019-2020[59].

[58] Ibíd., p. 2.
[59] COLOMBIA. POLICÍA NACIONAL. Op. cit., p. #17.

5.1.8 Hurto por Medios Informáticos y Semejantes. Según el Art. 269 i[60] de la Ley 1273 de 2009. Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el art. 240 de este código.

Las actividades relacionadas a este delito se presentan a diario en todo el país, los delincuentes haciendo uso de la ingeniería social logran acceder a sus víctimas y de esta manera persuadirlos para que entreguen información con la que los delincuentes pueden tener acceso a sistemas financieros para cometer hurtos, dentro de estos están la clonación de tarjetas de crédito y débito, el cambio de tarjeta en cajero electrónico.

En lo corrido del 2020 este delito presentó un incremento del 37% con más de 16654 casos reportados [61], las modalidades sobre las cuales se presentaron son a través del hurto de tarjetas bancarias como también el acceso a información relacionada con estos elementos, sus claves, numero de producto, también se presenta el Ransomware como secuestro de la información.

[60] GRISALES, GIOVANNI. Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art. 269i) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009.
[61] CAMARA COLOMBIANA DE INFORMATICA Y TELECMUNICACIONES. Op. cit., p. #45.

5.1.9 Transferencia no consentida de activos. Delimitado en el Art. 269J de la Ley 1273 de 2009[62]. “El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad”.

Este delito utiliza medios informáticos y técnicas como el phishing y el pharming a través de estos los delincuentes logran acceder a información importante por lo general financiera y sin consentimiento de la víctima, durante el periodo pandemia covid-19 comprendido en entre el 25 de marzo y 8 de noviembre ha presentado una variación significativa al aumento con un 103% con 2064 casos, en comparación con los casos denunciados para el mismo periodo 2019 con 1018 casos[63].

5.2 CAUSAS POR LAS CUALES LAS MIPYMES ESTÁN SIENDO VULNERABLES A LOS ATAQUES INFORMÁTICOS E IDENTIFICACION DE VULNERABILIDADES Y AMENAZAS.

Enmarcados en el contexto de la pandemia covid-19 y de la reactivación, luego de ser el año 2020 un periodo de tiempo durante el cual las empresas y la ciudadanía en general experimentaron cambios significativos en su desarrollo económico y comercial es importante mencionar el crecimiento que se ha venido presentando en la ciberdelincuencia y conocer los espacios que estos han encontrado para la materialización de sus delitos. Es claro que el mundo digital avanza de manera

[62] COLOMBIA. CONGRESO DE LA REPUBLICA. Op. cit., p. #40.
[63] COLOMBIA. POLICIA NACIONAL. , Op. cit., p. 40.

acelerada. Día a día se desarrollan nuevos productos, servicios y canales de comercio que requieren una principal atención por parte de los dueños de los procesos y por supuesto de las empresas a fin de proteger sus activos, enfocando una atención importante en la inversión de recursos tendientes a fortalecer sus sistemas de seguridad informática, según el programa SAFE[64] en los tres últimos años en Colombia los ciberdelitos se han consolidado como la modalidad delictiva de mayor crecimiento, con un aumento del 30% en el 2021 en comparación con el año anterior, posicionándose el ransomware como el principal delito que ataca a las empresas; en este mismo estudio realizado por el Tanque de Análisis y creatividad del sector TIC de la Cámara Colombiana de Informática y Telecomunicaciones – TicTac da a conocer que en Colombia se han identificado diez familias de ransomware en casos afectados a empresas, datos que sitúan al país en el puesto 25 a nivel mundial. Desafortunadamente las empresas y organizaciones han cedido espacio frente a esta situación, si bien es cierto que el índice de los ciberdelitos ha venido en aumento en los últimos años, el impacto que trajo consigo la pandemia ha acelerado de manera significativa la presencia de eventos delictivos informáticos, a raíz de los confinamientos como contingencia muchos sectores económicos trasladaron sus áreas de trabajo a los hogares de los trabajadores sin tener la capacidad logística y de seguridad informática requerida. La firma Deloitte en su artículo COVID-19 Ataques cibernéticos ante la oficina remota ¿Cuál será el futuro del trabajo después de esta pandemia?[65], presenta lo que denomina ejemplos de relajación de controles de ciberseguridad entorno al trabajo en casa, poniendo al descubierto errores importantes que tuvieron las empresas al implementar en muchos casos de manera improvisada el teletrabajo, en la siguiente imagen se listan seis aspectos relevantes.

[64] CAMARA COLOMBIANA DE INFORMATICA Y TELECMUNICACIONES. Op. cit., p. #45.
[65] DELOITTE. Artículos. [sitio web]. Abril 2020. [Consultado:11 de abril de 2022]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Cambiando%20la%20forma%20de%20trabajo%20y%20la%20ciberdefensa.pdf

Figura 4. Ejemplos observados de relajación de controles de ciberseguridad.

Fuente: DELOITTE. La Ciberseguridad Ejemplos observados de relajación de controles de ciberseguridad [imagen]. COVID-19 Ataques cibernéticos ante la oficina remota ¿Cuál será el futuro del trabajo después de esta pandemia? Abril 2020. p.9.

Los anteriores ejemplos dejan ver claramente las debilidades en seguridad informática que ocasionaron generando un alto impacto en los sistemas informáticos, el trabajo remoto requirió la demanda de más soporte técnico que quizá las organizaciones no tienen, los equipos desde los cuales se realizaron las conexiones carecen de elementos y software de seguridad que permitan un control y protección de la información, además de los accesos y transferencia de datos sin la respectiva vigilancia.

La delincuencia cibernética es un problema que afecta a todos, ciudadanía, empresas de todos los sectores, organizaciones privadas y del estado; no tienen distinción siempre que se existan las vulnerabilidades sobre las cuales puedan efectuar los

ataques, el informe Tendencias del Cibercrimen 2021-2022[66] muestra como los cibercriminales a través de la suplantación de entidades del gobierno como la Fiscalía General de la Nación, la DIAN, el Ministerio de Salud, la Registraduría Nacional del Estado Civil, el Departamento Administrativo Nacional de Estadísticas – DANE y Policía Nacional haciendo uso del phishing y el smishing logran direccionar a las víctimas a sitios en internet captando datos personales como números de identificación, información financiera, direcciones, números de contacto telefónico, los cuales son usados para hurtos, adquisición de productos financieros, suplantación de identidad, estas modalidades están asociadas a la Violación de Datos Personales, delito con el mayor porcentaje de crecimiento en Colombia, aumentó 45% en el año 2021 frente al 2020, el acceso abusivo a sistemas informáticos, en segundo lugar de crecimiento con un total de 9926 denuncias para el 2021 equivalente a un incremento del 18% respecto al año anterior, seguido del hurto por medios informáticos con 17608 denuncias para el periodo enero – noviembre 2021.

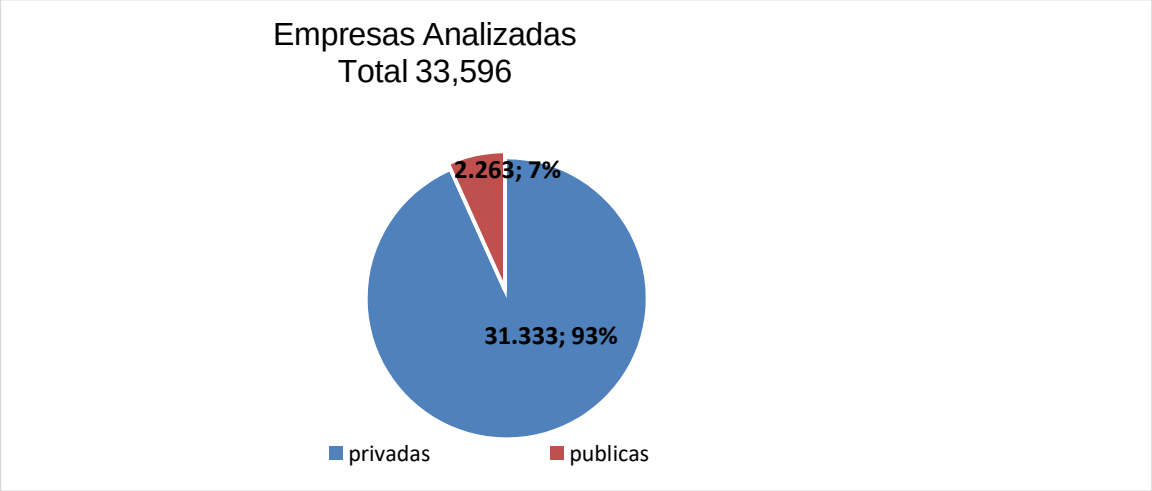
Es importante mencionar que la cantidad de denuncias agrupan la población tanto de ciudadanía como empresarial y organizacional, para un estudio más específico frente a la situación que afecta el sector de las Mipymes, a continuación se con base en el Estudio de Medidas De Seguridad en el Tratamiento de Datos Personales realizado por la Superintendencia de Industria y Comercio[67] se enuncian a continuación las debilidades e incumplimientos que presentan las empresas de Colombia, en cuanto a la seguridad de la información, dando origen a las causas de vulnerabilidad para las Mipymes frente a los diversos ataques cibernéticos que a diario se presentan y que se están especializando, para este estudio se tomó una muestra de 33.596 empresas de

[66] CCIT. Cámara Colombiana de Informática y Telecomunicaciones. Tanque de Análisis y Creatividad de las TIC – Tictac. Tendencias del Cibercrimen 2021-2022 Nuevas Amenazas al Comercio Electrónico. Diciembre 2021. 27. [En línea]. Disponible en Internet: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-2021-2022-nuevas-amenazas-al-comercio-electronico/

[67] COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en Internet: https://www.sic.gov.co/s.ites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

las cuales 31.333 son empresas privadas (93.3%) y 2.263 entidades públicas (6,7%), representados en la siguiente gráfica.

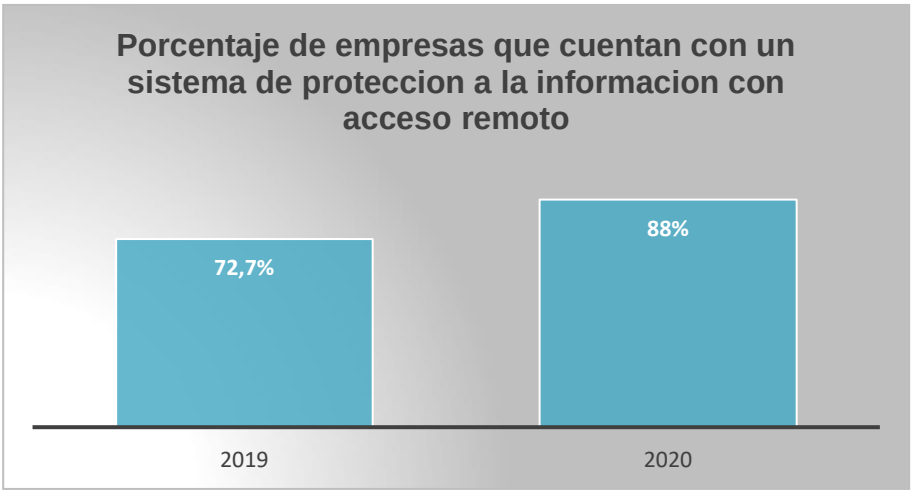
Gráfica 1. Empresas analizadas estudio Superintendencia de Industria y Comercio



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.1 Política de protección para acceso remoto a la información personal. Las empresas no tienen dentro de su sistema de información una política que defina los lineamientos para protección de información personal que es accedida remotamente, en la gráfica relacionada a continuación se puede observar que para el año 2019 el 88% de las empresas no lo tienen, si se hace un comparativo con los datos para el año 2020 se cuenta con el 72.7%, lo que permite afirmar que disminuyó el número de empresas que no cuentan con lineamientos claros y específicos que permitan ofrecer garantías de seguridad en la información personal que es accedida de manera remota por los ciudadanos; sin embargo, el índice sigue siendo alto.

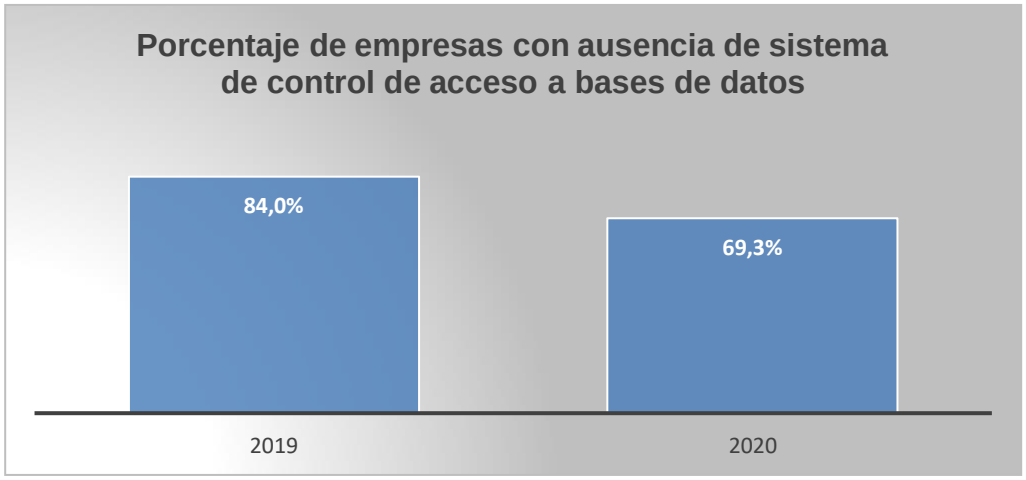
Gráfica 2. Empresas que carecen de una política de protección para acceso remoto a la información personal



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.2 Mecanismos de monitoreo de consulta de las bases de datos. para el 2020 el 69.3% las empresas en su sistema interno no cuentan con mecanismos que permitan realizar un control de consulta a las bases de datos, esto permite que la información pueda estar expuesta a accesos y modificaciones no autorizadas, en comparación con el 2019 que tuvo 84% se puede decir que el índice ha disminuido y que un 14.7%, es decir 4.938 empresas acogieron algún mecanismo de seguridad frente al manejo de sus bases datos, sin embargo el índice de incumplimiento sigue siendo elevado en contraste con el riesgo de exposición, en la siguiente gráfica se puede observar la representación de estos datos.

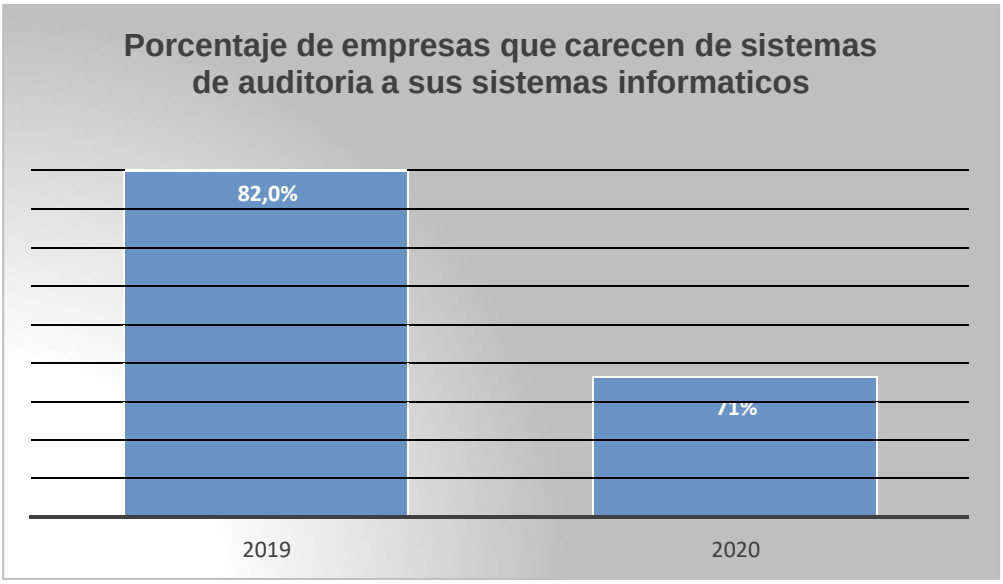
Gráfica 3. Empresas que carecen de un sistema de control de acceso a bases de datos



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.3 Auditoría de los sistemas de información. Para 2020 el 71.3% de las empresas carecen de sistemas de auditorías a sus sistemas informáticos, a raíz de esto no pueden tener una visión clara frente a las vulnerabilidades, amenazas y riesgos que presentan, por consiguiente, se les dificulta emprender acciones correctivas y de mejoramiento, este porcentaje disminuyó frente al de 2019 con un valor de 83%, lo que permite determinar que 3930 empresas representadas por el 11.7%, dieron inicio a la implantación de actividades inspección y verificación con lo cual podrán dar un mejor manejo en la seguridad informática, en la siguiente grafica observa la relación de variación presente para los dos periodos que fueron analizados.

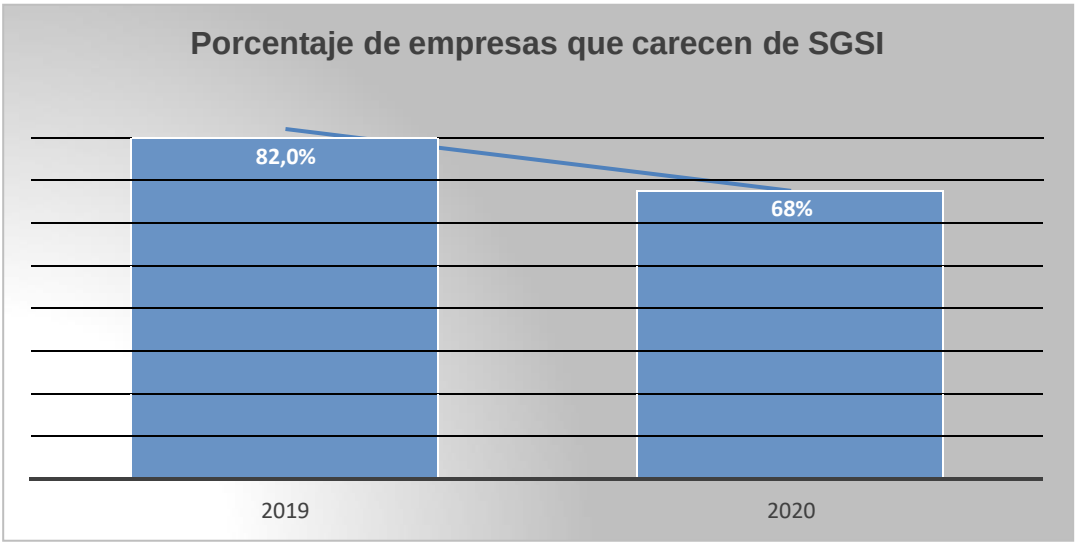
Gráfica 4. Empresas que carecen de sistemas de auditoria informática



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.4 Sistemas de gestión de seguridad o un programa integral de gestión de datos. Para el año 2020 el 67,5% de las empresas analizadas no han implementado un sistema gestión de seguridad de la información que permitan tener control para el cumplimiento normativo, en comparación con los valores encontrados en 2019 con 82%, se puede decir 4871 empresas correspondientes al 14.5% del total de las empresas que hicieron parte del estudio, tomaron la decisión de mejorar la seguridad informática a través de un Sistema de Gestión de la Seguridad de la Información (SGSI), si bien el índice de incumplimiento ha disminuido es muy importante la toma de conciencia y la destinación de recursos por parte de las organizaciones para fortalecer sus sistemas seguridad informática, la siguiente gráfica muestra la tendencia de disminución en el incumplimiento de las empresas.

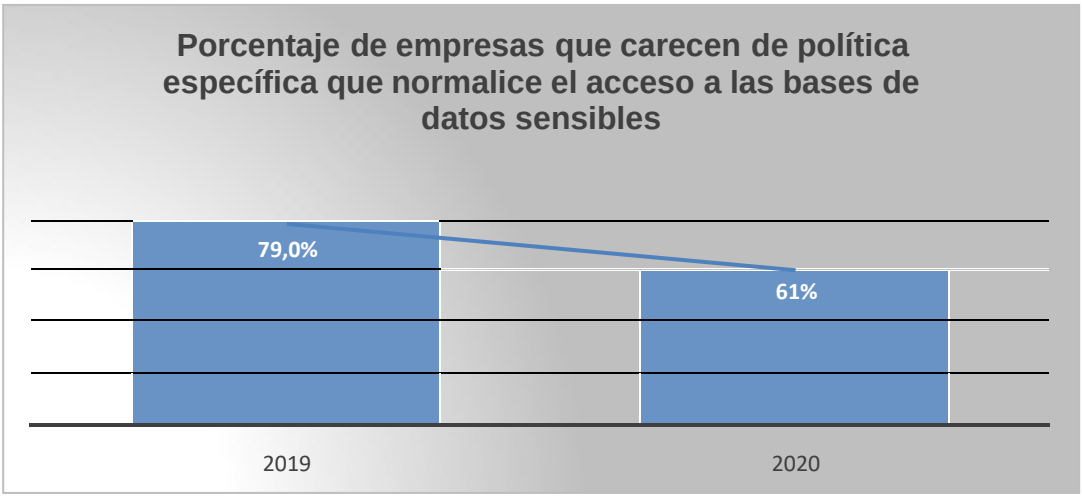
Gráfica 5. Empresas de carecen de Sistema de Gestión de la Seguridad de la Información



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.5 Medidas especiales para proteger datos sensibles. Para el año 2020 el 61,3% de las empresas carecen de una política específica que normalice el acceso a las bases de datos que contienen información personal sensible, valor menor comparado con los resultados obtenidos en el año 2019 con 79%, en un año 5946 empresas tomaron conciencia frente a la importancia del tema y asumieron estrategias de protección de datos personales, estos resultados permiten identificar un mejoramiento ya que son menos las organizaciones que les hace falta la implementación de sistemas de protección a datos sensibles, la relación de estos valores se puede observar en la siguiente gráfica.

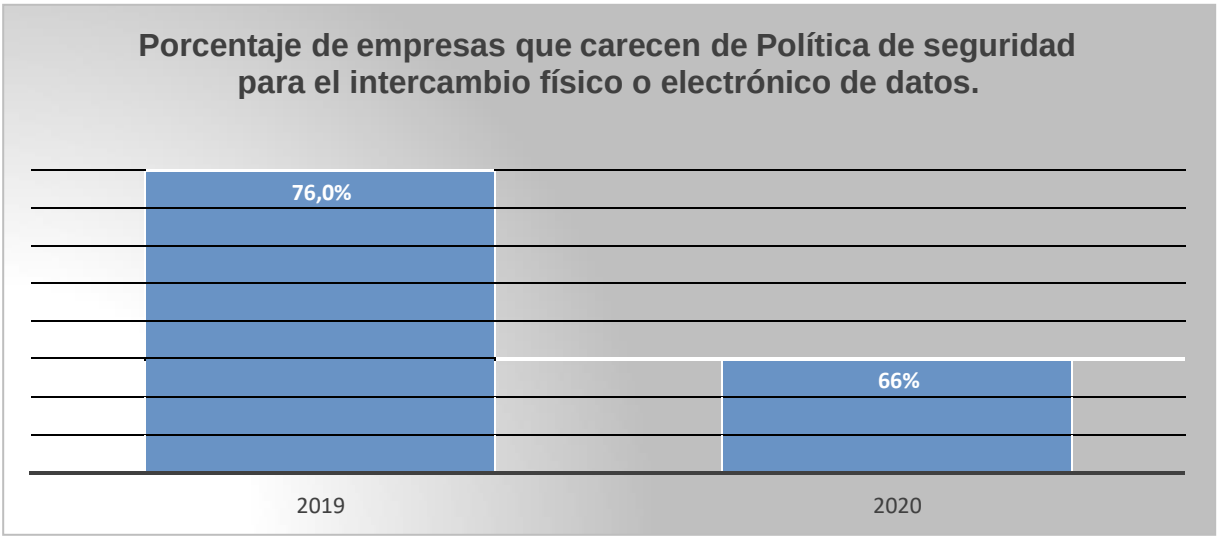
Gráfica 6. Empresas que carecen de política específica que normalice el acceso a las bases de datos sensibles



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.6 Política de seguridad para el intercambio físico o electrónico de datos. Para el año 2020, 22.206 empresas correspondientes al 66.1%, carecen de una Política para garantizar la seguridad en el intercambio de información a través de medios físicos y digitales, actualmente el uso de servicios por medios electrónicos ha aumentado, las compras, el pago de servicios públicos y educativos, registros y tramites , etc. son procesos que implican la transmisión de datos personales, desafortunadamente el estudio de la SIC muestra un elevado índice en las organizaciones frente al incumplimiento de garantías que respalden estos procesos, si bien en comparación con los valores del año 2019 con un 76% el número ha disminuido, es importante que se establezcan controles necesarios a fin de mitigar los riesgos que se pueden presentar, a continuación en la gráfica se pueden observar los porcentajes de incumplimiento.

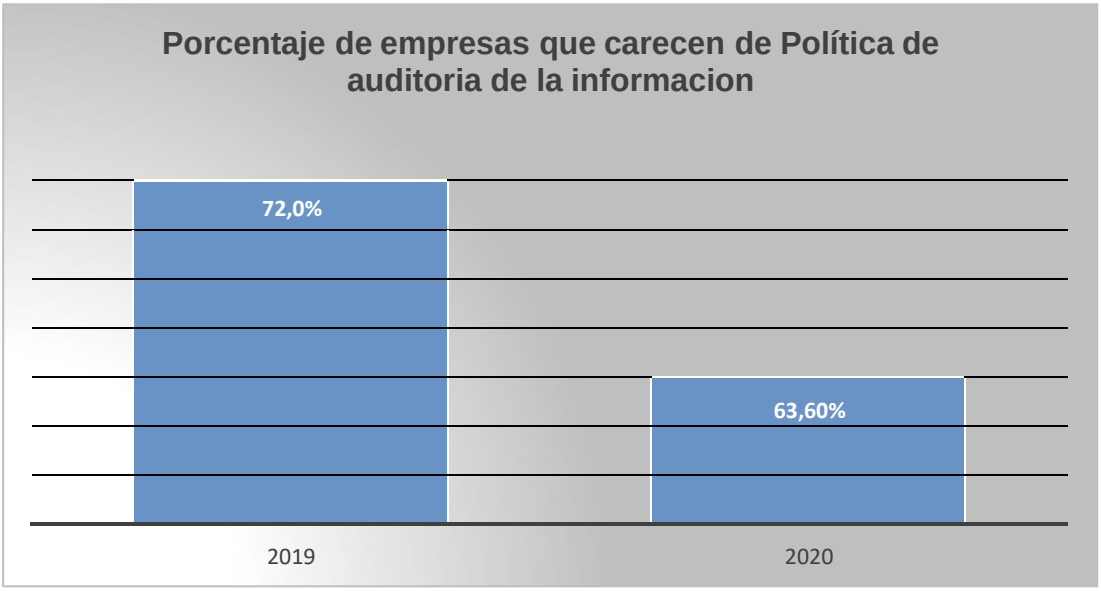
Gráfica 7. Empresas que carecen de Política de Seguridad para intercambio físico o electrónico de datos



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.7 Política de auditoría de seguridad de la información. Las políticas de seguridad de la información son un conjunto de actividades y procesos que de manera organizada y metódica buscan tener un control dentro de una organización con el fin de proteger la información y minimizar sus riesgos, el estudio de la SIC muestra que en el año 2020 el 63.6% de las empresas no cuentan con Políticas de auditoría de seguridad informática, por lo cual se considera que sus sistemas de información se encuentran con alto índice de vulnerabilidad, aunque el porcentaje ha disminuido comparado con los resultados obtenidos por este mismo estudio para el año 2019 con 72%, datos que pueden ser observados en la siguiente gráfica.

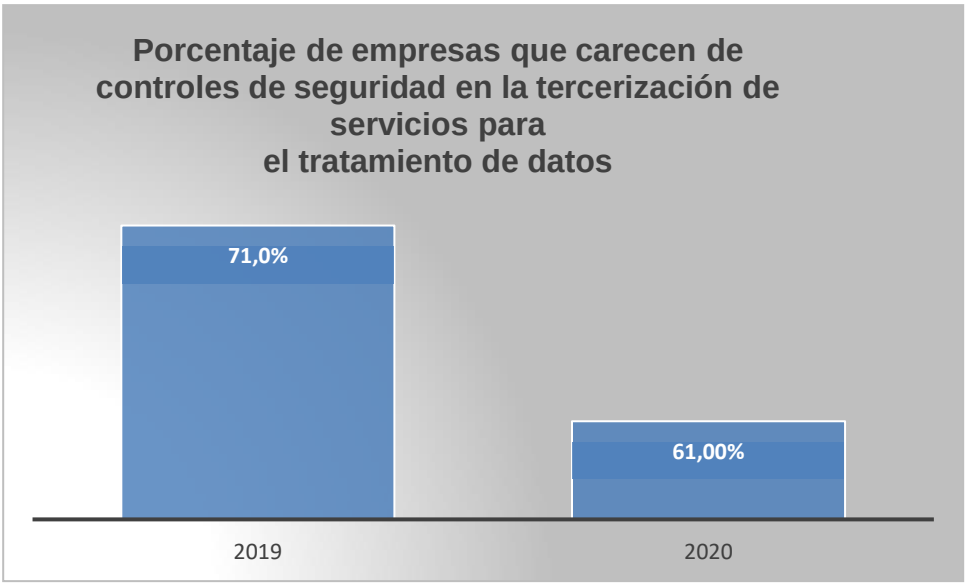
Gráfica 8. Empresas que carecen de Política de auditoría de la información



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.8 Controles de seguridad en la tercerización de servicios para el tratamiento de datos. Las empresas que ofrecen servicios a través de terceros carecen de controles de seguridad para el tratamiento de datos, para el año 2020 el 61% de las empresas analizadas en el estudio, no ejerce ningún control frente a estos servicios, situación que no sólo expone la seguridad de los datos la empresa y de terceros sino también el cumplimento legal frente a ellos, además del aspecto reputacional al que se ven expuestas las organizaciones ante la materialización de amenazas, en la gráfica relacionada a continuación se puede observar la diferencia frente al año 2019, reportado con el 71%, mostrando una mejora del 10%.

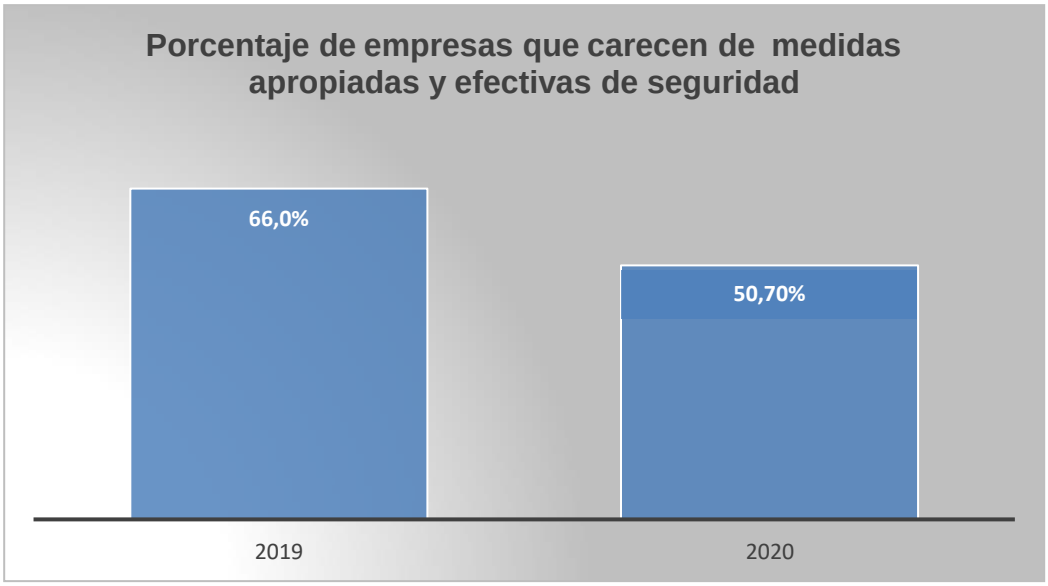
Gráfica 9. Empresas que carecen de controles de seguridad en la tercerización de servicios para el tratamiento de datos



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.9 Medidas apropiadas y efectivas de seguridad. Las medidas se seguridad de información en una empresa están determinadas por el sistema de seguridad que estás manejen, no necesariamente se debe tener un sistema robusto, de acuerdo con la estructura de la organización serán los mecanismos que se implementen, desde lo más sencillo hasta sistemas complejos. El análisis del estudio de la SIC reporta que para el año 2020 el 50.7% de las empresas no cuentan con estas medidas, carecen de medidas mínimas efectivas de seguridad, que respalden la integridad, disponibilidad y confidencialidad de los datos tratados propios y de terceros, si se compara con los resultados del 2019 con un 66% se evidencia que, aunque el valor ha disminuido aún persiste un nivel alto de incumplimiento frente a esta medida, situación que las hace vulnerables a cualquier tipo de ciberataque, la proporción del incumplimiento puede observarse en la gráfica siguiente.

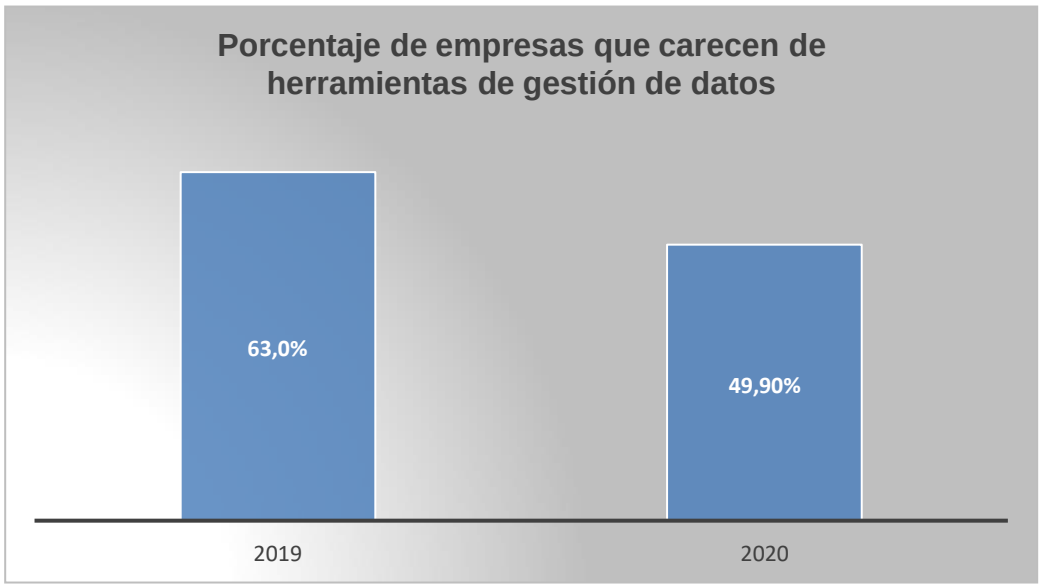
Gráfica 10. Empresas que carecen de medidas apropiadas y efectivas de seguridad



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.10 Herramientas de gestión de datos. Las herramientas de gestión de datos ofrecen un gran aporte a las organizaciones, ya que permiten analizar, almacenar y proteger sus datos a través de plataformas destinadas para tal fin, el estudio de la SIC muestra que las empresas en un 49.9% no cuentan con estas herramientas, lo que genera en ellas disminución en la productividad e ineficiencia en la gestión de su información, respecto a los resultados para el 2019 sobre este mismo ítem, 62%,se observa una disminución considerable que permite inferir sobre la responsabilidad que las empresas están tomando, a continuación se relacionan los valores en la siguiente gráfica.

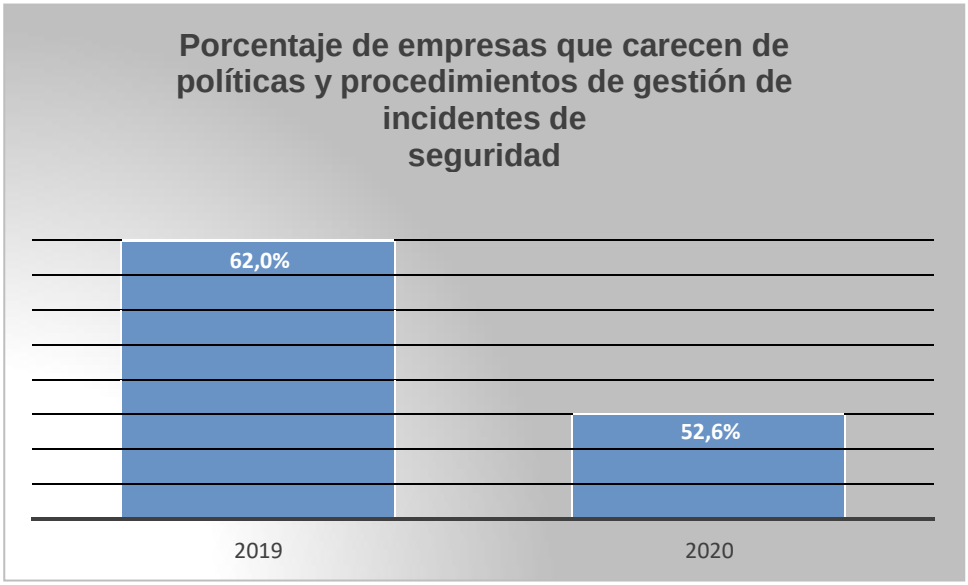
Gráfica 11. Empresas que carecen de herramientas de gestión de datos



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

5.2.11 Políticas y procedimientos de gestión de incidentes de seguridad. La Política de gestión de incidentes tiene como objetivo el establecimiento de los lineamientos para su gestión, dentro de las interrupciones y restauración de los servicios informáticos, para 2020 las empresas tienen un incumplimiento del 52.6%, es decir que menos de la mitad si cumplen frente a este tema, lo que determina la calidad de respuesta ante la presencia de incidentes de seguridad, frente al año anterior con 62% al análisis del actual del estudio se presenta disminución en 10%, considerado un mejoramiento menor en el cumplimiento, es alarmante que más de la mitad de las empresas analizadas carezcan de lineamientos claros que permitan dar un manejo adecuado y una oportuna respuesta a un incidente, a continuación se relacionan los porcentajes encontrados en la siguiente gráfica.

Gráfica 12. Empresas que carecen de políticas y procedimientos de gestión de incidentes de gestión de incidentes de seguridad



Fuente: SIC-Superintendencia de Industria y Comercio. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. 2020. 41. [En línea]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC%20RNBD.pdf

La información aportada en el año 2019 y 2020 por la SIC - Superintendencia de Industria y Comercio de Colombia con relación a la situación que presentan las empresas en seguridad de la información, muestra especialmente que las Mipymes presentan debilidades importantes en la seguridad informática.

A nivel general frente a los incumplimientos descritos hay un 12,73% promedio de aumento de cumplimiento , 2019 con 75.09% y 2020 con 62.36%, sin embargo el índice general sigue siendo alto situación que las está haciendo vulnerables frente a la cantidad de ataques cibernéticos que de manera frecuente se presentan, con ello se están exponiendo no solo a pérdidas económicas, sino también a afectaciones financieras y reputacionales, además de las consecuencias legales que deja la materialización de un evento delictivo sobre bienes cuyos propietarios son terceros. Existe una realidad que se hace necesario confrontar de manera urgente, las Mipymes requieren apoyo constante por parte del gobierno y de las autoridades competentes para fortalecer sus sistemas de gestión de seguridad de la información, para que a través de estos puedan acceder al variado número de herramientas tecnológicas que actualmente están disponibles para su uso.

5.2.12 Vulnerabilidades informáticas y amenazas que afectan las Mipymes.

Como se ha mencionado tras la aparición de la pandemia Covid-19, por parte de las empresas y de la ciudadanía como consumidor, surgió la necesidad de implementar estrategias comerciales que permitieran un sostenimiento de producción, empleo y por su puesto de consumo, convirtiéndose el internet una herramienta y medio esencial dentro de todas las alternativas de oferta y comercio, no solo de productos si no también servicios; al haberse presentado esta circunstancia de manera inesperada y desconocida, pues la población actual no había vivido un pandemia, presentándose como dato de historia la última pandemia de gripe que afectó a Colombia en los años de 1918-1919[68], el incremento del marketing digital se dio en un ambiente en muchos casos improvisado, informal y desafortunadamente inseguro.

De acuerdo con las causas que han sido identificadas y mencionadas anteriormente, sobre las cuales están cimentadas las debilidades que las micro, pequeñas y medianas empresas en el entorno informático, a continuación, se enuncian las principales vulnerabilidades y amenazas que afectan el sector empresarial y que ha tenido un fuerte impacto en la economía del país durante el desarrollo de la actual pandemia covid-19:

- Implementación de servicios digitales sin un manejo adecuado de seguridad.
- Carencia de una política de acceso remoto a la información personal colocando así en alto riesgo la violación a los datos personales.
- Falencia en las estructuras organizacionales, sus funciones y responsabilidades.
- Gestión de recursos errada afectando la disponibilidad de estos por consumos excesivos de los mismos.

[68] MARTÍNEZ MARTÍN, Abel; MELÉNDEZ ÁLVAR, Bernardo; MANRIQUE CORREDOR, Edwar y ROBAYO AVENDAÑO, Omar. Análisis histórico epidemiológico de la pandemia de gripa de 1918-1919 en Boyacá un siglo después. En: Revista Ciencias de la Salud. [en línea]. Universidad del Rosario, 4 de junio de 2019. vol. 17, nro. 2. p. 334-351. [Consultado: 09 de abril de 2022]. Disponible en: https://revistas.urosario.edu.co/index.php/revsalud/article/view/7944

- Sistemas operativos y Aplicaciones como los antivirus desactualizados, con ello se evita la ejecución de parches para el mejoramiento en su funcionamiento y protección.
- Carencia de política de gestión de contraseñas, permitiendo una inadecuada creación y administración de estas por lo tanto se pone en riesgo el acceso a los sistemas de bases de datos, aplicaciones y sistema informático general.
- Falta de implementación de auditorías de los sistemas de información provocando un desconocimiento del estado actual de los procesos, sus fallas y mejoras.
- Operaciones sobre redes inalámbricas abiertas exponiendo información personal en la red sin ningún tipo de protección. obsoleto
- Personal no capacitado, muchos errores se presentan por desconocimiento en procesos de seguridad por parte del talento humano, la falta de capacitación y actualización frente a procesos que a diario están presentando cambios y avances como lo es la tecnología y el manejo de los datos, como también el manejo inseguro de controles de acceso tanto físicos como digitales.
- Conexión a redes abiertas exponiendo los datos de terceros.
- Error en la administración de accesos y permisos tanto lógicos como fiscos, se presentan permisos abiertos sin tener en cuenta el manejo de la confidencialidad de la información, razón por la cual los datos quedan expuestos para ser manipulados, eliminados o robados.
- Errores de configuración de aplicaciones, presentándose errores de formato en cadena, desbordamiento de buffer, condición de carrera; estos afectan el procesamiento de datos.
- Firewall con puertos abiertos permitiendo el acceso a información del sistema operativo, sus aplicaciones y a datos confidenciales.

Las amenazas informáticas son los eventos o acciones potenciales que pueden llegar a presentarse por medio de una vulnerabilidad, en el entorno cibernético las empresas presentan las siguientes amenazas más relevantes, estás fueron tomadas

del estudio Evaluación Retos y Amenazas a la Ciberseguridad[69] y el artículo COVID-19 Ataques cibernéticos ante la oficina remota ¿Cuál será el futuro del trabajo después de esta pandemia?[70]

- El ransomware, malware de rescate o secuestro de datos.
- El malware
- Rootkit
- Fraude Bec (Compromiso de correo comercial empresarial)
- Phishing, vishing, smishing
- Ataques DDos
- Robo de identidad
- Fuga de datos
- Defacement
- Ciber extorciones

[69] CCIT - TANQUE DE ANÁLISIS Y CREATIVIDAD DEL SECTOR TIC EN COLOMBIA. Evaluación Retos y Amenazas a la Ciberseguridad. SAFE- Seguridad Aplicada al Fortalecimiento Empresarial 2021. [Consultado: 14 de abril de 2022]. Disponible en: https://www.ccit.org.co/estudios/informe-evaluacion-retos-y-amenazas-a-la-ciberseguridad/

[70] DELOITTE. Op. cit., p. 56.

5.3 HERRAMIENTAS OPEN SOURCE PARA LA SEGURIDAD INFORMATICA

El término open source o traducido al español como código abierto, está ligado al software open source (oss), cuyo objetivo está en el suministro de código de manera que éste pueda ser modificado y accesible de forma general a quien requiera su uso, su origen se remonta al nacimiento de las comunicaciones por redes sobre los años 1950 y 1960, tiempo en que de manera abierta y colaborativa se desarrollaban los estudios, el resultado de estos eran compartidos y a partir de estos se tomaba como base para otros desarrollos, para 1969 laboratorios bell con ken thompson y dennis ritchie [71] crearon unics hoy conocido como unix, su código fuente creado en lenguaje c, estaba disponible y corría sobre cualquier compilador c, de esta manera teniendo un gran uso a nivel mundial, debido a que su código era compartido sin ningún tipo de soporte técnico quienes lo utilizaban realizaban modificaciones, fue licenciado para usos educativos, comerciales y militares.

UNIX fue asumido por la Universidad de Berkeley, y para 1976 se logra mejorar su kernel bajo el trabajo de los estudiantes Bill Joy y Chuck Haley, dando origen a BSD (Berkeley Software Distribution) un paquete de herramientas y utilidades generando así un gran avance para UNIX, a partir de ese momento se producen diferentes versiones que contienen mejoras, incluida en 1983 la 4.2BSD desarrollada con el apoyo de ARPA (agencia de investigación del Pentágono, y espónsor de ARPANET), la cual integraba el protocolo de comunicación de internet TCP/IP en UNIX, convirtiéndose en el software base de Internet; debido a que su comercialización empezó a ser restringida con fines de comercialización, surge entonces en 1984 y bajo la supervisión de Richard Stallman, la Free Software Foundation (Fundación por el Software Libre) creando GNU, sistema operativo basado en UNIX que buscaba ser de uso y distribución libre, declarado sobre 4 libertades.[72]

---

[71] UOC. Universitat Oberta de Catalunya. El software libre en Catalunya y en España. Historia y desarrollo del software libre y de código fuente.

[72] GNU. El Sistema Operativo GNU. [Sitio Web]. [Consultado: 28 de agosto de 2021]. Disponible en Internet: https://www.gnu.org/home.es.html

- La libertad 0.
  Ejecutar el programa como lo desee, con cualquier propósito.

- La libertad 1.
  Estudiar el funcionamiento del programa y modificarlo de modo que realice las tareas como usted desee.

- La libertad 2.
  Redistribuir copias para ayudar a los demás.

- La libertad 3
  Distribuir copias de sus versiones modificadas a otras personas.

Junto con GNU fue creado también GPL[73] (General Public License) cuyo fin estaba basado en el respaldo frente a la libertad en el uso, copia y modificación de software con miras a garantizar su naturaleza y evitar su apropiación.

Dado los requerimientos necesarios para UNIX y ante la necesidad de adaptación de este a un PC(Computador personal) en 1991 Linus Torvalds[74], ingeniero de software finlandés crea un kernel y lo comparte en internet buscando apoyo en el desarrollo convirtiéndose en un código fuente libre con autorización de modificación, crea Linux, para 1992 entrega su nueva versión soportada como GPL, con base en lo anterior se crea el software libre.

En 1998 ya con la versión Linux 2.0 es propuesto por parte de la organización Linux y miembros de la comunidad libre de programadores como Eric Raymond del movimiento Free Software el término “Open Source”, este nuevo termino agrupaba las características del software libre bajo una licencia sobre la cual se regía su uso

[73] GNU. El Sistema Operativo GNU. Licencias. [Sitio Web]. [Consultado: 30 de septiembre de 2021]. Disponible en Internet: https://www.gnu.org/licenses/licenses.es.html
[74] JORBA. Suppi, JOSEP.Remo. Software Libre. Administración avanzada de GNU/Linux. [En línea]. [Consultado: 30 de septiembre de 2021]. Disponible en Internet: https://libros.metabiblioteca.org/bitstream/001/425/1/871.pdf

modificación y distribución, para este mismo año se fundó Open Source Initiative – OSI[75], organización sin ánimo de lucro cuyo objetivo está basado en el apoyo al desarrollo del código abierto.

Dentro de las principales características del código abierto están:

- Trabajo colaborativo, el código puede ser accedido por gran número de personas en busca de mejorarlo, razón por la cual está en constante cambio y ajuste.

- Código transparente, cada uno puede acceder y verificar la información sin tener limitantes por derechos de propiedad.

- Dado que el código abierto está en constante cambio por las revisiones y ajustes realizadas, ofrece seguridad frente a los procesos de evaluación a los que ha sido sometido.

- A través las organizaciones como OSI que promueven y apoyan el desarrollo open Source, se obtiene ayuda para su implementación de acuerdo con las necesidades de las comunidades y/o organizaciones.

- Ofrece la posibilidad de desarrollo a cero costos, ya que el código es gratuito y no está sujeto al derecho de propiedad, permitiendo así su uso, modificación y distribución a partir de la misma licencia libre.

[75] OSI - Open Source Iniciative. Historia OSI. www.opensource.org

5.3.1 Herramientas Open Source para la seguridad informática en Mipymes.

La seguridad informática en las organizaciones se encuentra enmarcada dentro de la base de la detección y prevención de intrusiones, a continuación, se presentan herramientas Open Source que han sido diseñadas para auditoria y seguridad informática, se han clasificado en cuatro grupos, Análisis DNS, Análisis de Red, Análisis Web y Análisis Forense de acuerdo con sus características para la búsqueda e identificación de vulnerabilidades como también para la valoración de información existente y/o eliminada sobre eventos acontecidos, y teniendo en cuenta las falencias que actualmente presentan las empresas en cuanto a seguridad informática, incidentes que en su gran mayoría se han desarrollado en la red, lo cual se ha anunciado anteriormente y se encuentra documentado en estudios oficiales por parte de entes gubernamentales como la Superintendencia de Industria y Comercio, la Policía Nacional y entidades privadas como la CCIT; debido a que el grupo Mipymes abarca un número de empresas de diferentes tamaños (micro, pequeña y mediana empresa) y de actividades económicas diversas, el uso y la aplicación de las herramientas se presenta de manera distinta, ya que una empresa mediana dentro de su estructura organizacional puede tener de manera específica un área TI con sus respectivos responsables mientras una micro empresa por organigrama y capacidad puede omitir estos roles, razón por la cual la identificación de herramientas se realiza de manera general, es claro que una empresa con una estructura más sólida puede llegar a tener una capacidad más amplia de manejo de los recursos tecnológicos pero el objetivo en común para todas en cuanto a seguridad informática es el mismo, ser competentes y ofrecer seguridad en el manejo de los datos a sus clientes y para sí mismos.

Ahora bien, las herramientas Open Source propuestas tienen una gran ventaja, su costo, además de la posibilidad de acceso y modificación del código de acuerdo a la necesidad específica para su utilización libre, pero es necesario aclarar que para aquellas organizaciones que carecen de personal específico en el manejo y responsables de TI se hace necesario la inversión de servicios profesionales idóneos que garanticen la correcta aplicación para su seguridad informática, otro aspecto importante a tener en cuenta es que estos procesos son continuos y están en constante cambio, es decir que siempre será necesario un manejo dinámico de herramientas a fin de identificar y prevenir la materialización de eventos informáticos delictivos.

5.3.1.1 Análisis DNS. El DNS (Domain name system). Sistema de nombres de dominio. Felipe Alejandro Espinosa es su informe Monitoreo en Tiempo Real de DNS Utilizando Herramientas Open Source, define un DNS como un sistema que permite acceder a los diferentes recursos disponibles en internet a través de la traducción de nombres de dominios a direcciones IP. Estos nombres se dividen de manera jerárquica, leyéndose de derecha a izquierda y separando cada nivel por un punto[76]

Los DNS son vulnerables ante las amenazas que tienen las organizaciones por la carencia de sistemas de seguridad, entre los más sobresalientes están la suplantación de sitios web, la denegación de servicios DDoS, DNS Spoofing.

A continuación, se describen herramientas que han sido diseñadas para apoyar la seguridad.

[76] ESPINOSA, Felipe. Monitoreo en Tiempo Real de DNS Utilizando Herramientas Open Source. [en línea]. Santiago de Chile. 2018. 68. [Consultado: 30 de septiembre de 2021]]. Disponible en Internet: https://repositorio.uchile.cl/bitstream/handle/2250/152424/Monitoreo-en-tiempo-real-de-DNS-utilizando-herramientas-open-source.pdf?sequence=1&isAllowed=y

- Nmap (Network Mapper). Herramienta open Source desarrollada por Gordon Lyon, su función es realizar auditorías de seguridad a través del escaneo de puertos y descubrimiento de hots, para su ejecución utiliza líneas de comandos, también se pude hacer por medio de Zenmap el cual proporciona para Nmap una interfaz gráfica para usuario, es compatible con los SO Windows, Linux y MacOs.

Está clasificada dentro de las aplicaciones de auditoria caja negra, con esta herramienta se puede identificar todas las terminales conectadas a la red analizada como también las configuraciones de estas, entre ellos los sistemas operativos que utilizan, los servicios no utilizados, usuarios, servicios de puertos, direcciones ip.
Utiliza 3 tipos de escaneo, a través de segmentos TCP, datagramas UDP y/o paquetes ICMP, tras su ejecución los puertos encontrados y analizados pueden tener los siguientes estados:

- **Open.** Puerto abierto y disponible, el puerto puede ser utilizado para que sea explorado por el analista de la auditoria.
- **Closed.** Puerto cerrado, no registra aplicaciones activas para el pero es visible para Nmap.
- **Filtered.** Corresponde a los puertos que tienen un filtro determinado por un firewall.
- **Open Filtered.** El puerto puede estar abierto porque no envía señal y filtrado porque no hay respuesta.
- **Closed | Filtered.** El puerto puede estar cerrado o filtrado

- Dnsmap. Herramienta de escaneo de dominios la cual busca subdominios comunes asociados a este, es utilizada en la recopilación de información en los procesos de

pentesting y administración de sitios web, en la página oficial de Kali Linux se enuncian las principales características[77]:

- Obtención de direcciones IP asociadas a los subdominios. En los resultados se puede encontrar dispositivos como cámaras ip que están configuradas mediante servicios de DNS dinámico.

- Obtención de direcciones IP y números de teléfonos asociadas a los subdominios.

- Interrumpir el proceso de fuerza bruta en caso de que el dominio de destino utilice comodines.

- Capacidad de poder ejecutar la herramienta sin proporcionar una lista para realizar un ataque de fuerza bruta.

- Guardar los resultados en un formato legible.

- Dnsnum. Herramienta que enumera la información DNS y descubre los bloques no contiguos, dispone de comandos para realizar consultas de acuerdo con la información.

Las siguientes son las opciones disponibles listadas por Erika Yáñez en su proyecto Análisis de Las Herramientas para el Proceso de Auditoría de Seguridad Informática Utilizando Kali Linux[78].

- Obtener la dirección del host.
- Obtener la dirección de los servidores de nombres.
- Obtener el registro del servidor de correo electrónico.
- Realizar consultas AXFR20 en servidores de nombres y obtener la versión de BIND21 (hilo).

[77] KALI LINUX. Herramientas Kali. [sitio web]. [Consultado: 30 de septiembre de 2021]]. Disponible en Internet: https://www-kali-org.translate.goog/tools/dnsmap/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=nui,sc

[78] YÁNEZ CEDEÑO, Erika. Análisis de Las Herramientas para el Proceso de Auditoría de Seguridad Informática Utilizando Kali Linux. [en línea]. 2015. 113. [Consultado: 30 de septiembre de 2021]]. Disponible en Internet: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf

- Obtener nombres adicionales y subdominios vía Google.
- Ejecuta ataques de fuerza bruta para la resolución de nombres, con la posibilidad de ejecutar ciclos recursivos en subdominios con registros NS(h).
- Calcula los rangos de direcciones de red de dominio de clase C y realiza consultas whois sobre ellos (h).
- Realiza lo que se conoce como Reverse DNS Lookup en rangos de IP (Rangos de direcciones clase C y/o whois) (h).
- Permite escribir los bloques de IP detectados en un archivo llamado domain_ips.txt

5.3.1.2 Análisis de red.

- Wireshark. Herramienta que analiza protocolos de red, en su página web oficial[79] está definido como el analizador más importante y utilizado en el mundo por diversas organizaciones y entidades públicas, privadas, de desarrollo económico, comercial, educativo, entre otras, dentro de sus principales funciones tiene:

  - Inspección de múltiples protocolos.
  - Análisis en línea y fuera de línea.
  - Multiplataforma, ejecución en varios sistemas operativos.
  - Filtros de pantalla potentes.
  - Análisis completo de VoIP.
  - Reconocimiento de muchos formatos de archivo de captura.
  - Descompresión de archivos de captura tipo Zip durante su ejecución.
  - Exportación de información en varios formatos tipo CVS, txt, xml.

[79] WIRESHARK. Sobre Wireshark. [sitio web]. [Consultado: 30 de septiembre de 2021]. Disponible en Internet:https://www-wireshark-org.translate.goog/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=nui,sc

- Dmitry (Deep magic Information Gathering Tool). Herramienta de recopilación de información profunda, tiene como función la captura total de la información de una máquina o equipo, entre ella scanner de puertos, correo electrónico, nombres de dominio, a través de sus diferentes comandos, se encuentran: -e, -n, -s, -o, pueden almacenar la información en modo denso siendo una consulta más rápida o en modo ligero con datos más completos.

5.3.1.3 Análisis Web

- Skipfish. Herramienta de scanner de seguridad para aplicaciones web, en su página oficial Kali Linux la define como una herramienta que prepara un mapa del sitio interactivo para el sitio de destino mediante la realización de un rastreo recursivo y sondeos basados en diccionarios, el mapa resultante se anota con el resultado de una serie de controles de seguridad activo, el informe final generado por la herramienta está destinado a servir como base para evaluaciones profesionales de seguridad de aplicaciones web[80], presenta su informe a través de un archivo HTML permitiendo así una mejor interacción y consulta.

Como características principales, Erika Yáñez Cedeño[81], lista las siguientes.

- Velocidad de Respuesta.
- Fácil Uso: Reconocimiento heurístico le permiten analizar sitios web con tecnología variada, construir automáticamente lista de palabras basadas en análisis de contenido del sitio web.
- Interactivo: Genera un archivo con los resultados en formato HTML que permite desplegar y encoger resultados.

[80] KALI LINUX. Herramientas Kali. [sitio web]. [Consultado: 30 de septiembre de 2021]]. Disponible en Internet:https://www-kali-org.translate.goog/tools/skipfish/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=nui,sc

[81] YÁNEZ CEDEÑO, Erika. Análisis de Las Herramientas para el Proceso de Auditoría de Seguridad Informática Utilizando Kali Linux. [en línea]. 2015. 113. [Consultado: 30 de septiembre de 2021]]. Disponible en Internet: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf

- Permite analizar la seguridad de un sitio web: Capaz de realizar un análisis preciso y coherente de las vulnerabilidades del sitio.
- Usa una lógica de seguridad de primera: Alta calidad, reducida cantidad de falsos positivos, capaz de detectar una serie de defectos sutiles incluyendo ataque a ciegas de vector SQL

- Maltego. Herramienta que reúne información de la web tanto de la infraestructura tecnológica como de las organizaciones y personas, realiza un análisis sobre ella logrando encontrar la relación que puede existir, utiliza técnicas OSINT, denominada según Lisa Institute a la información -o inteligencia- obtenida de fuentes abiertas y que está disponible para cualquier usuario, sin restricciones de ningún tipo[82].

- Piwik: Herramienta cuya función es analizar el comportamiento de visitantes en sitios web, cuenta con una política de privacidad que brinda a las empresas confiabilidad, dentro de la información importante que ofrece esta el tiempo de permanencia en el sitio web, numero de las visitas, como también las keywords por medio de las cuales es accedida.

Dentro de las principales características están[83]:

- Visión en tiempo real de los visitantes de la web.
- Conocimiento del perfil de los visitantes (origen, género, edad, etc). Esto te ayuda a identificar cómo actúan los diferentes perfiles de usuarios.
- Seguimiento de e-commerce analytics (se pueden trackear los pedidos, las compras, los productos o servicios añadidos al carrito, las fichas de producto visitadas, etc.).
- Disposición de una app gratuita para móviles, que sirve para iOS y Android.

[82] LISA INSTITUTE. OSINT (Open Source Intelligence). [sitio web]. [Consultado: 30 de septiembre de 2021]. Disponible en Internet: https://www.lisainstitute.com/blogs/blog/osint-inteligencia-fuentes-abiertas
[83] THE POWER MBA. [sitio web]. [Consultado: 30 de octubre de 2021]]. Disponible en Internet: https://www.thepowermba.com/es/herramientas/mejores-herramientas-de-analitica-web/

Una de sus ventajas frente a otras herramientas es que permite importar los logs generados por el servidor para extraer toda la información relevante para el sitio web.

- OWA (Open Web Analytics): Es un marco de software que se usa para el rastreo y análisis del uso de los sitios web y las aplicaciones, a continuación se relacionan las principales características:[84]
    - Medición mediante JavaScript o cliente PHP.
    - Seguimiento de Visitas, páginas vistas y visitantes.
    - Seguimiento de visitantes únicos, recurrentes y nuevos.
    - Páginas de entrada, salida.
    - Ecommerce.
    - Soporte para dominios ilimitados.
    - Click-Streams,ver el rastro de clicks de cada visita.
    - Click Tracking , seguimiento de clicks.
    - Seguimiento de eventos
    - Seguimiento de usuarios.
    - Posibilidad de crear métricas nuevas métricas calculadas.

5.3.1.4 Análisis Forense

- HashDeep. Conjunto de herramientas para calcular hashsums MD5, SHA1, SHA256, tiger y whirlpool de un número arbitrario de archivos de forma recursiva.[85]

Dentro de sus principales características están la comparación con listas hash conocidos, muestra de coincidencias y no coincidencias con listas, como también hacer hash por partes.

[84] OPEN WEB ANALYTICS. [sitio web]. [Consultado: 30 de octubre de 2021]. Disponible en Internet: https://www-openwebanalytics-com.translate.goog/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=nui,sc

[85] KALI LINUX. Herramientas Kali. [sitio web]. [Consultado: 30 de octubre de 2021]. Disponible en Internet: https://www-kali-org.translate.goog/tools/hashdeep/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=nui,sc

Utiliza los siguientes comandos con funciones específicas[86]:

- md5deep: Calcula y compara resúmenes de mensajes MD5
- sha1deep: Calcular y comparar resúmenes de mensajes SHA-1
- sha256deep: Calcular y comparar resúmenes de mensajes SHA-256
- tigerdeep: Calcular y comparar resúmenes de mensajes de Tiger
- Whirlpool Deep: Calcula y compara resúmenes de mensajes de Whirlpool

- Autopsy: Herramienta de análisis forense no intrusiva, se ejecuta mediante línea de comandos y utiliza una interfaz gráfica para usuario, analiza imágenes de discos, tarjetas de memoria, celulares y demás dispositivos de almacenamiento, en su página oficial The Sleuth Kit, organismo creador de la herramienta, enuncia las siguientes funciones:[87]

- Análisis de la línea de tiempo: muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad.
- Búsqueda de palabras clave: los módulos de búsqueda de índice y extracción de texto le permiten encontrar archivos que mencionan términos específicos y encontrar patrones de expresión regular.
- Artefactos web: extrae la actividad web de los navegadores comunes para ayudar a identificar la actividad del usuario.
- Análisis de registro: utiliza RegRipper para identificar documentos y dispositivos USB a los que se accedió recientemente.
- Análisis de archivos LNK: identifica atajos y documentos a los que se accede
- Análisis de correo electrónico: analiza mensajes en formato MBOX, como Thunderbird.

[86] Ibid.

[87] The Sleuth Kit. Autopsy. [sitio web]. [Consultado: 30 de septiembre de 2021]. Disponible en Internet: https: //www-sleuthkit-org.translate.goog/autopsy/features.php?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=nui,sc

- EXIF: extrae la ubicación geográfica y la información de la cámara de los archivos JPEG.
- Clasificación por tipo de archivo: agrupe los archivos por su tipo para encontrar todas las imágenes o documentos.
- Reproducción de medios: vea videos e imágenes en la aplicación y no requiera un visor externo.
- Visor de miniaturas: muestra imágenes en miniatura para ayudar a ver las imágenes rápidamente.
- Análisis robusto del sistema de archivos: compatibilidad con sistemas de archivos comunes, incluidos NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, Yaffs2 y UFS de The Sleuth Kit.
- Etiquetas: etiquete archivos con nombres de etiqueta arbitrarios, como "marcador" o "sospechoso", y agregue comentarios.
- Extracción de cadenas Unicode: extrae cadenas del espacio no asignado y tipos de archivos desconocidos en muchos idiomas (árabe, chino, japonés, etc.).
- Detección de tipo de archivo basada en firmas y detección de discrepancias de extensión.
- El módulo de archivos interesantes marcará archivos y carpetas según el nombre y la ruta.
- Compatibilidad con Android: extrae datos de SMS, registros de llamadas, contactos, Tango, Palabras con amigos y más.

Es utilizada en casos de análisis forense de robos, suplantaciones de identidad, hurto de datos informáticos, estafas.

- Digital Forensics Framework(DFF): Herramienta basada en Ubuntu, no intrusiva con interfaz de línea de comandos con gráfica de usuario, analiza discos duros, dispositivos móviles y también realiza análisis forense de redes, está disponible para usuarios Linux y Windows también para sistemas operativos software libre y de código abierto como Debían, dentro de sus funciones están la recolocación, preservación y revelación de evidencias.

Entre sus características están la capacidad de preservar la cadena de custodia digital, acceder a los dispositivos locales y remotos, leer formatos de archivo de análisis forense digital estándar, reconstrucción de discos de máquinas virtuales, de forma rápida triage y la búsqueda de (meta) datos.[88]

- Caine Linux (Computer Aided INvestigative Environment): Creado como proyecto digital forense, desarrollado actualmente por Nanni Bassetti, integra varias herramientas entre ellas Grissom Analyzer, Stegdetect, Guymager, SFDumper, Foremost and Scalpel, Automated Image & Restore (AIR), entre otras.
Dentro de sus características están la interoperabilidad, entorno grafico amigable, generación semi-autonatica de informes y reportes.[89]

- Deft (Digital Evidence & Forensic Toolkit): Es una distribución de análisis forense, booteable desde CD, integrada por un amplio número de herramientas forenses, está compuesta por un entorno de análisis forense y otra DART[90].
Es un sistema muy profesional y estable que incluye una excelente detección de hardware y las mejores aplicaciones gratuitas y de código abierto dedicadas a Incident Response, Cyber Intelligence y muchas otras investigaciones y análisis forenses informáticos. DEFT está destinado a ser utilizado por militares, policías, profesionales de seguridad privada, auditores de TI e individuos también. La última versión de DEFT son las versiones 8.2 y DEFT Zero. Si desea realizar una prueba de manejo, puede descargar una copia de la imagen de instalación desde aquí. Para una experiencia

[88] SOFTOWARE. [sitio web]. [Consultado: 30 de octubre de 2021]]. Disponible en Internet: http://es.softoware.org/apps/download-digital-forensics-framework-for-linux.html
[89] CAINE. [sitio web]. [Consultado: 30 de octubre de 2021]]. Disponible en Internet: https://www.caine-live.net/
[90] Dart es un lenguaje de programación open source, relativamente nuevo, que fue desarrollado por Google y que lanzó su primera versión en 2011. Este lenguaje se creó con el objetivo de permitir a los desarrolladores utilizar un lenguaje orientado a objetos y con análisis estático de tipo. Disponible en Internet: https://www.hiberus.com/crecemos-contigo/que-es-el-lenguaje-de-programacion-dart/

completa, opte por DEFT 8.2, ya que el nuevo DEFT Zero viene con solo un puñado de las herramientas del primero.[91]

La efectividad de la seguridad de los sistemas informáticos tiene su base en la menor presencia de eventos adversos y delictivos, por no decir que la nulidad de estos, pero es evidente que hoy en día cualquier sistema informático puede estar expuesto a amenazas por la presencia de vulnerabilidades, es por esto que toda actividad que se pueda realizar con el fin de minimizar esos riesgos aportará de manera significativa en la existencia y productividad de la organización; las acciones que conllevan a conseguir este objetivo están enmarcadas dentro de los planes preventivos, todas aquellas actividades y procesos para lograr identificar y analizar las debilidades en los sistemas informáticos que permiten definir de manera concreta las correcciones y/o adecuaciones requeridas para la reducción de eventos o incidentes informáticos en las empresas. Es así como se considera de gran importancia la utilización y aplicación de herramientas de identificación y análisis de vulnerabilidades; en la actualidad toda empresa está conectada a la red, su uso está ligado al almacenamiento de información como también al comercio de bienes y servicios, y esta misma situación ha provocado que estén más expuestas, entorno a esta realidad y en las herramientas open source caracterizadas, a continuación se describen las ventajas que estás ofrecen al ser implementadas en las organizaciones.

- El mapeo de redes y puertos permite identificar todos los dispositivos que se encuentran conectados a una red como también los servicios que sobre esta se ejecutan, utilizando diversas estructuras de paquetes por medio protocolos de la capa de transporte; esto proporciona información valiosa para realizar control y gestionar la seguridad.
- Las herramientas de análisis de redes aportan información importante sobre el funcionamiento de tráfico de la red y sus protocolos, su análisis permite definir

[91] LINUX-UBUNTU. [sitio web]. [Consultado: 30 de octubre de 2021]]. Disponible en Internet: https://www-linuxandubuntu-com.translate.goog/home/deft-linux-a-linux-distribution-for-computer-forensics?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=nui,sc

los requerimientos como el ancho de banda y determinar o modificar las condiciones de asignación de recursos de acuerdo a la necesidad, también valida la seguridad de transmisión de y entrada de paquetes para identificar si existe vulnerabilidades como virus o programas maliciosos. Los resultados de estos análisis permiten de manera oportuna determinar la necesidad de recursos para su optimización, así como la verificación en tiempo real de todos los dispositivos conectados a ella con lo cual se consigue una rápida detección de amenazas y su oportuna gestión.

- Los scanner de seguridad para aplicaciones web ofrecen grandes beneficios como lo son el análisis de las bases de datos utilizados por los sitios, los scripts, datos almacenados por los usuarios como direcciones de correos y contraseñas, así como también la detección de errores de formato en el código, inclusive puede tener la capacidad para ejecutar el bloqueo de ataques por fuerza bruta dirigidos a las claves, estas aplicaciones cuentan con una amplia capacidad de detección de vulnerabilidades web, tras la ejecución de las herramientas se generan informes de evaluación que contienen datos de seguridad importantes los cuales permiten determinar acciones a emprender sobre posibles fallos con el fin de fortalecer estas características, dentro de este grupo también se encuentran las aplicaciones de rastreo y análisis de comportamiento de sitios web, que para el tema comercial ofrece muchas ventajas ya que entrega datos de seguimiento de visitas, usuarios, tramites o compras, preferencias, etc, con esta información las empresas pueden realizar análisis de mercado para ser más competitivos además de tener ofertas más enfocadas a la necesidad de sus usuarios fortaleciendo su desarrollo económico.
- Tras la presencia de eventos delictivos las herramientas de análisis forense ofrecen beneficios importantes, mediante la agrupación y verificación de datos electrónicos pueden llegar a encontrar pruebas importantes que permitan determinar los responsables como también el modus operandi sobre el cual ha operado un ciberdelincuente, estas aplicaciones ofrecen un amplio campo de acción ya que su ejecución y análisis puede contemplar software, hardware,

redes y seguridad en general del sistema informático, una ventaja que sobre sale es la recuperación de datos, en las empresas estos procesos tienen gran importancia ya que permite tener un control de la información procesada además de la trazabilidad que esta tiene al ser accedida, manipulada o incluso eliminada por parte de un empleado o tercero.

- Es importante mencionar que las herramientas descritas y todas aquellas que existen en el mundo tecnológico son muy importantes y generan gran aporte al desarrollo de todas las actividades no solo comerciales, sino también estudiantiles, administrativas, de investigación, científicas, judiciales, no sin antes interponer estas al componente quizá más importante y sobre el cual gira la razón de ser de cada organización, el capital humano, de manera prioritaria y urgente ésta clara la ventaja y los beneficios que se obtienen al contar con personal capacitado, todas las empresas dentro de sus prioridades y políticas de seguridad informática conviene que contengan capacitación y la actualización de procesos, normatividad y gestión de información al personal a su cargo, debido a la alta permeabilidad la ingeniería social a las empresas, considerada uno de los principales vectores sobre el cual se están presentando la presencia de ciberdelitos.

  La aplicación de herramientas de análisis en los sistemas informáticos sin distinción de tipo de enfoque aplicada a cualquier área permiten a las organizaciones realizar un control preventivo de seguridad, gestionando los riesgos a los que están expuestos y subsanando a tiempo vulnerabilidades, además de la optimización de recursos, con ello se contribuye a la reducción de costos por la materialización de eventos y la disminución de la exposición al riesgo reputacional al tener un adecuado y seguro manejo de datos de terceros, para los casos específicos de las empresas que hacen e-commerce, al mismo tiempo una administración segura de los datos garantiza el cumplimiento normativo legal.

5.3.2 Manual de buenas prácticas para Mipymes

El aumento en el índice del uso de herramientas tecnológicas como método alterno en la comercialización de productos, servicios y teletrabajo ha permitido el desarrollo de actividades delictivas que están afectando a empresas y clientes. En lo que va corrido del tiempo desde que inicio la actual pandemia covid-19, las Mipymes han hecho de internet un aliado estratégico que les ha permitido sostenerse en el desarrollo de sus actividades ante la situación adversa por la que se ha atravesado en lo que tiene que ver con los aislamientos y las restricciones de movilidad surgidos por la pandemia; el comercio electrónico y de servicios ha tomado gran auge, la facilidad de adquirir un artículo, pagar un servicio, asistir al médico, estudiar, hacer trámites en línea sin salir de casa, sin duda alguna estos desarrollos aportan a la vida de cualquier persona y por su puesto del comercio, desafortunadamente el lado oscuro de esta coyuntura electrónica y tecnológica también crece, la delincuencia ahora ha enfocado su actuar en el mundo virtual, y está aprovechando del alto nivel de vulnerabilidad que tienen muchas empresas, de manera errada quizá se ha tenido la concepción de seguridad en las instalaciones físicas, y al incursionar en la virtualidad no se ha contado con las herramientas mínimas para gestionar los riesgos a los que se está expuesto en la red.

Es evidente que las Mipymes en Colombia tienen un alto nivel de incumplimiento de medidas de seguridad informática, esto lo revela la SIC-Superintendencia de Industria y Comercio en su estudio de Medidas de Seguridad en el Tratamiento de Datos Personales para el año 2020, que refleja que para este año el 62.3% de las empresas analizadas no cumplían con medidas de seguridad.

Dado que muchas empresas por su capacidad económica y por su tamaño operativo tienen limitantes económicos que impiden la inversión en la implementación de un sistema de seguridad informática, se considera importante que estas cuenten con herramientas sencillas como lo es un manual de buenas prácticas, que permitan guiar el desarrollo de actividades preventivas tendientes a la protección de la información propia y de terceros, además del cumplimiento legal que deben dar las empresas en la protección de datos personales.

El Anexo 1 presenta un manual de buenas prácticas informáticas que sirve como herramienta a las Mipymes para la gestión de la seguridad de la información.

6 CONCLUSIONES

- Debido al aumento considerable en el uso de medios tecnológicos como herramienta de trabajo y también de comercialización de productos se hace necesario de que las empresas de manera urgente implementen sistemas de seguridad informática que permitan definir políticas claras de manejo y protección de datos, la pandemia Covid-19 ha abierto un espacio importante para que los ciudadanos accedan a servicios virtuales, algunos por el desarrollo de sus labores, por lo cual las organizaciones han expuesto su valioso activo la información a la red, muchas de ellas con sistemas de seguridad informática obsoletos y en el peor de los casos otras sin las medidas de protección mínimas; también la adquisición de productos por este medio ha crecido, pero se vuelve a la misma situación base de vulnerabilidad, los datos con los que están suministrando para adquirirlos están siendo interceptados por los delincuentes quienes están haciendo de esta situación un lucrativo negocio. Como se ha mencionado y con las cifras que se han expresado, el sector de las Mipymes en Colombia está desprotegidas frente al uso de los sistemas informáticos y la protección de datos de sus clientes y usuarios.

- Las Mipymes como eje fundamental de la economía del país requieren apoyo de los entes de estado como también de las organizaciones que los agrupan como las Cámaras de Comercio para orientarlos, guiarlos y darles soporte permanente frente al manejo de su seguridad informática, si bien se hacen estudios con encuestas y se tienen las cifras por parte de los entes policivos, las empresas que se han visto afectadas económicamente por la pandemia Covid-19, ahora están amenazadas a diario por las pérdidas económicas a de las que pueden ser víctimas por ciberdelincuentes además de la violación a los datos propios y de terceros bajo su responsabilidad, como lo es en el comercio electrónico.

- Dado que el sector que está siendo afectado en gran medida por la ciberdelincuencia es el de las Mipymes, debido a que estás en su mayoría carecen

de sistemas de seguridad informática que permitan dar un adecuado manejo y control a estos eventos, en muchos casos por limitantes en los recursos económicos, se presentan un variado número de herramientas de código abierto y que no tienen ningún costo para que implementen medidas básicas de seguridad y logren mitigar los riesgos a los que están expuestos en el desarrollo de sus actividades comerciales y de servicios. Si bien es necesario que estas organizaciones destinen recursos para la gestión de su ciberseguridad la utilización de herramientas open Source ofrecen un alivio económico, al no tener la necesidad de incurrir en costos de licencias de software además de su fácil adaptación de acuerdo con la necesidad de cada una, a su campo de acción y sus vulnerabilidades.

7 RECOMENDACIONES

- A medida que la tecnología avanza y permite interactuar de manera rápida y fácil para el acceso a muchos servicios, es necesario que las empresas destinen recursos para invertir en la seguridad informática, para minimizar costos pueden hacer uso de herramientas open source que el mercado ofrece, pero debido al escaso conocimiento de sus propietarios y empleados acerca del tema inicialmente es necesario el apoyo de un profesional en esta área.

- Las entidades que agrupan las empresas, como las cámaras de comercio y los entes del estado como la Superintendencia de Industria y Comercio ofrecen programas de apoyo y capacitación a los cuales cualquier empresa puede acceder, es importante que las Mipymes en cabeza de sus gerentes y representantes legales ejerzan roles de responsabilidad frente al manejo y tratamiento de datos personales, de esta manera podrán al interior de sus organizaciones tener una visión más clara de los riesgos y vulnerabilidades a los cuales están expuestos

- Las Mipymes de manera urgente deben tener las medidas mínimas de seguridad informática, como la instalación de virus, capacitación a su personal acerca de la modalidad de ingeniería social, realizar copias de seguridad de manera periódica, restricción del uso de dispositivos USB en sus equipos de cómputo para minimizar el riesgo de ataques por malware, restricción de acceso a bases de datos, asignación de perfiles a usuarios como limitantes en el acceso a la información almacenada

8 BIBLIOGRAFÍA

ACURIO DEL PINO, S. Delitos informáticos: Generalidades. [Consultado: 16 de julio de 2021]. Disponible en: http://www. oas.org/jurídico/spanish/cyb_ecu_delitos_inform.pdf. Noviembre 2011

ASOBANCARIA. COLOMBIA DIGITAL. Gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones, Bogotá. Abril 2018. [Consultado: 24 de abril de 2021]. Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

BALUJA GARCÍA, Walter. *et al*. OSSIM, Una alternativa para la integración de la gestión de seguridad en la red. Telemática [en línea]. 2012. [Consultado: 29 septiembre de 2021] Disponible en https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdoj&AN=edsdoj.31d87a75fac8405286713c224584bf54&lang=es&site=eds-live&scope=site

BID y OEA. CIBERSEGURIDAD: Riesgos, Avances y El Camino a Seguir En América Latina y El Caribe. Reporte ciberseguridad 2020. [en línea]. 2020. 204. [Consultado: 14 de julio de 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

BBC NOTICIAS. Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo. [en línea]. 2017. [Consultado: 16 julio de 2021]. Disponible en http://www.bbc.com/mundo/noticias-internacional-40422053

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES-CCIT. Tendencias del Cibercrimen en Colombia; primer trimestre de 2020. [en línea]. [Consultado: 14 de julio de 2021]. Disponible en: https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES - CCIT. Tanque de Análisis y Creatividad del sector TIC en Colombia. Tendencias del Cibercrimen 2021-2022 Nuevas Amenazas al Comercio Electrónico. [en línea]. [Consultado: 13 de abril de 2022]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-2021-2022-nuevas-amenazas-al-comercio-electronico/

CAYÓN, Juan. y GARCÍA, Luis. La importancia del componente educativo en toda estrategia de Ciberseguridad. Estudios en seguridad y defensa. [en línea]. Bogotá. 2014. 10. Volumen 9. [Consultado: 14 de julio de 2021]. Disponible en https://doi.org/10.25062/1900-8325.9

ESPINOSA, Felipe. Monitoreo en Tiempo Real de DNS Utilizando Herramientas Open Source. [en línea]. Santiago de Chile. 2018. 68. [Consultado: 30 de septiembre de 2021]. Disponible en internet: en: https://repositorio.uchile.cl/bitstream/handle/2250/152424/Monitoreo-en-tiempo-real-de-DNS-utilizando-herramientas-open-source.pdf?sequence=1&isAllowed=y

FERNANDEZ, María. Historia y evolución de la comunicación. [blog]. María's Blog. 11 de marzo de 2009. [Consultado: 15 de julio de 2021]. Disponible en https://mariafernandezuc3m.wordpress.com/2009/03/11/historia-y-evolucion-de-la-comunicacion/

GUZMÁN, Clara. Contextualización del cibercrimen en Colombia. Bogotá. 6 de julio de 2009. [Consultado: 16 de julio de 2021]. Disponible en

https://doi.org/10.26620/uniminuto.inventum.4.7.2009.56-62

GRUPO DE RESPUESTA A EMERGENCIAS CIBERNÉTICAS DE COLOMBIA (ColCERT). Alertas de seguridad. [sitio web]. Bogotá. [Consultado: 10 de julio de 2021]. Disponible en: http://www.colcert.gov.co/

KALI LINUX. Herramientas Kali. [sitio web]. [Consultado: 30 de septiembre de 2021]. Disponible en: https://www-kali-org.translate.goog/tools/dnsmap/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=nui,sc

SERRANO GUZMAN. María Fernanda, *et al*. Implementación y mejora de la consola de seguridad informática OSSIM una experiencia de colaboración universidad-empresa. [en línea]. Cali. 2012. 6. [Consultado: 28 de septiembre de 2021] Disponible en: https://educacioneningenieria.org/index.php/edi/article/view/6

MARTÍNEZ, Jhon. BLANCO, Leidy. Recomendaciones de buenas prácticas de ciberseguridad en Pymes para la generación de soluciones de detección de intrusos usando Snort. [en línea]. Bucaramanga. 2020. [Consultado: 28 de septiembre de 2021] Disponible en: http://hdl.handle.net/20.500.12749/13911.

MENESES, Cristián. Delitos Informáticos y nuevas formas de resolución del conflicto penal chileno. [en línea]. Chile. 2001. [Consultado: 10 de julio de 2021]. Disponible en: http://www.delitosinformaticos.com/delitos/penalchileno.shtml

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Sistemas de Gestión de la Seguridad de la Información (SGSI). [en línea]. [Consultado: 20 de junio de 2021]. Disponible en: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Impactos de los incidentes de seguridad digital en Colombia 2017. [en línea]. 2017.

[Consultado: 28 de junio de 2021]. Disponible en: https://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

MINISTERIO DE HACIENDA. MAGERIT v.3. 29/01/2019, de Portal de Administración Electrónica Sitio Libro II. 2012, (consultado el 31 de agosto de 2021) Recuperado de https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

POLICÍA NACIONAL DE LA REPÚBLICA DE COLOMBIA. Informe: Tendencias del Cibercrimen Colombia (2019-2020). [en línea]. 2020. [Consultado: 24 de abril de 2021]. Disponible en https://caivirtual.policia.gov.co/#observatorio

POLICÍA NACIONAL DE LA REPÚBLICA DE COLOMBIA. Informe: Balance Cibercrimen 2020 - Semana 45. [en línea]. 2021. [Consultado:16 de julio de 2021]. Disponible en https://caivirtual.policia.gov.co/contenido/balance-cibercrimen-2020-semana-45

SIC-SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. [en línea]. 2020. 41. [Consultado: 14 de julio de 2021]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC

VANGUARDIA. Hurtos informáticos delincuentes invisibles. [en línea]. 2019. [Consultado: el 2 de febrero de 2021]. Disponible en: https://www.vanguardia.com/colombia/hurtos-informaticos-delincuentes-invisibles-xg1338198

YÁNEZ CEDEÑO, Erika. Análisis de Las Herramientas para el Proceso de Auditoría de

Seguridad Informática Utilizando Kali Linux. [en línea]. 2015. 113. [Consultado: 30 de septiembre de 2021]. Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf

ANEXOS

ANEXO 1. MANUAL DE BUENAS PRACTICAS DE SEGURIDAD INFORMATICA PARA LAS MIPYES EN COLOMBIA

MANUAL DE BUENAS PRACTICAS

Un manual de buenas prácticas es un documento que agrupa una serie de acciones a realizar en una organización con el fin de lograr un objetivo. Dentro del área de la información estos documentos determinan practicas seguras que se realizan y están enfocadas en contribuir con el cumplimiento de la seguridad de la información permitiendo a la persona o empresa que las implemente identificar y conocer las vulnerabilidades presentes y los riesgos a los cuales pueden estar expuestos, con miras a emprender acciones preventivas y de mitigación, además de capacitar a empleados y propietarios el correcto uso de recursos de tecnología.

Objetivos del Manual

- Permitir a las Mipymes identificar sus activos y determinar los riesgos a los cuales están expuestos.
- Identificar los responsables de administración y gestión de cada activo.
- Presentar a los propietarios y empleados prácticas seguras para la gestión de seguridad informática.
- Formar al talento humano en buenas prácticas de seguridad informática.

A continuación, se enuncian las prácticas básicas a implementar por las Mipymes para fortalecer su seguridad informática, las cuales están clasificadas de acuerdo con activos de la información generales que puede tener una empresa teniendo como base los pilares de la seguridad de la información, disponibilidad, confidencialidad e integridad.

La norma ISO 27000:2013 define el activo como aquello que tiene valor dentro de una organización y debe ser protegido, como primera medida se debe realizar la identificación y clasificación de activos, esto permite tener claridad sobre la gestión a realizar sobre cada uno de ellos.

Los tipos de activos a clasificar basados en la metodología Magerit - Metodología de análisis y gestión de riesgos de los Sistemas de Información.

- Datos

  Dentro de estos están las copias de respaldo, Bases de datos con información personal, bases de datos con información de clientes y/o proveedores, contraseñas, control de accesos, datos de configuración.

- Servicios

  Página Web, correo electrónico, servidor,

- Software

  Paquetes ofimáticos, antivirus, sistema operativo, servidor de correo electrónico, aplicaciones de comunicación, licencias de software

- Personal

  Empleados, propietarios, proveedores, clientes

- Soporte

  Memorias USB, discos, dvd, tarjetas de memoria, discos virtuales, material impreso.

- Auxiliar

  Muebles, cuartos de rack, cableado, generadores eléctricos.

- Hardware

Router, Switch, módems, impresoras, firewall, teléfonos, datafonos, scanner, equipos periféricos.

- Comunicaciones

Red inalámbrica, red telefónica fija, red telefónica celular, red local, internet.

Toda organización

La gestión de seguridad para estos activos está determinada por la implementación de buenas prácticas, estás se clasifican en obligatorias o recomendables, además de la asignación responsabilidades al personal involucrado.

Cuadro 1. Listado de Activos y buenas prácticas para la seguridad informática.

ACTIVOS		**BUENAS PRACTICAS**
DATOS	Copias de respaldo	- Realización de copias de seguridad de manera periódica (mensual) y su almacenamiento seguro. - Clasificación de la información de acuerdo a su nivel de confidencialidad. - Utilización de contraseñas seguras, combinación alfanumérica y con caracteres especiales. - Evitar crear contraseñas con información personal, como fechas especiales, números de contacto, números de identificación. - Utilizar contraseñas diferentes para cada
	Bases de datos	
	Contraseñas	
	Control de acceso	

	Datos de Configuración	aplicación. - Control en los privilegios de administrador - Cifrado de información transmitida
SERVICIOS	Página Web	- Acceso a páginas seguras. -Utilización de contraseñas seguras, combinación alfanumérica y con caracteres especiales. - Confirmación de remitentes de correos electrónicos.
	Correo electrónico	- Verificación y depuración de la carpeta spam en correo electrónico. - Evite ejecutar y abrir archivos adjuntos de correos sospechosos y/o desconocidos. -Evite acceder a sitios web direccionados a través de correos desconocidos o sospechosos. - Acceso sólo a través de equipos empresariales

	Servidor	y/o personales autorizados. - Uso del protocolo HTTPS para navegar No inicie sesión en computadoras públicas. -Evitar la divulgación y propagación de información no veraz.
SOFTWARE	Paquetes ofimáticos Antivirus Sistema Operativo Servidor de Correo Electrónico Aplicaciones de Comunicación Licencias de Software	- Uso de software licenciado y/o open source - Actualización periódica del antivirus, y del sistema operativo. - Realizar Copias de seguridad periódica. - Interactúe en la red solo con personal conocido y autorizado.
PERSONAL	Empleados Propietarios	- Capacitación frecuente los empleados para explicar las modalidades de hurto electrónico y los riesgos a los que se está expuesto frente a un ciberdelito. - Evitar establecer comunicación física y/o virtual con personas desconocidas que requieran datos personales o información de la empresa - No divulgue información de la empresa a terceros

	Proveedores	- La empresa debe tener una Política de control de accesos, que determine limitantes por roles de acuerdo con la necesidad. - Documentación de procesos catalogados por áreas, todos los procesos de la empresa deben estar clasificados y determinados los dueños de cada uno con los respectivos roles.
	Clientes	
SOPORTE	Memorias USB Discos, Dvd, Tarjetas de Memoria Discos Virtuales Material Impreso	- Configuración y bloqueo de terminales para uso de dispositivos de almacenamiento portátil como USB - Custodia del dispositivo de almacenamiento en espacios seguros. - Control de accesos a dispositivos de acuerdo con los roles autorizados -Realización periódica de mantenimientos
AUXILIAR	Cuartos De Rack	- Los archivadores deben tener cerraduras seguras que dificulten el acceso no autorizado. - Las llaves del cuarto del rack deben ser asignadas a la persona autorizada bajo el respectivo soporte
	Cableado	
	Archivadores	
	Generadores Eléctricos	
	Router	- Mantenimiento periódico de equipos - Configuración de equipos - Establecimiento de control de acceso a impresoras, scanner, servidor.
	Switch	
	Módems	
	Firewall	

HARDWARE	Equipos Periféricos	
	Scanner	
	Impresoras	
	Teléfonos	
	Datafonos	
	Equipos de Computo	
COMUNICACIONES	Red Inalámbrica	- Mantenimiento periódico de redes - Segregación de redes - Definición de controles de acceso por roles - Instalación de software autorizado legal
	Red Telefónica Fija	
	Red Telefónica Celular	
	Red Local	
	Internet	

Fuente: Propia del autor

El talento humano en una empresa se convierte en un activo fundamental, por lo que es importante la correcta asignación de responsabilidades y establecimiento de controles, los roles de funcionamiento por lo cual deben ser configurados a fin de que se garantice el acceso a los datos sólo por personal autorizado, dentro de la contratación de personal las empresas pueden determinar cláusulas de cumplimiento frente a la privacidad, confidencialidad de la información.

Es de destacar, el establecimiento de Políticas de Seguridad de la Información en la cual contemple los procesos, procedimientos y medios de protección de datos de clientes dando cumplimiento a la normatividad legal vigente establecida en la Ley 1266 de 2008[92], dentro de ellos el conocimiento a terceros y solicitud de autorización para el manejo de los datos por estos suministrados y tratados dentro del comercio electrónico.

[92] Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.”

CONCLUSIONES

La implementación de prácticas seguras permite un adecuado manejo de la información en una organización, con ello se ofrecen a los usuarios y clientes la seguridad en el tratamiento de sus datos personales, logrando cumplir con la normatividad vigente que hay en Colombia.

Existen medidas básicas de prevención y a bajo costo, inclusive sin costo, a ser implementadas por las organizaciones, su personal, como también la ciudadanía en general, quienes actúan como usuarios y consumidores del comercio electrónico, dichas medidas mitigan los efectos adversos a los que pueden verse expuestas las empresas ante situaciones de ciberdelincuencia.

Los procesos de scanner de vulnerabilidades se convierten en un insumo valiosos para las empresas en los procesos de gestión de seguridad informática, conocer los riesgos a los cuales están expuestos les permite dar un adecuado manejo y por ende una afectación menor.

ANEXO 2. RESUMEN ANALITICO ESPECIALIZADO

Fecha de Realización:	25/11/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Investigación Gestión de Sistemas
Título:	Ataques Cibernéticos más Frecuentes en Las Mipymes de Colombia Durante El Periodo 2020 - 2021 de La Pandemia Covid-19
Autor(es):	Derly Paulina Martínez Vargas
Palabras Claves:	Amenazas informáticas, Ataques Informáticos, Mipymes, normatividad, Open Source, seguridad informática, vulnerabilidad.
Descripción: (250 palabras)	El desarrollo de este proyecto busca identificar los ataques informáticos que están afectando las Micro, pequeñas y medias empresas en Colombia dentro del marco de la actual pandemia Covid-19 la cual inició en el país en el mes de marzo del año 2020, se tomará como principal insumo los informes presentados por organismos judiciales quienes de manera conjunta trabajan con entes no gubernamentales cuyo objetivo está en la promoción y fomento de acciones tendientes a la seguridad informática de las organizaciones, con base en los datos aportados los cuales tienen su origen en las denuncias realizadas por las víctimas sobre casos reales se pueden establecer los niveles de aumento de estas modalidades delictivas, el tipo de organizaciones sobre las cuales se están presentando y las causas de vulnerabilidad existentes por medio de las cuales se están materializando los eventos delictivos. Con el fin de proponer un aporte a la solución de la problemática antes mencionada se realiza la presentación y caracterización de herramientas Open Source a las cuales pueden acceder las organizaciones para ser implementadas buscando generar un esquema de seguridad informática integral que permita mitigar la presencia de los ciberataques.
Fuentes bibliográficas destacadas: ASOBANCARIA. COLOMBIA DIGITAL. Gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones, Bogotá. Abril 2018. [Consultado: 24 de abril de 2021]. Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf	

BID y OEA. CIBERSEGURIDAD: Riesgos, Avances y El Camino a Seguir En América Latina y El Caribe. Reporte ciberseguridad 2020. [en línea]. 2020. 204. [Consultado: 14 de julio de 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

BBC NOTICIAS. Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo. [en línea]. 2017. [Consultado: 16 julio de 2021]. Disponible en http://www.bbc.com/mundo/noticias-internacional-40422053

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES-CCIT. Tendencias del Cibercrimen en Colombia; primer trimestre de 2020. [en línea]. [Consultado: 14 de julio de 2021]. Disponible en: https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/

CAYÓN, Juan. y GARCÍA, Luis. La importancia del componente educativo en toda estrategia de Ciberseguridad. Estudios en seguridad y defensa. [en línea]. Bogotá. 2014. 10. Volumen 9. [Consultado: 14 de julio de 2021]. Disponible en https://doi.org/10.25062/1900-8325.9

ESPINOSA, Felipe. Monitoreo en Tiempo Real de DNS Utilizando Herramientas Open Source. [en línea]. Santiago de Chile. 2018. 68. [Consultado: 30 de septiembre de 2021]. Disponible en internet: en: https://repositorio.uchile.cl/bitstream/handle/2250/152424/Monitoreo-en-tiempo-real-de-DNS-utilizando-herramientas-open-source.pdf?sequence=1&isAllowed=y

GUZMÁN, Clara. Contextualización del cibercrimen en Colombia. Bogotá. 6 de julio de 2009. [Consultado: 16 de julio de 2021]. Disponible en https://doi.org/10.26620/uniminuto.inventum.4.7.2009.56-62

GRUPO DE RESPUESTA A EMERGENCIAS CIBERNÉTICAS DE COLOMBIA (ColCERT). Alertas de seguridad. [sitio web]. Bogotá. [Consultado: 10 de julio de 2021]. Disponible en: http://www.colcert.gov.co/

KALI LINUX. Herramientas Kali. [sitio web]. [Consultado: 30 de septiembre de 2021]. Disponible en: https://www-kali-org.translate.goog/tools/dnsmap/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=nui,sc

Martínez, Jhon. Blanco, Leidy. Recomendaciones de buenas prácticas de ciberseguridad en Pymes para la generación de soluciones de detección de intrusos usando Snort. [en línea]. Bucaramanga. 2020. [Consultado: 28 de septiembre de 2021] Disponible en: http://hdl.handle.net/20.500.12749/13911.

MENESES, Crisitan. Delitos Informáticos y nuevas formas de resolución del conflicto penal chileno. [en línea]. Chile. 2001. [Consultado: 10 de julio de 2021]. Disponible en: http://www.delitosinformaticos.com/delitos/penalchileno.shtml

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Sistemas de Gestión de la Seguridad de la Información (SGSI). [en línea]. [Consultado: 20 de junio de 2021]. Disponible en: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Impactos de los incidentes de seguridad digital en Colombia 2017. [en línea]. 2017. [Consultado: 28 de junio de 2021]. Disponible en: https://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

POLICÍA NACIONAL DE LA REPÚBLICA DE COLOMBIA. Informe: Tendencias del Cibercrimen Colombia (2019-2020). [en línea]. 2020. [Consultado: 24 de abril de 2021]. Disponible en https://caivirtual.policia.gov.co/#observatorio

POLICÍA NACIONAL DE LA REPÚBLICA DE COLOMBIA. Informe: Balance Cibercrimen 2020 - Semana 45. [en línea]. 2021. [Consultado:16 de julio de 2021]. Disponible en https://caivirtual.policia.gov.co/contenido/balance-cibercrimen-2020-semana-45

SERRANO GUZMAN. María Fernanda, et al. Implementación y mejora de la consola de seguridad informática OSSIM una experiencia de colaboración universidad-empresa. [en línea]. Cali. 2012. 6. [Consultado: 28 de septiembre de 2021] Disponible en: https://educacioneningenieria.org/index.php/edi/article/view/6

SIC-SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales. [en línea]. 2020. 41. [Consultado: 14 de julio de 2021]. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estudio%20de%20seguridad%202020%20SIC

VANGUARDIA. Hurtos informáticos delincuentes invisibles. [en línea]. 2019. [Consultado: el 2 de febrero de 2021]. Disponible en: https://www.vanguardia.com/colombia/hurtos-informaticos-delincuentes-invisibles-xg1338198

YÁNEZ CEDEÑO, Ericka. Análisis de Las Herramientas para el Proceso de Auditoría de Seguridad Informática Utilizando Kali Linux. [en línea]. 2015. 113. [Consultado: 30 de septiembre de 2021]. Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf

Contenido del documento:	El estudio de los delitos cibernéticos en Colombia durante la Pandemia Covid-19, parte de la revisión de informes técnicos y judiciales de organismos como la Policía Nacional de Colombia a través del Centro Cibernético Policial y la SIJIN, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT, la Cámara Colombiana de Informática y Telecomunicaciones – CCIT con los cuales se logra identificar los diferentes ataques a los que están siendo expuestas las Mipymes en Colombia y que se han intensificado durante el periodo 2020 – 2021 de la Pandemia Covid-19 a raíz del aumento en el uso de las tecnologías informáticas por parte de las empresas para desarrollar sus actividades comerciales y de servicios ante los confinamientos preventivos, la limitante en la movilización de la población y el traslado del trabajo a casa, establecidos como medida preventiva para la prevención y disminución del contagio. Ante la realidad que muestran los índices de ataques cibernéticos a las Mipymes se busca determinar las causas por las cuales estas organizaciones están siendo vulnerables, como base se toma el estudio realizado por la Superintendencia de Industria y Comercio en el año 2020 denominado “Estudio de Medidas de Seguridad en el Tratamiento de Datos Personales” además de los informes judiciales y policiales. Como medida de mitigación ante la problemática que enfrentan las empresas ante la presencia de los delitos cibernéticos, se propone el uso de herramientas open source, de las cuales pueden hacer uso para la implementación, gestión, seguimiento y mejora continua de sistemas de seguridad informática, proporcionando espacios físicos y virtuales más seguros que permitan mejorar su desarrollo comercial, establecer ambientes de confianza en seguridad de datos personales y comercio electrónico a los clientes y salvaguardar los activos de cada empresa.
Conceptos adquiridos:	Modalidades de delitos cibernéticos, normatividad vigente en Colombia para la protección de la información y los datos, lineamientos de política para ciberseguridad y ciberdefensa, herramientas open Source enfocadas en la detección de vulnerabilidades, análisis forense y seguridad en redes.
Conclusiones:	- En Colombia el sector empresarial está representado en una gran mayoría por las Mipymes, estás a su vez aportan

	un porcentaje importante al desarrollo económico del país, sin embargo, tienen un alto grado de vulnerabilidad frente a los riesgos cibernéticos, la aparición de la pandemia Covid-19 llevo a muchas de estas organizaciones a entrar en el mundo virtual para ofrecer sus productos y servicios, quedando en evidencia la debilidad que tienen en seguridad informática y peor aún la ausencia de medidas mínimas frente al tema. - Toda organización debe establecer y desarrollar políticas claras frente a su seguridad informática, con ello se podrá mitigar la materialización de amenazas a las cuales se enfrentan, el inadecuado manejo de la información y los datos están afectando significativamente a toda la población y sin duda alguna el patrimonio de las empresas. - Si bien las empresas tienen limitantes económicas para la seguridad informática, se puede decir que quien no invierta en un sistema informático seguro estará siempre expuesto a perder sus clientes y su patrimonio.