DISEÑO DOCUMENTAL DE LAS ACTIVIDADES DEL CSIRT, ORIENTADO A PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS DESDE EL ENFOQUE ADMINISTRATIVO

JONATHAN VELA CADENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

DISEÑO DOCUMENTAL DE LAS ACTIVIDADES DEL CSIRT, ORIENTADO A PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS DESDE EL ENFOQUE ADMINISTRATIVO

JONATHAN VELA CADENA

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director: Christian Angulo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 04 de marzo de 2022

DEDICATORIA

Dedico este trabajo a toda mi familia, a mi abuela, mi padre, mi madre y mi hermano quienes han creído en mí y me ha apoyado desde siempre con la esperanza de verme crecer no solo a nivel profesionalmente, sino personalmente, ellos han sido los testigos de todo el sacrificio que he realizado para llegar a este punto y poder superarme cada vez más, toda mi motivación ha sido gracias a todos ellos, aunque el camino nunca fue fácil, los retos no terminan aquí, este es un paso más en el interminable camino del conocimiento.

A mi abuelo quien en su último año de vida me enseño que todas las cosas se obtienen con esfuerzo, dedicación y disciplina, su ejemplo siempre permanecerá en mí.

.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración este logro no hubiera sido posible.

CONTENIDO

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

. Pág.

GLOSARIO

ACTIVOS: De acuerdo con Romero Castro Martha[1], Son los recursos que tienen un valor importante para la organización, la información es uno de los activos principales de las organizaciones y empresas.

AMENAZA: Son todas las situaciones tanto lógicas como físicas que desencadenan un incidente en la organización dejando como resultado perdidas en sus activos de información.

ATAQUE: De acuerdo con ISO 27000[2], es el Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

EFICIENCIA: Según informática fandom[3], se define como la relación de los recursos utilizados en un proyecto y todos los logros conseguidos con el mismo, la eficiencia también ocurre cuando se utilizan menos recursos para lograr un objetivo o se utilizan los mismos recursos para lograr mayores objetivos.

EVOLUCIÓN: Se orienta a todos los cambios que surgen en las tecnologías cuyo propósito es mejorar, ser más eficientes, ofrecer nuevas funcionalidades y mayores experiencias al usuario final, sin embargo, también aplica para todas las amenazas que circulan en la red, porque cada vez más son más peligrosas y sofisticadas.

[1] ROMERO CASTRO Martha. Introducción a la seguridad informática y al análisis de vulnerabilidades [en línea]. 2018. [consultado: 23 de septiembre 2020]. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[2] ISO 27000. Definición termino ataque [en línea]. [consultado: 23 de septiembre 2020]. Disponible en: https://www.iso27000.es/glosario.html

[3] INFORMATICA FANDOM. Eficiencia [en línea]. [consultado: 23 de septiembre 2020]. Disponible en: https://informatica.fandom.com/wiki/Eficacia_y_eficiencia

IMPACTO: La definición indica “El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales etc”[4].

INFORMACIÓN: Con base en Avenía Delgado Carlos[5], Conformada por un grupo de datos supervisados y ordenados, se utilizan para construir un mensaje basado en cierto fenómeno, puede existir impresa o escrita en papel, transmitida por correo electrónico, almacenada electrónicamente, presentado en imágenes o hasta expuesta en conversaciones.

POLÍTICAS DE SEGURIDAD: Consisten en un conjunto de normas y directrices con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información minimizando los riesgos.

RIESGO: Es la posibilidad de que una amenaza pueda aprovechar o explotar una vulnerabilidad causando una afectación o perdida en los activos.

SEGURIDAD: Según Horney Security[6], En informática se orienta a la seguridad de la información, su principal objetivo consiste en evitar la manipulación, el robo y mantener la confidencialidad de la información y sistemas por parte de terceros no autorizados, no solamente incluye el ámbito digital, también el físico y la nube.

SERVICIO: De acuerdo con Servicetonic[7], Un servicio es un medio para entregar valor a los clientes, facilitando los resultados que los clientes quieren lograr y sin

[4] ISO 27000. Termino impacto. Op. cit, [en línea].
[5] AVENIA DELGADO Carlos. Fundamentos de seguridad informática - Información [en línea]. Pág. 10. 2017. [consultado: 24 de septiembre 2020]. Disponible en: https://digitk.areandina.edu.co/handle/areandina/1367
[6] HORNET SECURITY. Definición del término seguridad informática [en línea]. [consultado: 25 de septiembre 2020]. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/seguridad-informatica/
[7] SERVICETONIC. Que es servicio [en línea]. [consultado: 25 de septiembre 2020]. Disponible en: https://www.servicetonic.com/es/itil/3-itil-conceptos-y-principios/

que éstos tengan que asumir los costes y riesgos asociados a la consecución de dichos resultados.

VIRTUALIDAD: con base al sitio Definiciona[8], Es un fenómeno moderno que trata de un ambiente digital creado por el hombre con la finalidad de interactuar en diferentes espacios sin la necesidad de estar presentes físicamente.

VULNERABILIDAD: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información permitiendo que un posible atacante pueda comprometer la integridad, disponibilidad o confidencialidad de este mismo.

[8] DEFINICIONA. Definición de Virtualidad [en línea]. [consultado: 25 de septiembre 2020]. Disponible en: https://definiciona.com/virtualidad/

RESUMEN

La empresa platino sistemas está enfocada en prestar servicios de seguridad de la información, uno de sus principales objetivos es la implementación de un centro de respuestas a incidentes cibernéticos CSIRT orientados en ofrecer un servicio de calidad para todos sus clientes, en la actualidad muchas organizaciones son víctimas de ataques cibernéticos, especialmente las pequeñas y medianas empresas debido al masivo uso de las redes y a la constante evolución de la tecnología, causando pérdidas incalculables representadas en tiempo y dinero, debido al aumento de ataques cibernéticos y a la aparición de nuevas amenazas se debe hacer frente a todas estas situaciones por lo tanto es necesario realizar un diseño documental para la implementación del CSIRT teniendo en cuenta los principales elementos como los diferentes servicios a operar, la identificación de los ciber ataques más relevantes, la definición de los perfiles para el equipo de trabajo, la implementación de políticas con los respectivos procedimientos y la estructura organizacional, la CSIRT se define como un centro de respuestas ante emergencias informáticas conformado por un grupo de expertos con la responsabilidad de mitigar o detener un impacto, así mismo implementar medidas preventivas y reactivas que permita fortalecer la seguridad de los sistemas en las organizaciones.

Palabras clave: Amenazas, CSIRT, Impacto, Seguridad, Servicios.

ABSTRACT

The Platino Sistemas company is focused on providing information security services, one of its main objectives is the implementation of a CSIRT response center for cyber incidents aimed at offering a quality service to all its clients, today many organizations are Victims of cyber attacks especially small and medium-sized companies due to the massive use of networks and the constant evolution of technology, causing incalculable losses represented in time and money, due to the increase in cyber attacks and the appearance of new threats must be faced In all these situations, therefore, it is necessary to carry out a documentary design for the implementation of the CSIRT, taking into account the main elements such as the different services to operate, the identification of the most relevant cyber attacks, the definition of the profiles for the work team , the implementation of policies with the resp ective procedures and the organizational structure, the CSIRT is defined as a computer emergency response center made up of a group of experts with the responsibility of mitigating or stopping an impact, as well as implementing preventive and reactive measures that allow strengthening the security of the systems in organizations.

Keywords: *Threats, CSIRT, Impact, Security, Services.*

INTRODUCCIÓN

Anteriormente las organizaciones empezaban a mirar la seguridad de la información con un alto nivel de importancia, ya que la pérdida de información que sufrieron muchas organizaciones en todo el mundo a causa de ataques informáticos como el *ramsonware* o el secuestro de la información dejó secuelas y muchas pérdidas, obteniendo como resultado la reflexión y las inclusiones de planes y estrategias para fortalecer la capa de seguridad en las organizaciones, que es totalmente necesaria con el solo hecho de conectarse a la red, esa misma herramienta que tantos beneficios ha ofrecido a la sociedad, también posee una parte oculta que puede ser peligroso para cualquiera que no tome las medidas pertinentes.

En la actualidad el consumo del internet y el uso de dispositivos tecnológicos se ha incrementado fuertemente especialmente en entornos empresariales debido a la pandemia, la mayoría de las organizaciones han tenido que cambiar su forma de operar, para suplir las actividades físicas han implementado el teletrabajo también llamado como el proceso de transformación digital, con el fin de conservar la continuidad del negocio, sin embargo al mismo tiempo las amenazas que circulan en la red también se han incrementado otorgando un cierto grado de riesgo para los activos de las organizaciones donde las más golpeadas son las pequeñas y medianas empresas.

No todas las organizaciones tienen la capacidad para establecer sus estrategias de seguridad digital acertadamente, adicional no tienen la prioridad de un servicio que les apoye o los oriente ante situaciones adversas, a pesar de que en Colombia el tema de la seguridad de la información ha tomado fuerza, aún quedan oportunidades de mejoras con el fin de que las organizaciones puedan desarrollar procesos para la continuidad del negocio de forma equitativa y al mismo tiempo generar la concientización que es un elemento indispensable para afrontar los retos de la ciber seguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En los últimos años la tecnología ha estado en constante evolución, de acuerdo con la república[9], de igual manera sucede lo mismo con las amenazas que circulan en la red, de hecho, en estos últimos años los ataques cibernéticos han aumentado de manera incontrolable en muchos casos causando pérdidas incalculables y esto es posible en gran medida porque muchas organizaciones no estaban preparadas para mantener sus activos de forma segura.

Según Factor capital humano[10], anteriormente con solo tener instalado el antivirus en los equipos de cómputo de las pequeñas o medianas empresas (pyme) bastaba para proteger de los peligros existentes, sin embargo, la sofisticación de los nuevos ataques requirió tomar el tema con toda la seriedad, de hecho los expertos coincidieron en la importancia de que las organizaciones generaran una cultura de la seguridad informática y así mismo incluyeran personal con los conocimientos idóneos para hacer frente a las amenazas que puedan comprometer la información en este tipo de organizaciones.

En España, el coste de los ciberataques ya se calcula en 40 millones de euros, siendo la pequeña y mediana empresa las más afectadas. Los datos indican que 7 de cada 10 ciberataques tienen como víctimas a las pymes, cinco días[11], indica que

[9] LA REPÚBLICA. Aumento de cibercrímenes [en línea]. [consultado: 27 de septiembre 2020]. Disponible en: https://www.larepublica.co/empresas/en-tiempos-de-covid-19-empresas-deben-protegerse-ante-aumento-de-cibercrimenes-3041263

[10] FACTOR CAPITAL HUMANO. Pymes estrategias integrales para la ciberseguridad [en línea]. [consultado: 27 de septiembre 2020]. Disponible en: https://factorcapitalhumano.com/emprendedores/pymes-necesitan-estrategias-integrales-de-ciberseguridad/2018/05

[11] CINCO DÍAS. 70% de los ciberataques son a pymes [en línea]. [consultado: 29 septiembre 2020]. Disponible en: https://cincodias.elpais.com/cincodias/2020/02/23/pyme/1582491990_626988.html

uno de los factores que facilita los ciberataques es que los usuarios no tienen en cuenta medidas básicas de seguridad, por ejemplo, el 90% de los internautas ignora la forma de crear una contraseña segura mientras que el 48% admite que no la cambia nunca o casi nunca. Además, dos de cada cinco empresarios ignoran las actualizaciones informáticas de su equipo, en otras palabras, es un riesgo.

Cisco, una de las principales compañías de tecnología del mundo, estima que el 53 % de las pequeñas y medianas empresas latinoamericanas sufren brechas de seguridad. Lo peor de todo es que cada incidente puede costar más de $8.000 millones. Ghassan Dreibi[12], responsable de seguridad de Cisco para América Latina, explica que los delincuentes están detrás de todo lo que implica dinero sin importar la actividad y el tamaño de la organización, a ellos les resulta muy fácil y lucrativo atacar a las pymes porque existen diferentes canales por los cuales pueden entrar. Se aprovechan del desconocimiento, de los pocos recursos de ciberseguridad, y de algunas prácticas de la organización y de algunos directivos para poder acceder a la información de la empresa.

Según las cifras conocidas por Latín Pymes Colombia[13], con base a la información brindada por el Departamento de Delitos Informáticos de la Policía Nacional de Colombia, el año pasado (2018) se recibieron 7.118 denuncias. El 43% de las empresas colombianas no están realmente preparadas para responder y desafortunadamente son las pymes las más vulnerables, ya sea en materia de capacidad instalada o de los recursos económicos.

[12] GHASSAN Dreibli. Pymes como blanco para los ciber delincuentes [en línea]. México. [consultado: 29 de septiembre 2020]. Disponible en: https://www.elespectador.com/noticias/tecnologia/las-pymes-como-blanco-para-los-ciberdelincuentes/

[13] LATIN PYMES. Pymes vulnerables [en línea]. [consultado: 30 de septiembre 2020]. Disponible en: https://www.latinpymes.com/pymes-vulnerables-a-ciberataques/

En Colombia, como indican las tendencias del cibercrimen[14], la fiscalía general de la nación expuso que el monto de pérdidas generadas por los ciberataques está entre 120 millones a 5.000 millones de pesos, dependiendo del tamaño de la organización afectada. El 45.5% de las denuncias se hicieron por canales virtuales y en el transcurso de 2019, se han reportado 28.827 incidentes de ciberseguridad empresarial en el país, de los cuales 17.531 casos han sido denunciados ante la fiscalía. De 2017 a 2019 se reportaron 52.901 denuncias de las cuales el mayor número de hurtos se realizan a través de medios informáticos (31.058), luego por robo de identidad (8.037), cabe resaltar que Bogotá fue la ciudad con más incidentes que se reportaron (5.308), seguido de Cali (1.190) y Medellín (1.186).

Según *Statics Securelist*[15]*,* A nivel nacional mensualmente se reportan entre 1.000.000 a 1.400.000 notificaciones de ataques. La Figura 1 refleja los incidentes reportados entre el mes de septiembre y octubre de 2019:

Figura 1. Incidentes reportados entre septiembre y octubre 2019

Fuente: STASTICS SECURELIST. Intrusión y detección en Colombia. [en línea]. 2019. Disponible en: https://statistics.securelist.com/es/country/colombia/on-access-scan/month

[14] CCIT. Cibercrimen [en línea]. Bogotá. [consultado: 20 de septiembre de 2020]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[15] STATICS SECURELIST. Intrusion Detection Scan Month [en línea]. Colombia. [consultado: 01 de octubre 2020]. Disponible en: https://statistics.securelist.com/es/country/colombia/intrusion-detection-scan/month

Sin embargo, Redscan[16], que es un proveedor de servicios de seguridad, reveló en su informe que: el año pasado (2020) se reportaron 18.103 vulnerabilidades, de las cuales en su mayoría 10.342 fueron clasificadas como de alta severidad o crítica, de hecho, estas vulnerabilidades superaron en número a la suma total de vulnerabilidades reportadas en 2010; incluyendo las de una severidad menor. Los indicadores de política y estrategia de seguridad cibernética se presentan desde el 2016 a 2020, de acuerdo con *Publication iadb*[17], se evidencia un avance importante, pero aún quedan muchos aspectos para mejorar, incluso para muchas organizaciones no es suficiente, el aspecto más destacado es el desarrollo de la estrategia, el menos destacado es la redundancia de las comunicaciones, la Figura 2 muestra en detalle el estado desde el año 2016 hasta el año 2020, esta información es la base para identificar en que aspectos se debe mejorar:

Figura 2. Indicadores política y estrategia de seguridad cibernética 2016 - 2020

Fuente: PUBLICATIONS.IADB política cibernética [en línea]. Disponible: Pág. 82. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[16] WELIVESECURITY. Record vulnerabilidades reportadas [en línea]. 2020. [consultado: 01 de octubre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2021/02/16/record-vulnerabilidades-reportadas-en-2020/

[17] PUBLICATIONS. Política de seguridad cibernética [en línea]. Pag.82. [consultado: 01 de octubre 2020]. 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

1.2 FORMULACIÓN DEL PROBLEMA

Las pymes y medianas empresas son mucho más vulnerables a los ataques cibernéticos, partiendo de que no todas poseen la orientación y todos los recursos necesarios para suplir la necesidad de establecer infraestructuras más seguras, se crea la necesidad de formar un CSIRT (para pymes y medianas empresas) con el fin de apoyar, orientar y solucionar las diferentes problemáticas que se puedan presentar en lo relacionado con la ciber seguridad, partiendo de este punto se desarrolla el siguiente proyecto que busca resolver el siguiente interrogante:

¿Cuáles son los elementos esenciales que necesita un CSIRT desde el enfoque administrativo para operar exitosamente y afrontar los retos actuales de la ciberseguridad en las pequeñas y medianas empresas?

2. JUSTIFICACIÓN

La transformación digital en las organizaciones llego para quedarse y en estos tiempos este cambio se aceleró debido a los efectos que causo la pandemia a nivel mundial.

La información es el activo más importante y valioso para las organizaciones, como indica Velázquez Durán Ana[18], teniendo en cuenta el surgimiento de nuevas amenazas que exponen nuevos riesgos, a nivel mundial cada día se envían 6400 millones de correos falsos, no cabe duda, poder combatir las filtraciones de datos y las posibles vulnerabilidades de la privacidad se ha convertido en todo un reto, adicionalmente el servicio de la nube ha sido cada vez más usado, pero sin tomar las medidas necesarias de seguridad lo que ha impactado a muchas organizaciones de forma considerable.

Un estudio en ABC[19], explica que, inclusive en los últimos años ataques como el phishing en el que los ciber delincuentes utilizan el virus para hacerse pasar por terceros, engañar a la víctima y de esta manera obtener todos sus datos bancarios han aumentado de forma incalculable, en España han descubierto varios tipos de estafas que abarcan desde correos hasta mensajes de celular o *Whatsapp* en los que se suplanta organismos oficiales, en otras partes del mundo los cibercriminales se están aprovechando del trabajo en remoto, servicio últimamente muy utilizado a raíz de la pandemia, diseñando falsas soluciones disfrazadas para el trabajo en casa con el fin de penetrar en algunos casos las redes empresariales para poder

[18] VELASQUEZ DURAN Ana. EL TIEMPO. Principales ataques de cibercriminales en Colombia [en línea]. 2019. [consultado: 02 de octubre 2020]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-ataques-de-cibercriminales-en-colombia-371096

[19] ABC. Ciberataques a hospitales [en línea]. EEUU. [consultado: 02 de octubre 2020]. Disponible en: https://www.abc.es/tecnologia/redes/abci-eugene-kaspersky-ciberataque-contra-hospitales-atentado-terrorista-202004230204_noticia.html

robar datos. Cifras de Retina el País[20], En el año 2019 hubo 8.914 detenciones e investigaciones por ciber delitos, una compañía puede tardar entre dos o más meses en resolver un ataque a sus sistemas.

Según USS[21], Las pequeñas y medianas empresas han sido creadas por el esfuerzo de familias, pequeños grupos de socios o hasta por un individuo, invirtiendo muchos recursos y tiempo, todos estos patrimonios deben estar resguardados de una forma óptima, ya que el impacto o las perdidas en una pyme que pueda sufrir a causa de una falla de seguridad informática puede ser totalmente irrecuperable. Por el tipo y tamaño de las organizaciones es poco viable que interna o individualmente implementen un servicio del CERT, por lo tanto, se evidencia una necesidad de ofrecer un servicio único orientado a pequeñas (pymes) y medianas empresas.

Las amenazas cibernéticas no conocen la diferencia entre grandes, medianas y pequeñas empresas, como lo indica en *sites oas*[22], sin embargo, las empresas pymes debido a su tamaño y naturaleza muy a menudo no pueden contar con la implementación de equipos de respuesta a incidentes, para esta comunidad de negocios se presenta una necesidad por ejemplo en España existe el INTECO-CERT el cual se enfoca en brindar servicios a la pyme.

El instituto nacional de ciberseguridad indica: “Las empresas deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios”[23].

[20] RETINA EL PAIS. Cifras ciberseguridad: Las cifras de los ataques informáticos [en línea]. [consultado el 02 de octubre]. Disponible en: https://retina.elpais.com/retina/2020/07/17/tendencias/1594958904_685745.html
[21] USS. Medidas de seguridad informática para empresas pymes [en línea]. 2018. [consultado: 4 de octubre 2020]. Disponible en: https://uss.com.ar/corporativo/medidas-de-seguridad-informatica-pyme/
[22] SITES OAS. Las buenas prácticas del CSIRT [En línea]. 2016. [consultado: 4 de octubre 2020]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
[23] INCIBE. Guía decálogo de ciberseguridad [en línea]. 2017. [consultado: 4 de octubre 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

En *Deloiite*[24], afirman que un evento cualquiera como un ataque de malware, robo de equipos, catástrofes, corrupción de datos o cualquier fallo crítico que interfiera en la actividad normal de cualquier negocio se convierte automáticamente en un incidente.

Para combatir todos estos nuevos métodos de ciber ataques que circulan en la red *search data center*[25], indica que los centros cibernéticos CSIRT conformados por un grupo de expertos en seguridad informática tienen la función de brindar una orientación para evitar, mitigar y restablecer los servicios ante cualquier amenaza que pueda causar un impacto negativo a las organizaciones en el menor tiempo posible y así mismo contribuir al desarrollo de actividades de evaluación de riesgos, desarrollos de planes de continuidad, documentaciones, experiencias y la concientización de los usuarios, de esta manera los CSIRT se convierten en un elemento indispensable especialmente para las medianas y pequeñas empresas.

[24] DELOITTE. Ciberseguridad enfocada a las pymes [en línea]. 2019. Pág. 8 [consultado: 4 de octubre 2020]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/risk/CyberMonth2019/guia-ciberseguridad-para-pymes-2019.pdf

[25] SEARCHDATACENTER. Equipo de respuestas frente a incidencias [en línea]. [consultado: 4 de octubre 2020]. Recuperado de https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Estructurar las principales actividades que conforman el CSIRT para brindar servicios de ciberseguridad a las pequeñas y medianas empresas, realizando un diseño documental.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer la taxonomía de los ataques más relevantes para la actuación del CSIRT en materia de ciberseguridad.

- Caracterizar el catálogo de los principales servicios del CSIRT para ofrecer a sus clientes.

- Formular políticas, procedimientos y manuales operacionales del CSIRT, para que sea adoptado y aplicado por el personal.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Las TIC ha desarrollado a través del tiempo la forma de comunicarse entre las personas, superando la barrera que existía en las comunicaciones y en el intercambio de información, creando una que actualmente todo el mundo coincide y no es más ni menos que el ciber espacio.

Tanto los gobiernos como las empresas deben promover una cultura de ciberseguridad en todos los niveles que propicie la prevención de las amenazas. La colaboración internacional y nacional entre los sectores públicos y privados juega un papel vital para el fortalecimiento de los marcos de ciberseguridad nacionales.

Como se indica en Publications IADB[26], Es necesario realizar más trabajo legislativo y regulatorio si se desea ver un progreso. El intercambio de información y la respuesta operativa también deben ser determinantes.

En Colombia los mecanismos técnicos y legislativos son:

- El centro cibernético policial: Quienes son responsables de la ciberseguridad del país otorgando apoyo, información, orientación y protección ante los delitos cibernéticos.

[26] PUBLICATIONS IADB. Reporte riesgos avances y el camino a seguir de ciberseguridad América latina y el caribe. [en línea]. 2020. Pag.20. [consultado: 05 de octubre 2020]. 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

- ColCERT: Su responsabilidad radica en proteger la infraestructura crítica del país frente a situaciones de emergencias relacionadas con la ciberseguridad.

- CCOC Comando conjunto cibernético de las fuerzas armadas de Colombia: planea y conduce operaciones militares en el ciberespacio, para contrarrestar amenazas y ataques en Internet.

Los principales objetivos del colCERT son:

- Coordinar con la comisión intersectorial el desarrollo y promoción de políticas, procedimientos, recomendaciones, protocolos y guías de ciberseguridad y ciberdefensa, en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento.

- Coordinar y asesorar a CSIRTs y entidades tanto del nivel público, privado y de la sociedad civil en la respuesta a incidentes informáticos.

- Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como aquellos de información, sensibilización y formación en materia de seguridad informática a todas las entidades que así lo requieran.

- Coordinar la ejecución de políticas e iniciativo público - privadas de sensibilización y formación de talento humano especializado, relativas a la ciberseguridad y ciberdefensa.

- Proveer al CCP y al CCOC la información de inteligencia informática que sea requerida.

En la Figura 3 se observa la interacción entre el ColCERT, comando conjunto cibernético y el centro cibernético policial donde su objetivo común es la cooperación en la resolución de incidentes:

Figura 3. Modelo de coordinación

Fuente: MINISTERIO DE DEFENSA. Marco legal CONPES [en línea].2011. Pág.21 disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

Con el fin de llevar a cabo la resolución de incidentes informáticos de una manera exitosa, la comisión intersectorial relaciona al ColCERT con el comando conjunto cibernético y a su vez con el centro cibernético policial, es decir existe un trabajo en equipo a pesar de que operan de forma independiente, pero gracias a esta estrategia existe una colaboración y comunicación para realizar diferentes tipos de actividades como por ejemplo la asistencia ante emergencias, anuncios

informativos sobre inteligencia cibernética o la coordinación en la gestión de incidentes, el trabajo en equipo es una forma más eficiente de brindar el servicio ante las amenazas que circulan por la red.

En la Figura 4, el modelo relacional del ColCERT demuestra cómo está conectado con cada sector, sin importar el ámbito el objetivo es el mismo, incluso va más allá del territorio nacional, el sector privado también hace parte de este modelo de estrategia nacional de ciberseguridad. El ColCERT brinda el direccionamiento político y estratégico a la comunidad, pero al mismo tiempo mantiene alianzas con otros organismos del estado teniendo en cuenta a los organismos judiciales.

Figura 4: Modelo Relacional colCERT

Fuente: MINISTERIO DE DEFENSA. Estrategia nacional de ciberseguridad [en línea]. Pag.24. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

4.1.1 La seguridad informática El concepto de seguridad informática se orienta básicamente en el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad de la información que reside en un sistema de información,[27] proceso que consiste en la detección y prevención de acceso no autorizado a los sistemas informáticos y recursos por parte de terceros hacia las organizaciones con la intención de causar afectaciones en el servicio.

Las organizaciones deben enfocarse en conocer su infraestructura para poder implementar medidas para la prevención de amenazas y de los riesgos que se pueden ocasionar al utilizar recursos internos, sin embargo esto va más allá de establecer políticas y mecanismos de defensa pues hoy en día el uso de la tecnología ha sido fundamental para optimizar procesos y cumplir objetivos organizacionales, sin embargo así mismo se han originado nuevas amenazas y se hace necesario que las empresas especialmente las pequeñas y medianas empresas cuenten con la correcta orientación para que los niveles de la seguridad informática respondan a las necesidades actuales, estos recursos en muchas ocasiones son sumamente costosas para algunas organizaciones.

Otro detalle fundamental se basa en que la seguridad informática en las empresas ya no es una responsabilidad totalmente de la oficina de TI, sino que se deben buscar estrategias para integrar a todos los colaboradores que formen parte del equipo con el objetivo de comunicar, educar y concientizar acerca de las amenazas existentes y como el actuar de cada integrante es clave para superar las posibles dificultades con respecto a la seguridad informática y de la información.

[27] SEGURIDAD INFORMATICA. Definición y principios de la seguridad informática [sitio web]. [Consultado: 08 de octubre de 2020]. Disponible en: https://sites.google.com/site/seguridadinformaticacmj/introduccion

4.1.2 Principios de la seguridad de la información

La seguridad de la información se basa en la protección de los activos de la información, en las organizaciones tiene un valor sumamente importante, los profesionales de la ciberseguridad evalúan las amenazas y las vulnerabilidades enfocadas en el impacto que tendrían sobre la confidencialidad, integridad y disponibilidad de los activos de la organización.

Integridad: Consiste en garantizar que los datos no hayan sido manipulados por terceros sin previa autorización, por lo tanto, al consultarlos se pueda tener la seguridad de que son totalmente confiables, esta integración se pierde cuando la información es alterada o por ejemplo se pierde parte de ella.

Confidencialidad: Se refiere a mantener datos secretos o privados, es decir tratar de controlar el acceso a los datos para evitar su divulgación de forma no autorizada, por ejemplo la confidencialidad se pierde cuando tiramos un disco duro sin antes eliminar la información o por lo menos cuando tampoco la ciframos, también podría suceder cuando dejamos nuestro usuario sin bloquear, de esta manera la confidencialidad de la información entra en riesgo.

Disponibilidad: Se enfoca principalmente en que los activos, los sistemas y aplicaciones estén en pleno funcionamiento en el momento que sean solicitados o requeridos y por lo tanto se pueda tener acceso oportuno y seguro, es decir que por ejemplo cuando necesitemos acceder a la información lo hagamos sin importar el momento, sin embargo cuando nuestra información está cifrada el acceso no es tan fácil, pero aquí entra la responsabilidad como usuario con respecto a la información.

4.2 MARCO CONCEPTUAL

4.2.1 CSIRT- Sector de las pymes Sus servicios están totalmente orientados a las pequeñas y medianas empresas, ya que por su naturaleza se les dificulta la implementación de la gestión de incidentes de forma individual, actualmente esta comunidad no es pequeña, incluso en España se encuentra el ejemplo de INTECO-CERT *Corporation* que además de ayudar a las pymes lo hace con los ciudadanos, a lo largo de los años este sector se ha olvidado y por la misma demanda se ha creado un CSIRT especialmente para que se haga cargo de todas las solicitudes e incidencias que se generan desde este sector.

4.2.2 CSIRT – Infraestructuras críticas Este tipo de CSIRT puede pertenecer más a una comunidad, su objetivo principal está orientada a la protección de activos de información y a la infraestructura critica de la nación como por ejemplo pueden operar el sector de la energía o del transporte sin importar si la organización está ubicado en el sector público o privado, en este tipo de CSIRT se suelen crear protocolos de interacción con otro tipo de equipos involucrados con el fin de adoptar nuevas medidas y estrategias para ser más efectivos antes las nuevas ciber amenazas.

4.2.3 CSIRT – Académicos Orientadas especialmente a comunidades académicas, como universidades, colegios o institutos, su tamaño y sus instalaciones puede variar y frecuentemente buscan unir fuerzas con otros CSIRT académicos con el fin de poder tener aliados que permitan el desarrollo de nuevas estrategias para prestar mejores servicios ante las diferentes incidencias que se puedan presentar, adicionalmente se especializan en investigaciones, el personal atendido básicamente son estudiantes y el personal que conforman las comunidades académicas.

4.2.4 CSIRT- Nacional Normalmente asumen el rol de coordinador nacional de respuesta a incidentes teniendo en cuenta a la biblioteca de seguranca[28], es el punto de contacto entre incidentes a nivel nacional e internacional, se puede decir que es un CSIRT de último recurso, ya que puede tomar cualquier papel que sea necesario, por ejemplo, si no hay un CSIRT enfocado para la estructura crítica, entonces el CSIRT nacional puede asumir las responsabilidades que normalmente son asignadas a un equipo de respuesta de infraestructura crítica, este tipo de CSIRT no tiene un cliente en específico, ya que normalmente actúa como intermediario en el país. En la Figura 5 se observa el principal objetivo de los CSIRT:

Figura 5. Objetivo de un CSIRT

Fuente: TB Security. Que se protege. [en línea]. Disponible en: https://cso.computerworld.es/alertas/tb-security-pasa-a-formar-parte-de-grupo-incita

[28]ORGANIZACIÓN DE LOS ESTADOS AMERCIANOS. Ámbitos del CSIRT y buenas prácticas Nacional [En línea]. [consultado: 07 de octubre 2020]. Washington D.C. Disponible en: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

4.2.5 CSIRT - Proveedores: Sus servicios están enfocados plenamente con los productos específicos de los proveedores, desarrolladores o fabricantes, su papel principal es diseñar soluciones para eliminar vulnerabilidades relacionadas con sus productos y al mismo tiempo atender incidentes de alto impacto que puedan afectar los producto o representar un riego, por ejemplo, los productos de Hewlett Packard (HP), Adobe PSIRT, Banelco CSIRT entre otros, básicamente su noción es específica para un tipo de cliente.

4.2.6 CSIRT – Militar: El CSIRT militar es el responsable de la infraestructura IT para la defensa nacional, según CCN-CERT CNI[29], su comunidad suele estar conformada por una institución relacionada con los estamentos militares, un ejemplo sería el NATO *Computer Incident Response Capability* (NCIRC), otorga servicios a 32 redes que proporcionan servicios técnicos para responder a los incidentes de seguridad informática dentro de la OTAN, es decir que un CSIRT presta sus servicios a instituciones militares de un estado, sus principales funciones se enfocan en las actividades de defensa o a las estrategias ofensivas.

4.2.7 CSIRT – Gubernamental: Su principal objetivo es garantizar la infraestructura IT del gobierno y toda la disponibilidad de los servicios gubernamentales ofrecidos a la población, la comunidad, las regiones a la que el servicio va dirigido, corresponder a los administradores y sus distintos organismos, deben garantizar que los servicios que se ofrezcan a los ciudadanos posen niveles adecuados de seguridad, un ejemplo sería el caso del Ministerio de Educación Nacional y el de transporte, estos pueden operar de manera totalmente independiente pero también colaborar regularmente.

[29] CCN-CERT CNI. Tipología de un CSIRT - Militar [en línea]. Pág. 51. [consultado: 07 de octubre de 2020] Disponible en: https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/657-el-papel-de-un-cert-gubernamental/file.html

4.3 MARCO HISTÓRICO

Según *Welivesecurity*[30], la historia comienza en 1998 cuando se conoció por primera vez el gusano de internet, en ese momento había muy pocos equipos conectados a la red internet, pero fue suficiente para saturar esos sistemas, este gusano llamado Morris tenía la capacidad de auto replicarse por lo que termino afectando alrededor de 6.000 servidores a nivel mundial, esta situación dio origen para fundar el primer equipo de respuesta a incidentes cibernéticos en todo el mundo.

Más tarde a mediados del año 2007 de acuerdo con CCN CERT[31], en España, nació el centro de respuestas a incidentes en tecnologías de la información para pymes y ciudadanos llamado (INTECO - CERT) enfocado en prestar apoyo en materia de seguridad brindando servicios clásicos como respuestas a incidentes, soluciones reactivas, servicios de prevención y concienciación pues los CSIRT se orientaban en varios ámbitos. En 2011 INTECO-CERT localizaba códigos maliciosos que clasificaba con la finalidad de conseguir una mayor seguridad en la red, adicionalmente asesoraba a los usuarios sobre cómo protegerse de las diferentes amenazas que poco a poco comenzaban a surgir, emitieron más de 60 alertas sobre malware y otras amenazas con el propósito de transmitir en tiempo real todos los riesgos que pudieran impactar las redes y los sistemas. A través de los años han surgido miles de incidentes de seguridad de la información que ha puesto en jaque la red entera, desde este punto la relevancia que ha tomado la ciberseguridad ha sido notable, pues los sistemas informáticos han tomado un rol de tanta importancia para la vida cotidiana y para las organizaciones.

[30] WELIVESECURITY. Malware años 80 [en línea]. 2018. [consultado: 10 de octubre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2018/11/05/malware-anos-80-recordando-virus-informatico-brain-gusano-morris/

[31] CCN CERT. INTECO CERT. [en línea]. pág. 28. [consultado: 11 de octubre de 2020]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

4.4 ANTECEDENTES O ESTADO ACTUAL

En el lapso de los años 2015 a 2017 iniciaban los indicios que las organizaciones disponían de barreras para afrontar adecuadamente los temas de ciberseguridad, pues a pesar de que siempre habían existido antecedentes de ataques informáticos los empresarios creían que invertir en ciberseguridad para las empresas era una necesidad no prioritaria y que incluso habían otros que pensaban que hacerlo sería perder dinero y que tenían temas más importantes, sin embargo también existían otros casos como la falta de recursos especialmente en las medianas y pequeñas empresas. En la Figura 6 se encuentran las principales barreras que tenían las organizaciones desde el año 2015 al 2017, a medida que los años pasaron se redujeron los problemas en temas presupuestales y de compatibilidad en sistemas, pero se aumentó la falta de personal capacitado:

Figura 6: El mayor obstáculo para las restricciones presupuestales de seguridad

Fuente: CISCO. Reporte anual de ciberseguridad. [en línea]. 2018. Pág.50. Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

De acuerdo con OAS[32] en el año 2017 las empresas consideraban que el riesgo de la ciberseguridad aumentaba en más de un 70%, la revista dinero indica[33], que la seguridad informática en Colombia 2019 demostró que el 87% de las organizaciones operan con niveles limitados en el ámbito de ciberseguridad, mientras que un 77 % opera con medidas de protección básicas, a pesar de que estos últimos años se han aprendido lecciones importantes, pero las juntas directivas no tienen en cuenta el tema de ciberseguridad como un plan estratégico para sus organizaciones. Por medio de un estudio de la firma *Comparitech*[34], en el que se incluye 76 países del mundo y basado en un análisis del estado actual de ciberseguridad Colombia se encuentra en la posición 40, claramente se puede mejorar más, en Latinoamérica Colombia se encuentra por detrás de países como Brasil, Perú, Ecuador, México Chile y Argentina los ítems calificados fueron:

- Dispositivos móviles infectados: 14.23%.
- Ordenadores afectados por malware: 8.8%.
- Ciberataques generados en Colombia: 0.59%.
- Grado de preparación: 56.5%.

En algunos casos las empresas tardan más de seis (6) meses en detectar que han tenido una violación de datos, en otras palabras, la organización es cada vez más susceptible a que le roben su información y cada vez más vulnerable a este tipo de ataques. Los incidentes más reportados en Colombia:

- El phishing es el incidente más reportado en Colombia con un 42%.
- La suplantación de identidad 28%.
- El envío de malware 14%.
- Los fraudes en medios de pago en línea con 16%.

[32] OAS. Riesgo cibernético sector financiero [en línea]. 2019. [consultado: 14 de octubre 2020]. Disponible en: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

[33] DINERO. Como actúa la ciberseguridad en Colombia [en línea]. 2019. [consultado: 15 de octubre 2020]. Disponible en: https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

[34] COMPARITECH. Which countries have the worst (and best) cybersecurity [en línea]. 2021. [consultado: 23 de septiembre de 2021]. Disponible en: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Teniendo en cuenta a *Netdatanetworks*[35], cerca del 90% de los ciberataques que sufren las empresas en Colombia se deben a la ingeniería social. Los cibercriminales obtienen información confidencial de empresas, directivos y empleados, a través de distintas técnicas para luego suplantar identidades, falsificar correos electrónicos y conseguir en la mayoría de los casos desviar dinero a cuentas bancarias bajo su control o generar despachos de insumos y mercancías engañando a clientes y proveedores.

Por otro lado, la emergencia sanitaria tuvo un impacto de manera inmediata en la conectividad de los diferentes dispositivos: “las conexiones durante la pandemia se han incrementado en más de 40%, lo cual hace que los riesgos aumenten dada la mayor exposición de los usuarios a ciberataques (...) Los delincuentes utilizan multitud de técnicas para sustraer de manera ilegal información”, aseguró Gerardo González, gerente transformación de Sonda Colombia[36].

Pymas[37], indicas que el 60 % de las pequeñas y medianas empresas en Colombia, realmente no pueden sostener sus negocios luego de sufrir un ataque informático, de acuerdo con el informe de tendencias del cibercrimen en Colombia (2019-2020). Lo más grave de este panorama actual es que las pymes carecen de sistemas robustos de ciberseguridad, esto los convierte en el tipo de víctimas preferidos por los ciberdelincuentes.

[35] NETDATANETWORKS. Ciberataques en Colombia [en línea]. 2020. [consultado 1 de diciembre 2020]. Disponible en: https://blog.netdatanetworks.com/ciberataques-en-colombia-recomendaciones-para-hacerle-frente

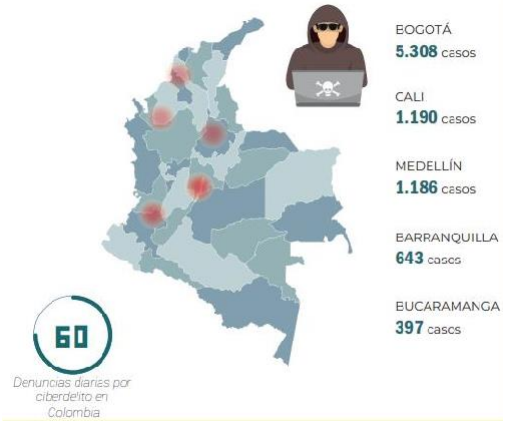
[36] LA REPÚBLICA. Reto que deben enfrentar las empresas en el mundo COVID [en línea]. 2020. [consultado: 28 de octubre de 2020]. Disponible en: https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083

[37] PYMAS. La ciberseguridad enfocada a pymes en Colombia [en línea]. [consultado: 28 de octubre 2020]. Disponible en: https://www.pymas.com.co/ideas-para-crecer/ayuda-legal/ciberseguridad-pymes-colombia

4.4.1 Delitos informáticos por ciudades La concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados.

Si bien la cifra obedece a los centros urbanos con mayor densidad poblacional y penetración de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar hacia PYMES, entidades financieras y grandes compañías con asiento en estas ciudades. En la Figura 7 están reflejadas las ciudades con más delitos informáticos para el 2019 en Colombia donde Bogotá fue la ciudad que obtuvo más casos seguidos por Cali, Medellín, Barranquilla y Bucaramanga, Sesenta denuncias diarias relacionas al ciberdelito parece una cifra inofensiva, pero en la realidad es un aviso inminente de que la situación puede empeorar, especialmente en estos departamentos donde no existe la suficiente información y preparación para enfrentarse a algún tipo de ataque informático.

Figura 7. Delitos informáticos por ciudades



Fuente: CCIT.ORG.CO. Informe tendencias del cibercrimen [en línea]. 2019.Pág 8. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

De acuerdo con CCN-CERT[38], dependiendo de la organización patrocinadora y de la comunidad que se atiende un CSIRT se puede clasificar en:

4.5.1 Modelo de organización independiente. En este modelo solo opera una organización independiente, es decir que esta creada por sus propias finanzas, empleados, estructura y políticas a lo que se denomina como un CERT.

4.5.2 Modelo integrado en una organización preexistente. En este modelo el CERT opera como un departamento de la organización, normalmente está comandado por un jefe líder del proceso.

4.5.3 Modelo campus. En este modelo se toma como ejemplo algunas entidades que tienen una sede central y otras distribuidas con un nivel de dependencia, en este caso hay un CERT principal y unidades o CERTs más pequeños de menos jerarquía dependientes del primero, ideal para grandes organizaciones con elevada descentralización.

4.5.4 Modelo basado en el voluntariado. En este modelo normalmente lo constituye un CERT “ad hoc” donde un grupo de especialistas se unen para apoyarse entre sí y prestar un servicio a una comunidad de forma voluntaria.

[38] CCN-CERT. Creación CERT-CSIRT [en línea]. 2011. Pág.21. [consultado: 02 de diciembre 2020]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf

4.6 MARCO LEGAL

4.6.1 Ley 1266 de 2008 De acuerdo con función pública[39], es conocida también como la ley de “HABEAS DATA”, establecida por el gobierno nacional con el objetivo de desarrollar el derecho constitucional que tienen las personas para conocer, actualizar y verificar informaciones que hayan sido recolectadas en el banco de datos, adicionalmente incluye todas las garantías constitucionales con la recolección de datos personales del artículo 15 de la constitución política sobre la información financiera, comercial, de servicios y crediticia. Esta ley se aplica para todos los datos personales financieros, comerciales y crediticios registrados en un banco de datos. Otros tipos de datos como por ejemplo aquellos mantenidos en un ámbito exclusivamente personal se encuentran excluidos de la aplicación de esta norma.

4.6.2 Ley 1273 de 2009. Consultando la secretaria de senado[40], esta ley desarrolló nuevos tipos penales relacionados con los delitos informáticos, la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales vigentes, el congreso de la república promulgó la ley 1273 “por medio del 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”, es decir que por medio de esta ley se estructuran los delitos informáticos, cada uno con sus propias penalizaciones.

[39] FUNCIÓN PÚBLICA. Ley 1266 de 2018. [31 de diciembre 2018]. Por la cual se dictan las disposiciones generales del hábeas data [en línea]. [consultado: 25 de septiembre 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3448

[40] SECRETARIA SENADO. Ley 1273 de 2009. [5 de enero 2009]. Por la cual se crea un nuevo bien jurídico “de la protección de la información y de los datos [en línea]. [consultado: 3 de diciembre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

4.6.3 Ley 1581 de 2012. En esta norma se dictan disposiciones generales para la protección de datos personales, teniendo en cuenta lo indicado desde la página de la alcaldía de Bogotá[41], que complementa la regulación vigente sobre el derecho fundamental que tienen las personas de tipo natural para autorizar información personal cuando es alojada en bases de datos, los datos sensibles son todos aquellos que afectan la intimidad y privacidad del titular, un uso indebido podría provocar discriminación por lo general son datos de tipo religiosa, política, filosóficas o incluso la pertenencia a organizaciones sociales.

4.6.4 CONPES 3701 de 2011. En Tic Bogotá conpes[42], este documento genera lineamientos de política en el tema de ciberseguridad y ciber defensa enfocado en desarrollar una estrategia a nivel nacional que contrarreste el incremento de las amenazas informáticas que impacten significativamente en el país, también recolecta todos los antecedentes nacionales e internacionales y la normatividad del país relacionado al tema.

4.6.5 CONPES 3854 de 2016. De acuerdo con la fuente Colaboración DNP[43], en este documento se define la política de seguridad digital enfocada en que tanto las entidades del gobierno, los empresarios y hasta los ciudadanos incluyan una gestión de riesgos de seguridad que les permita, detectar e identificar los riesgos a los cuales están expuestos con el fin de poder protegerse y responder a los ataques cibernéticos que se pueden generar en el entorno digital.

[41] ALCALDIA DE BOGOTA. Ley 1581 de 2012 [17 de octubre de 2012]. Por la cual se dictan disposiciones generales para la protección de datos personales [en línea]. [consultado: 29 de septiembre de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[42] TIC BOGOTA. CONPES 3701 2011 [14 de julio 2011]. Lineamientos de política para ciberseguridad y ciberdefensa [en línea]. Colombia. 2011. [consultado: 4 de diciembre 2020]. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

[43] COLABORACIÓN DNP. CONPES 3854 2016 [11 de abril de 2016]. Política nacional de seguridad digital. [en línea] Colombia. 2011. [consultado: 4 de diciembre de 2020]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

4.6.6 Decreto 2693 de 2012. En función pública[44], por medio del Ministerio de las tecnologías de la información y las comunicaciones establecen estrategias de gobierno en línea en la república de Colombia como el artículo 3°: principios y fundamentos de la estrategia de gobierno en línea que se desarrollará conforme a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998 y 3° de la Ley 1437 de 2011. Sus fundamentos de estrategias constan de construcción colectiva, innovación, neutralidad tecnológica, confianza y seguridad**.**

4.6.7 Decreto 1377 de 2013. Con este decreto el gobierno nacional reglamenta algunas disposiciones con respecto a la protección de datos personales, teniendo en cuenta el documento en función pública[45], concediendo el derecho a la personas de conocer, modificar o actualizar la información recolectada y almacenada en las bases de datos, mediante la Ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia, el ministerio de industria, comercio y turismo establece que el tratamiento de los datos personales siempre debe estar legalizado por medio de un contrato suscrito entre el responsable de la información y el dueño de la actividad donde se aclare el alcance, la entidad responsable de la información tendrá que responder por los daños ocasionados al titular de los datos personales por el posible manejo inadecuado de los datos.

[44] FUNCION PÚBLICA. Decreto 2693 de 2012 [21 de diciembre 2012]. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia [en línea]. [consultado: 5 de diciembre 2020]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51198

[45] FUNCIÓN PÚBLICA. Decreto 1377 de 2013 [27 de junio 2013]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. [en línea]. [consultado: 28 de septiembre 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

5. DISEÑO METODOLÓGICO

Teniendo presente la naturaleza de este proyecto, se utilizará la metodología de investigación documental:

Una investigación documental es aquella que se desarrolla por medio de la consulta de documentos como libros, revistas, periódicos, memorias, registros, artículos con el fin de conocer los antecedentes del problema, el estado y la manera de aplicarlo al diseño documental para el desarrollo de actividades del CSIRT[46].

El desarrollo del proyecto consta de las siguientes fases:

- Análisis de la problemática: Aquí se revisa parte de la información que existe en cuanto a los ataques cibernéticos orientados a las pymes y medianas empresas del mundo a través de los años, pero en especial en Colombia.

- Selección del enfoque del CSIRT: Se define el ámbito del CSIRT para el desarrollo del proyecto, teniendo en cuenta que existen varios enfoques, para este proyecto el ámbito seleccionado es para pymes y medianas empresas porque este sector generalmente es olvidado.

- Establecer la taxonomía de ataques: Por medio de una investigación se realiza una estructura de los ataques cibernéticos más importantes y relevantes de los últimos años con el fin de poder tener una vista amplia sobre los riesgos que se pueden presentar para las pymes y medianas empresas a futuro, así mismo sirve como insumo para ofrecer soluciones y servicios a los clientes.

[46] UJAEN. Definición de diseño documental. [en línea]. [consultado: 06 de noviembre 2020]. Disponible en: http://www.ujaen.es/investiga/tics_tfg/dise_documental.html

- Definir el catálogo de servicios: En esta fase se listas los principales servicios que se ofrecerán a los clientes, este catálogo estará dividido en los servicios proactivos y reactivos los cuales serán especificados pensando en la necesidad del cliente.

- Crear políticas y procedimientos internos: En esta nueva fase se establecen los principales procedimientos internos, se define su organización y su forma en que deben operar cuando el CSIRT este prestando el servicio a los clientes, es necesario e importante recalcar que el alcance solo está enfocado a la parte administrativa.

- La última fase del proyecto consiste en elaborar las respectivas conclusiones y recomendaciones del proyecto que serán imprescindibles para la continuación del proyecto en el ámbito técnico.

6. DESARROLLO DE LOS OBJETIVOS

6.1 ACTUALIDAD DE LOS ATAQUES CIBERNÉTICOS MÁS REPORTADOS EN COLOMBIA

Con el uso frecuente de los sistemas informáticos y redes en estos últimos años, los colombianos han reportado incidentes informáticos que los ha afectado de alguna manera, según cifras de CCIT ORG[47], en el Cuadro 1 se encuentra el reporte de incidentes en Colombia desde el año 2019 a 2020 que reflejan las principales amenazas que más han generado incidentes: En este top 4, el phishing se convierte en la amenaza más reportada, la combinación de esta técnica más el desconocimiento y la desinformación a las organizaciones (especialmente las pymes y medianas empresas) la convierten en una de las más peligrosas, sin embargo, las demás que ocurren con menos frecuencia no dejan de ser una completa amenaza para los activos de las organizaciones.

Cuadro 1. Reporte de incidentes en Colombia

Reporte de incidentes en Colombia 2019 - 2020	
Nombre de la amenaza	**Porcentaje de afectación**
Phishing	42%
Suplantación de la identidad	28%
Envió de Malware	14%
Fraudes en medio de pagos en línea	16%

Fuente: CCIT.ORG. Tendencias cibercrimen [en línea]. Pág.7. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[47] CCIT ORG. Informe tendencias cibercrimen [En línea]. 2019. [consultado: 10 de noviembre 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Por el otro lado los delitos informáticos son cometidos por cibercriminales motivados por intereses económicos bien sea a organizaciones o personas civiles, el hurto por medios informáticos es el delito más reportado con unas cifras muy alarmantes, sin duda es la estrategia preferida por los ciberdelincuentes teniendo en cuenta las debilidades en los sistemas informáticos, estos datos son la base para buscar estrategias de seguridad que permitan mitigarlos a futuro. En el primer trimestre de 2020, los ciberdelitos subieron alrededor de un 39% donde la suplantación de sitios web y el robo de datos fueron los delitos que más fueron denunciados, sin duda una de las consecuencias del nuevo Covid-19 que obligó a interactuar con más plataformas digitales, incluyendo tanto a los usuarios y a las organizaciones, esta nueva etapa de la era digital ha revelado lo vulnerables que todos pueden ser en el ámbito de la seguridad cibernética, a continuación, en el Cuadro 2 se visualiza el reporte de delitos informáticos que más se presentan en Colombia durante el periodo de 2019 – 2020:

Cuadro 2. Reporte sobre delitos informáticos en Colombia

DELITOS INFORMATICOS EN COLOMBIA 2019 – 2020	
Nombre del delito	**Número de casos**
Hurtos por medios informáticos	31.058
Violación de datos personales	8.037
Acceso abusivo a sistemas informáticos	7.994
Transferencia no consentida de activos	3.425
Software malicioso	2.387

Fuente: CCIT.ORG. Tendencias cibercrimen [en línea]. Pág.7 - 8. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

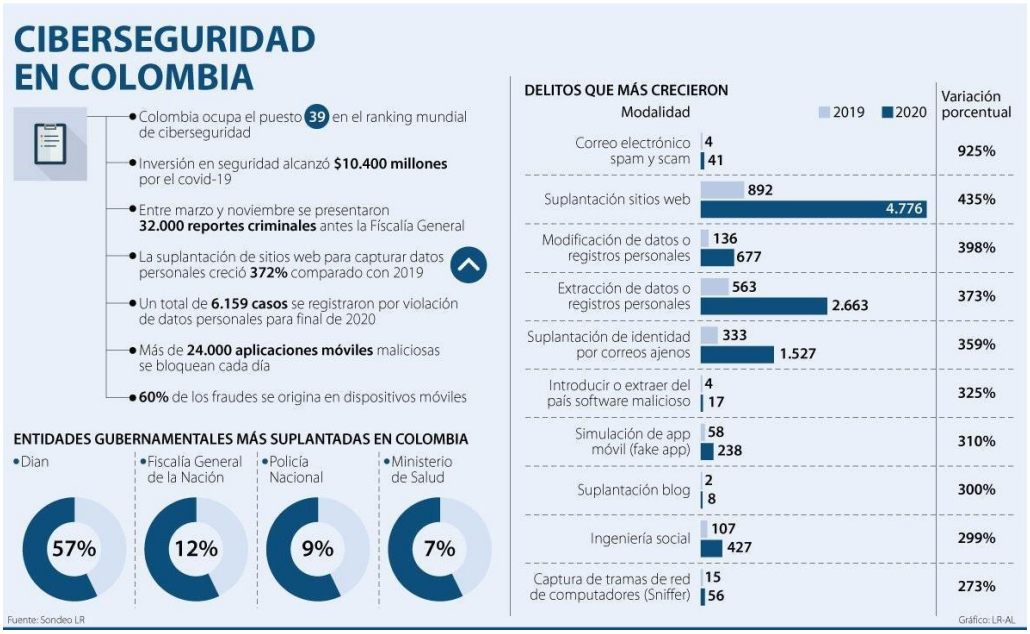
El hurto por medios informáticos es el delito más reportado con unas cifras muy alarmantes, sin duda es la estrategia preferida por los ciberdelincuentes teniendo en cuenta las debilidades en los sistemas informáticos, estos datos son la base para buscar estrategias de seguridad que permitan mitigarlos a futuro. En el primer trimestre de 2020, los ciberdelitos subieron alrededor de un 39% donde la suplantación de sitios web y el robo de datos fueron los delitos que más fueron denunciados, sin duda una de las consecuencias del nuevo Covid-19 que obligó a interactuar con más plataformas digitales, incluyendo tanto a los usuarios y a las organizaciones, esta nueva etapa de la era digital ha revelado lo vulnerables que todos pueden ser en el ámbito de la seguridad cibernética.

Colombia ocupa el puesto 39 en el ranking mundial de ciberseguridad, el sitio de asuntos legales[48], indica que, a pesar de los esfuerzos de inversión queda mucho camino para mejorar porque los ataques se han incrementado de todas las formas, incluso inimaginables, otras muy curiosas se aprovechan del momento por ejemplo los famosos correos de suplantación a nombre del ministerio de salud sobre información del Covid-19, que finalmente son técnicas para robar información.

En la Figura 8 se reflejan los datos de los delitos que más crecieron a comparación de los años 2019 – 2020, todos los delitos informáticos crecieron a comparación del año 2019, donde la suplantación de sitios web es la más destacada, estos delitos han sido potenciados por la virtualidad que emplea el mundo para acceder a las actividades cotidianas, esta información es una base para el reto de poder disminuir las cifras a futuro:

[48] ASUNTOS LEGALES. Ciberdelitos subieron primer semestre [en línea]. 2020. Colombia. [consultado: 3 de marzo de 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

Figura 8. Ciberseguridad en Colombia 2019 - 2020



Fuente: ASUNTOS LEGALES. Ciberseguridad en Colombia [en línea]. 2021. Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

Según las cifran de Infobae[49], en el año 2020 Colombia tuvo más ciberataques a comparación de años anteriores, la seguridad informática se vio comprometida sin importar los niveles, desde los datos pertenecientes a los ciudadanos hasta los servicios gubernamentales, se espera que el año 2021 sea un año más difícil en cuanto al reto de la ciberseguridad en el país.

Entre los principales riesgos que sufren las pymes se encuentran los correos basura (aproximadamente 907.000), el malware (737) y URL maliciosas (48.000), de acuerdo con Revistabye[50], as previsiones indican que las cifras de ciberataques seguirán aumentando, según el “State of Website Security and Threat Report” el 75% de las pymes cree que los ataques ocurrirán con más frecuencia en 2021.

[49] INFOBAE. 2020 año que Colombia tuvo más ciberataques [en línea]. 2021. Colombia. [consultado: 5 de marzo de 2021]. Disponible en: https://www.infobae.com/america/colombia/2021/02/25/2020-fue-el-ano-que-colombia-tuvo-mas-ciberataques/

[50] REVISTABYE. Aumento de ciberataques para las pymes españolas [en línea]. 2021. [consultado: 3 de mayo de 2021]. Disponible en: https://revistabyte.es/ciberseguridad/pymes-ciberataques/

La república[51], indica que el ministerio de trabajo comunico que en Colombia la adopción del teletrabajo aumento considerablemente hasta en un 80% durante la pandemia hacia finales del 2020, no hay comparación con los años anteriores, pero lo cierto es que esta modalidad se mantendrá por el momento, ante esta realidad los ciberdelincuentes han aprovechado la masiva conectividad para llevar a cabo sus ataques, por ejemplo se aprovechan de la situación actual y en sus ataques agregan información relacionada con las vacunas, curas o tratamientos para el COVID 19 con el fin de tener más éxito en sus ataques, incluso la organización mundial de salud (OMS) denuncio que una vez se anunció la pandemia se crearon 22.000 dominios falsos sobre servicios relacionados con la cura de la enfermedad, pero el phishing se convirtió en un enemigo letal por su eficacia para robar información confidencial, su impacto produjo más del 80% de los incidentes de seguridad en el año 2020 y adicionalmente produjo un aumento del 345% en las estafas, los ataques malware aprovecharon para ocultarse entre las redes sociales de la víctima obteniendo como resultado la encriptación de datos en un 73% de los casos, adicionalmente las organizaciones se vieron afectadas por casos de filtración de información. Los mecanismos tradiciones de seguridad se mostraron insuficientes especialmente la combinación de usuario y contraseña, las organizaciones como pymes y medinas empresas deberán adelantarse a las amenazas y fortalecer sus mecanismos de defensa ante la inminente evolución de los métodos y estrategias de los cibercriminales para el transcurso del año 2021.

[51] LA REPÚBLICA. Fraude una amenaza para la ciberseguridad [en línea]. 2021. [consultado: 5 de mayo 2021]. Disponible en: https://www.larepublica.co/internet-economy/fraude-una-amenaza-para-la-ciberseguridad-3151358

6.1.1 Establecer taxonomía de los ataques más relevantes para la actuación del CSIRT. Teniendo presente a INCIBE CERT[52], la taxonomía de ciberseguridad propuesta contiene los diferentes tipos de ataques que principalmente han afectado a las organizaciones en estos últimos años, permitiendo conocer la categoría, amenaza y su descripción.

En el siguiente Cuadro se aprecia la descripción de los principales ataques organizados por categoría, amenaza y el respectivo detalle:

Cuadro 3. Cuadro de taxonomía de ataques

Taxonomía de ataques		
Categoría	**Amenaza**	**Detalle**
Desastre	Desastre natural	Ocasionado por fenómenos naturales que no se pueden predecir.
Fallos	Configuración inadecuada	En las organizaciones hay ocasiones donde pueden operar elementos con configuraciones no adecuadas.
	Vulnerabilidades en el software	Se generan cuando se utilizan aplicaciones con credenciales débiles o usan las que vienen por defecto, así mismo como las secuencias de *exploit.*
Intercepción / obtención de la información	Reconocimiento de red	Extracción de información sobre la red, sistemas operativos, puertos, dispositivos conectados etc.
	Man in the middle	Consiste en que el atacante se ubica en el medio de una comunicación entre dos víctimas.

[52] INCIBE CERT. Taxonomía ciberataques [en línea]. España. [consultado: 6 de mayo 2021]. Disponible en: https://www.incibe-cert.es/taxonomia

Continuación

	Intercepción de información	Es una intercepción ilegal de procesos confidenciales de comunicación como correos electrónicos donde existe la posibilidad de modificar los datos.
	Secuestro de la sesión	Se trata del robo de la conexión de datos para actuar como host legítimo en la red con la intención de alterar, robar o eliminar información.
	Denegación de servicio distribuido (DDoS)	El ataque tiene como fin saturar un objetivo dejándolo inactivo por medio de varios sistemas que dirigen el ataque con varias conexiones.
Ataques	Malware	Son programas informáticos que tienen la intención de alterar sistemas y realizar acciones no autorizadas para ocasionar robos de información y daños (como el *ransomware*).
	Dirigidos	Son ataques que por lo general son efectuados con el propósito de mantenerse ocultos en la red para recolectar toda la información posible sin el consentimiento de los administradores.
	Modificación de información	El atacante no se interesa en borrar la información, en lugar de eso modificar, alterar o manipula la información con algún tipo de beneficio personal o en su diferencia para crear caos.

Continuación:

	Destrucción	Cuando los dispositivos son robados o alterados de forma física.
Ataques Físicos	Filtrado de datos	En el ataque consiguen revelar información confidencial perjudicando a la organización.
Revelación activos	Caída del servicio de red	Cuando el servicio de red en la organización es interrumpido de forma accidental o intencionada.
Fallas e interrupciones	Derechos de autor	Instalación de software protegido por derechos de autor.
Fraude	Derechos de autor	Instalación de software protegido por derechos de autor.

Fuente: INCIBE. Taxonomías de ciberseguridad [en línea]. España. Disponible: https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

6.1.2 Desastre natural. Según Geeks[53] **,** son eventos y fenómenos naturales que no se pueden predecir y que pueden generar un impacto negativo en una organización (como terremotos, sismos, tsunamis, inundaciones, huracanes, tormentas eléctricas, fuego por sobrecarga eléctrica, apagones) si no se cuenta con los planes de contingencia para recuperar el acceso al software, Hardware y la información, elementos como la nube son claves.

Esto quiere decir que los activos informáticos pueden ser averiados por alguna de las anteriores causas las cuales suelen provocar cortos circuitos,

[53] GEEKS. Recuperación ante desastre natural [en línea]. 2017. [consultado: 13 de mayo 2021]. Disponible en: https://geeks.do/que-es-la-recuperacion-ante-desastres-como-servicio-o-draas/

destrucción parcial o total de los equipos de cómputo, servidores y demás activos informáticos, normalmente con una probabilidad baja, pero con el solo hecho de que exista representa un riesgo que no se debe dejar pasar por alto.

6.1.3 Configuración inadecuada. Una mala administración y configuración de los diferentes elementos informáticos que se utilizan en las organizaciones puede causar desde fallas en el servicio, *softwareone*[54], indica hasta vulnerabilidades en los sistemas (como por ejemplo no cambiar las claves por defecto de un sistema o base de datos) donde se puede comprometer la información, los errores humanos se pueden presentar y es necesario tomar medidas preventivas.

Un ejemplo es el caso de Sony, de acuerdo con microgestio[55], donde una grieta de seguridad dejo expuestos miles de correos internos, ediciones, guiones y contraseñas de unas películas que todavía no habían sido estrenadas, aproximadamente fueron 100 GB de datos sensibles publicados, una vez se analizó el ataque se comprobó que el problema correspondía a los pobres niveles de control y políticas, lo que aprovecharon los ciberdelincuentes para infiltrarse en la red y fácilmente acceder a la información del gigante del entretenimiento. En *Godaddy*[56], indican que una configuración de seguridad incorrecta abre la puerta a que ciber delincuentes puedan acceder a datos privados o funciones de páginas web que pueden comprometer parcial o completamente el sistema, en estos casos la información podría ser alterada o robada.

[54] SOFTWAREONE. No disponibilidad en los sistemas [en línea]. 2020. [consultado: 13 de mayo 2021]. Disponible en: https://www.softwareone.com/es-co/blog/articles/2020/02/17/las-6-causas-mas-comunes-de-la-no-disponibilidad-en-los-sistemas

[55] MICROGESTIO. Tipos de riesgos de la seguridad informática [en línea]. [consultado: 14 de mayo 2021]. Disponible en: https://microgestio.com/blog/content/riesgos-de-la-seguridad-informatica/1213

[56] GODADDY. Amenazas informáticas [en línea]. 2020. [consultado: 14 de mayo 2021]. Disponible en: https://co.godaddy.com/blog/7-amenazas-informaticas-toda-pyme-debe-conocer

6.1.4 Vulnerabilidad en el software. El software es un recurso clave en la optimización de los procesos, de acuerdo con *redeszone*[57], ha facilitado la vida a muchas personas optimizando tiempos y procesos, en los últimos años su constante evolución y actualización indica que no existe una versión final porque siempre hay algún aspecto para mejorar sin embargo en el ámbito de seguridad los ciber delincuentes siempre están analizando alguna brecha para explotarla y vulnerar la información y privacidad por lo tanto siempre es recomendable tener presente todos los elementos necesarios como los estándares y las mejores prácticas de seguridad para reducir esa probabilidad de vulneración. En teoría todo el software tiene vulnerabilidades, el daño que pueda causar depende de que tan grave sea como algunas que se listan a continuación según las fuentes de enciclopedia Kaspersky[58], estas son algunos de los riesgos que pueden causar un impacto importante dentro de las organizaciones:

- Permite a un hacker ejecutar comandos como otro usuario.
- Permite a un hacker hacerse pasar por otra entidad o usuario.
- Permite a un hacker acceder a información confidencial.
- Permite a un hacker secuestrar un sistema por completo.
- Permite a un hacker detener el funcionamiento de la aplicación.
- Permite a un hacker alterar el funcionamiento normal de la aplicación.

[57] REDESZONE.NET. Vulnerabilidades del software 2020 [en línea]. 2020. [consultado: 14 de mayo 2021]. Disponible en: https://www.redeszone.net/noticias/seguridad/vulnerabilidades-software-importantes-2020/
[58] ENCYCLOPEDIA.KASPERSKY. Las vulnerabilidades del software [en línea]. [consultado: 15 de mayo 2021]. Disponible en: https://encyclopedia.kaspersky.es/knowledge/software-vulnerabilities/

6.1.5 Reconocimiento de red. En la actualidad cada vez más los ciber delincuentes utilizan estrategias más sofisticadas para atacar redes según PC actual[59], con el apoyo de herramientas hacking puede ser posible que puedan acceder a información de las redes organizacionales sin el debido permiso o consentimiento con el fin de hacerse una idea para luego producir un ataque más serio que puede ser peligroso, es ideal plantear mecanismos de defensa para aumentar el nivel de seguridad en las organizaciones, manteniendo seguro sus activos y conservando la disponibilidad, integridad y privacidad.

El reconocimiento de la red es el primer paso para un intento de intrusión, ya que el objetivo es hallar la vulnerabilidad para explotarla en el sistema víctima, los ataques de red pueden clasificarse en:

- **Ataques de reconocimiento:** Enfocada en reconocer el esquema de red de forma no autorizada incluyendo vulnerabilidades y servicios. Estos pueden ser por consultas en internet, barridos de ping, escaneos de puertos y programas detectores de paquetes.

- **Ataques de acceso:** Manipulación no autorizada de datos.

- **Denegación del servicio:** Consiste en dañar redes, servicios o en desactivarlos.

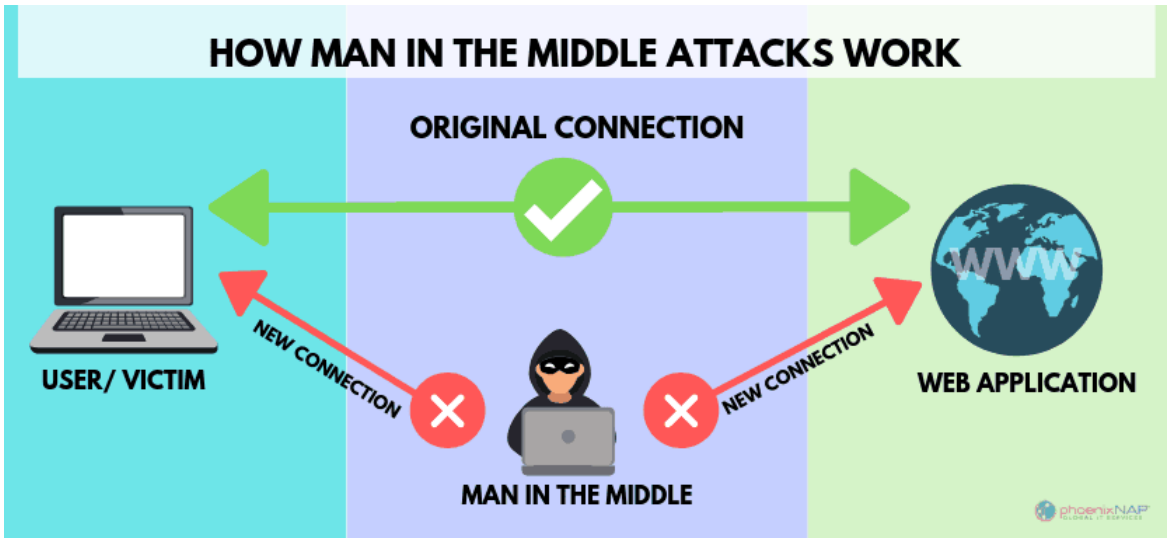
Los ciber atacantes pueden usar algunas herramientas de internet como nslookup para determinar el rango de direcciones IP asignadas en una organización, la fuente Itroque[60], indica, luego procede a realizar ping a las direcciones públicas para encontrar las direcciones activar, para más

[59] PC ACTUAL. Que es hacker. [en línea]. 2021. [consultado: 17 de mayo 2021]. Disponible en: https://www.pcactual.com/noticias/trucos/espia-conviertete-hacker-2_3708
[60] ITROQUE. Ciso Modulo 11 tipos de ataques de reconocimiento [en línea]. México. [consultado: 19 de mayo 2021]. Disponible en: http://itroque.edu.mx/cisco/cisco1/course/module11/11.2.2.2/11.2.2.2.html

eficiencia pueden disponer de herramientas como *gping,* que realiza ping sistemáticamente a todas las direcciones de una red en una subred o rango determinado.

6.1.6 Man in the middle. En godaddy[61], se refiere a un intermediario no deseado, normalmente es un software malicioso o un cibercriminal que se incrusta entre la víctima la fuente legítima de datos como por ejemplo (cuentas bancarias) el objetivo real es interceptar, leer y/o manipular la información de forma exitosa sobre la comunicación entre la víctima y sus datos sin que se den cuenta. En la Figura 9 es posible visualizar de qué manera los ciber atacantes interactúan en la interceptación de un mensaje con el fin de visualizar la información y actuar de acuerdo a su interés:

Figura 9. Explicación del ataque Man in the middle



Fuente: WALLSTREETINV. *Man in the middle* [en línea]. 2021. Disponible en: https://wallstreetinv.com/cyber-security/man-in-the-middle-attack-mitm/

[61] GODADDY. Ataque man in the middle [en línea]. 2019. [consultado: 20 de mayo 2021]. Disponible en: https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/

6.1.7 Intercepción de información. Es un ataque contra la confidencialidad de un sistema por medio de un programa, proceso o usuario que consigue acceder a los recursos que no tiene autorización, teniendo en cuenta la fuente blog de seguridad[62], este tipo de ataque es difícil de poder detectar, ya que no produce alteración al sistema. Para efectos legales la Ley "1273 DE 2009, en su artículo INTERCEPTACIÓN DE DATOS INFORMÁTICOS, la SIC[63], indica que quien viole este artículo incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses cuando se intercepte datos informáticos desde su origen, destino o en el interior de un sistema informático, así mismo en las emisiones electromagnéticas que las transporte".

6.1.8 Secuestro de la sesión. En *gb advisors*[64] , este ataque consiste en la explotación de una sesión de una computadora para obtener acceso no autorizado a la información o servicios de un sistema por medio del robo de cookies del sistema, con esto se pueden autenticar en un servidor remoto y obtener acceso al servidor, luego del robo efectivo de las cookies el atacante puede usar una técnica conocida como "*pass the cookie*" para realizar el secuestro de la sesión, las credenciales o ID de la sesión son apetecidos por los ciberdelincuentes, con este acceso puede ingresar a las aplicaciones web y suplantar a un usuario válido. Esta práctica como lo indican en *ryte*[65] , también es conocida como "*hijacking*" o secuestro que tiene como fin tomar un elemento específico del entorno de Internet a través de rutas no autorizadas, es decir además del secuestro de sesión también existen:

[62] BLOG SEGURIDAD. Tipos de ataques intercepción de información [en línea]. [consultado: 23 de mayo 2021]. Disponible en: https://blogseguridadandrea.wordpress.com/2016/11/13/4-1-tipos-de-ataques/
[63] SIC. Ley 1273 de 2009 [5 de enero 2009]. "por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". [en línea]. [consultado: 23 de mayo 2021]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
[64] GB ADVISORS. Secuestro de sesión [en línea]. 2020. [consultado: 25 de mayo de 2021]. Disponible en: https://www.gb-advisors.com/es/secuestro-de-sesion-aprende-evita-acceso-autorizado-datos/
[65] RYTE. Tipos de ataques informáticos: Hijacking [en línea]. [consultado: 25 de mayo 2021]. Disponible en: https://es.ryte.com/wiki/Hijacking#Hijacking_de_sesi.C3.B3n

- Hijacking de navegadores.
- Hijacking de DNS.
- Hijacking de URL.
- Hijacking de redes.
- Hijacking de dominios.
- Hijacking de motores de búsqueda.
- Hijacking de contenido.

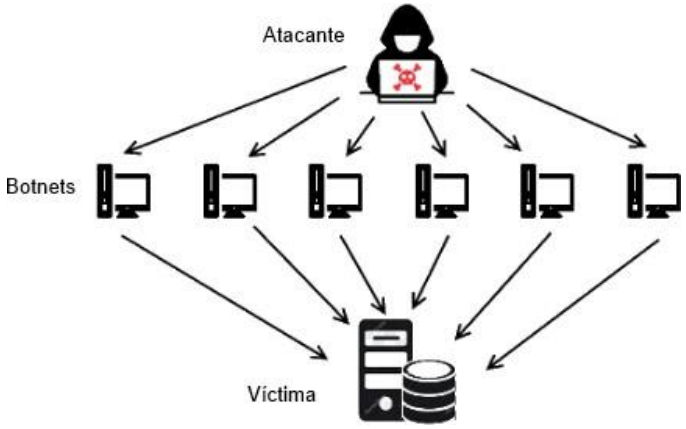
6.1.9 Denegación de servicio distribuido (DDoS). CCN CERT[66], indica que este tipo de ataque se utiliza para intentar interrumpir el normal funcionamiento de un servicio de red o cualquier servidor por medio de un número muy elevado de peticiones que provocan la caída temporal del sistema o servicio, en situaciones actuales son unas amenazas para considerar.

Entre los objetivos comunes de los ataques DDoS, Kaspersky[67], explica que se encuentran las tiendas online y cualquier organización que dependa de proporcionar servicios online, tanto los servidores web como los recursos de la red poseen un límite de solicitudes que pueden atender de manera simultánea, adicionalmente la capacidad del servidor posee un límite y el canal que conecta al servidor con la red internet también tendrá un límite de capacidad o ancho de banda, entonces cuando el número de solicitudes supera cualquier componente de la infraestructura el servicio se verá afectado y se podría reflejar en las respuestas más lentas de lo normal para las solicitudes de los usuarios o que se ignoren algunas o todas, produciendo una denegación del servicio, en algunos casos los atacantes pueden solicitar un pago para detener el ataque. En la Figura 10 se demuestra la forma en que un atacante puede manipular varias *bootnets* al mismo tiempo para enviar numerosas peticiones a un servidor con el fin de saturarlo y suspender el servicio de forma temporal o permanente:

[66] CCN-CERT. Ataques de negación recomendaciones [en línea]. 2020. [consultado: 25 de mayo 2021]. Disponible en: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/10067-ataques-de-denegacion-de-servicio-distribuido-recomendaciones-y-buenas-practicas.html

[67] KASPERSKY. Denegación de servicio distribuido DDoS Ataques [en línea]. [consultado: 28 de mayo 2021]. Disponible en: https://www.kaspersky.es/resource-center/threats/ddos-attacks

Figura 10. Ataque de denegación del servicio distribuido (DDoS)



Fuente: SEGURÍSIMOS EN LA WEB. Denegación de servicio distribuido [en línea]. Disponible en: https://segurisimosenlaweb.com.ar/denegacion-de-servicio-dos/

6.1.10 Malware. Es un software malicioso, en *latam kaspesrsky*[68], lo define como un tipo de programa informático diseñado para infectar el equipo de cómputo de un usuario legítimo y dañarlo de varias formas, se presentan de distintas maneras como por ejemplo virus, gusanos, troyanos spyware etc. Es posible que el virus sea el malware más conocido, ya que posee la habilidad de propagarse creando copias de sí mismo, otros como el spyware transmite información persona como por ejemplo de tarjetas de crédito. Algunos de los tipos de malware:

- **Ransomware:** Una vez activado bloquea el acceso a los datos del sistema, posteriormente solicita un rescate que consiste en pagar una suma de dinero en la mayoría de los casos el medio de pago predilecto es el bitcoin, sin embargo, no existe una garantía real de que una vez realizado el pago sea recuperado los archivos.

[68] LATAM KASPERSKY. What is Malware and how to protect [en línea]. [consultado: 28 de mayo 2021]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

- **Spyware:** Los programa espías tienen como fin recolectar información concreta sobre datos existentes supervisando la actividad de una persona esto incluye información de tarjetas, credenciales y todo lo relacionado con los datos privados.

- **Gusanos informáticos:** Se utilizan para ingresar a las áreas del ordenador, el proceso inicia infectando el dispositivo para luego replicarse y extenderse hacia otros dispositivos, normalmente sus fines son sobrecargar el dispositivo o integrar software malicioso para reducir la seguridad de dicho dispositivo.

- **Adware:** Consiste en la gran variedad de anuncios indeseados incluyendo juegos, barras de tareas o programas de suscripción, que se activan normalmente en los navegadores, recolectan información personal.

- **Troyanos:** En *Hornet Security*[69], indican que tiene como fin realizar un ataque encubierto para infiltrarse en el dispositivo como un software que es legítimo a primera vista. En la gran mayoría de los casos, el troyano solo se activa luego de realizar la instalación, posteriormente descarga malware adicional de forma no deseada, es muy difícil poder detectarlo.

- **Botnets:** Son una especie de dispositivos con un código asociado a ellos con la capacidad de ejecutar malware para infectar un grupo de dispositivos. En *Ret Hat*[70], también hablan de que en general las *botnets* llevan a cabo ataques de denegación de servicio distribuido (DDoS), enviar spam o realizar tareas de minería de criptomonedas.

[69] HORNET SECURITY. Base tipos y subcategorías de Malware en el mundo [en línea]. [consultado: 29 de mayo 2021]. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/malware/

[70] RET HAT. Seguridad: que es el Malware [en línea]. [consultado: 29 de mayo 2021]. Disponible en: https://www.redhat.com/es/topics/security/what-is-malware

6.1.11 Ataques dirigidos. Estos tipos de ataques tienen una planificación previa que es producido por ciberdelincuentes con un fin u objetivo específico que desean conseguir, en *Kaspersky*[71], informan que la diferencia con otro tipo de ataques es que son oportunistas de acuerdo con la vulnerabilidad que sea descubierta.

Un ataque dirigido puede ser muy peligroso y una de las principales razones consisten en que los atacantes están dispuestos a dedicar más esfuerzos y recursos para entender a su objetivo, utilizaran ataques muy sofisticados y difíciles para detectar, por ejemplo, un correo con un adjunto malicioso para instalar un Remote *Administration Toolking* (RAT), en *It Digital Security*[72] , indican que el atacante tenga claro que la recompensa puede ser alta ya sea de propiedad intelectual, secretos, información financiera o algún tipo de beneficio. Un ataque dirigido consta de seis fases:

- Fase 1: Recogida de información: Identifican y recopilan información disponible públicamente sobre el objetivo para personalizar los ataques.
- Fase 2: Punto de entrada: Se selecciona la técnica para filtrarse a la infraestructura del objetivo como por ejemplo el phishing.
- Fase 3: Comunicaciones C&C: Luego de acceder a los sistemas, se ejecutan rutinas maliciosas o recopilan información por medio de servidores de comando y control (C&C), esta comunicación permanece oculta.
- Fase 4: Movimiento lateral: Buscan por toda la red buscar información valiosa o también infectar otros sistemas importantes.

[71] KASPERSKY. Objetivo de los ataques dirigidos [en línea] [consultado: 430 de mayo 2021]. Disponible en: https://www.kaspersky.es/blog/ataques-dirigidos-que-conseguirian-sin-un-objetivo/104/
[72] IT DIGITAL SECURITY. Que es un Ataque dirigido [en línea]. 2017. [consultado: 02 de junio 2021]. Disponible en: https://www.itdigitalsecurity.es/reportajes/2017/08/que-hace-diferente-a-un-ataque-dirigido

- Fase 5: Descubrimientos de activos y datos: Luego de hallar los datos valiosos, estos se aíslan para la exfiltración con herramientas como troyanos de acceso remoto (RAT) y otras similares.
- Fase 6: Exfiltración de los datos: Consiste en la transferencia de esos datos valiosos o del objetivo planteado inicialmente de forma gradual o rápida, estos ataques suelen permanecer sin ser detectados en la red.

6.1.12 Modificación de la información. Se refiere a la información que es modificada de forma desautorizada, la fuente *Segu-Info*[73], en los datos o en el software en el sistema o red de la víctima, son más perjudícales cuando previamente han adquirido derechos de administrador lo que les otorga la capacidad de ejecutar cualquier comando para alterar, modificar, dañar o hasta borrar la información, como consecuencia puede incluso terminar dando de baja el sistema por completo.

De acuerdo con protégete[74], la seguridad de la información juega un papel muy importante porque su objetivo principal consiste en la protección de los datos, evitando su perdida y modificación no autorizada, pero hay que partir por el interés de la organización o del administrador porque las consecuencias de una información modificada pueden representar pérdidas económicas y otras consecuencias negativas.

[73] SEGU – INFO. Tipos de ataques de modificación [en línea]. [consultado: 02 de junio de 2021]. Disponible en: https://www.segu-info.com.ar/ataques/ataques_modificacion

[74] PROTEJETE. Seguridad y protección de la información [en línea]. [consultado: 03 de junio de 2021]. Disponible en: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

6.1.13 Destrucción de los activos físicos: Orientado al momento en que los activos que hacen parte del sistema informático sufren algún tipo de daño o avería de tipo físico por diferentes causas (internas, externas, voluntaria o involuntariamente) se debe evaluar el caso intentar la restauración del elemento o si contiene información poder realizar el proceso de recuperación. Los activos físicos pueden estar en riesgo de sufrir alguna afectación que se podría ver reflejado en la interrupción de los servicios que presta la organización aquí podemos incluir elementos como el aire acondicionado, suministro eléctrico, medios magnéticos como discos duros, USB, discos externos, cintas, *switches*, *routers* entre otros.

6.1.14 Filtrado de datos: En PMG-SSI CIA[75], explican que La información confidencial en las organizaciones normalmente es protegida mediante ciertos mecanismos, sin embargo, no existe un método 100% por lo que siempre existirá algún tipo de vulnerabilidad, sin embargo, si la información cae es manos equivocadas y es revelada, la organización tendrá un impacto muy alto en sus objetivos y estrategias.

Según MINTIC[76], como una filtración de datos ocurre en el momento en que se compromete un sistema, exponiéndose a una revelación de datos a un entorno desconocido, las filtraciones de datos se dan como consecuencia de ataques maliciosos con el fin de obtener información privada o confidencial para usarlos con fines malintencionados.

[75] PMG -SSI. CIA [en línea]. 2017. [consultado: 03 de junio de 2021]. Disponible en: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

[76] MINTIC. Guía de seguridad información My pimes [en línea]. [consultado: 05 de junio de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

6.1.15 Caída del servicio de red. Ionos[77], explica que en las organizaciones los servicios informáticos son indispensables, puesto que hoy en día todo se realiza a través de estos, con el uso de la red internet y de las nuevas tecnologías que surgen día a día de igual forma se generan riegos que pueden terminar en la caída o en la interrupción de los servicios de red, que pueden ser causados a nivel interno (corte de luz, incendios, fuego etc.) o nivel externo (ciberdelincuentes, ataques, virus etc.) en ese escenario lo más importante es poder restablecer el servicio lo más pronto posible, puesto que puede representar pérdidas económicas y de prestigio. En *Medux*[78], explican que las caídas de red pueden ocurrir en cualquier momento y estas pueden ser las causas:

- **Congestión de la red**: Debido a que demasiados usuarios de la red intentan acceder al mismo tiempo generando la reducción de calidad en el servicio, bloqueos y lentitud.

- **Fluctuación de la velocidad del proveedor de internet:** Sucede cuando la velocidad de la red sufre una conexión de velocidad inestable, puede deberse a la falta de optimización de la red o incluso a los servicios del proveedor.

- **Fallo del equipo:** Puede presentarse debido a problemas técnicos, de hardware, configuración e incluso pueden ser vulnerables a las sobrecargas.

- **Errores de funcionamiento:** Se incluyen a configuración incorrecta, cortafuegos o a daños de cableado entre otras.

[77] IONOS. Servidor caído: riesgos, efectos y prevención [en línea]. 2020. [consultado: 07 de junio de 2021]. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/servidor-caido-que-hacer/
[78] MEDUX. Why do Services outages happen [en línea]. 2021. [consultado 08 de agosto 2021]. Disponible en: https://medux.com/es/why-do-service-outages-happen/

- **Problemas de enrutamiento:** En algunas redes complejas los protocolos de enrutamiento no están instaladas o configuradas adecuadamente, llegando a generar apagones.

6.1.16 Fraude – Derechos de autor. De acuerdo con la fuente informática jurídica[79], Internet ha facilitado el acceso a la información, compartir datos, imágenes, libros, etc. todo esto con solo dar clic. Es tan fácil obtener, copiar, compartir, descargar la información que no hay límites a la hora de navegar. La protección de los derechos de autor y la propiedad intelectual en internet se ha convertido en un tema de discusión, esto, con el fin de implementar políticas para salvaguardar las diferentes creaciones que se encuentran publicadas en internet. En la Figura 11 están plasmados los diferentes tipos de plagio y las sanciones contempladas en la ley 23 de 1982 que pueden aplicarse de acuerdo con los derechos de autor de tipo moral y patrimonial:

Figura 11. Aspectos relevantes sobre el derecho de autor

Fuente: ASUNTOS LEGALES. Derechos de autor [en línea]. 2019. Disponible en: https://www.asuntoslegales.com.co/actualidad/por-hacer-plagio-puede-pagar-hasta-ocho-anos-de-prision-y-multas-de-hasta-1000-salario-minimos-2907914

[79] INFORMATICA JURIDICA. Colombia y los derechos de autor en internet [en línea]. [consultado: 09 de junio de 2021]. Disponible en: http://www.informatica-juridica.com/trabajos/colombia-y-los-derechos-de-autor-en-internet/

En asuntos legales[80], Penalmente, por el hecho de la violación a derechos morales tiene penas de prisión desde los treinta y dos (32) hasta los noventa (90 meses y multas desde los 26,66 a 300 Smmlv), por otro lado, si se violan los derechos patrimoniales del autor las penas son prisión y van desde cuatro (4) a ocho (8) años y multas de 26,66 a 1.000 Smmlv.

6.2 CARACTRIZAR EL CATÁLOGO DE SERVICIOS PROACTIVOS Y REACTIVOS DEL CSIRT PARA OFRECER A SUS CLIENTES

A continuación, se presentan los servicios TI del CSIRT, que se ofrecen a los clientes de manera clara, precisa y detallada.

6.2.1 Servicios Proactivos del CSIRT. Los servicios proactivos permiten realizar el análisis para tomar medidas de manera anticipada con la finalidad de minimizar la materialización de incidentes por medio de las implementaciones estratégicas de seguridad, el Cuadro 4 contiene los servicios disponibles y su respectiva descripción:

Cuadro 4. Servicios proactivos

Catálogo de servicios proactivos	
Servicio	**Detalle**
Monitoreo	Contiene la detección y prevención de intrusos.
Análisis de vulnerabilidades	Como Pentests de forma remota o en sitio.

[80] ASUNTOS LEGALES. Plagio penas de prisión y multas [en línea]. 2019. [consultado: 11 de junio 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/por-hacer-plagio-puede-pagar-hasta-ocho-anos-de-prision-y-multas-de-hasta-1000-salario-minimos-2907914

Continuación:

Concientización	Capacitación de forma presencial o remota para tratar los temas de ciberseguridad actuales con el fin de compartir información y medidas que son útiles para utilizar los sistemas de forma segura.
Contingencia	Métodos de respaldo y planes estratégicos para la continuidad del negocio.
Anuncios	Informa, comunica y difunde toda la información relacionada con la ciberseguridad actual, advirtiendo sobre nuevas amenazas.
Mejores prácticas	Metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT. Los controles adecuados para las vulnerabilidades se realizan de acuerdo con los estándares ISO/IEC 27002:2013.

Fuente: CCN CERT. Guía creación de un CERT- CSIRT. [en línea]. Pág.25. 2011. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

6.2.2 Monitoreo. Incluye la orientación, implementación y verificación de sistemas de monitoreo, de acuerdo con Incibe[81], un IDS está diseñado para proporcionar alertas ante un incidente potencias lo que permite al analista investigar el evento y determinar si requiere de acciones más puntuales, mientras que un IPS toma medidas por sí mismo para bloquear intentos de intrusión, estos dos sistemas son importantes para la ciberseguridad, el uso de ambos es un complemento adecuado recomendado para las organizaciones, a continuación su respectiva definición

- IDS: (Intrusion Detection System) (sistema de detección de intrusiones) es una aplicación utilizada para detectar accesos no autorizados a un ordenador o a una red, su funcionamiento básico consiste en monitorear

[81] INCIBE. Para que sirven los IDS e IPS [en línea]. 2020. [consultado: 13 de junio 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

el tráfico entrante para compararlo con una base de datos que contiene información de los ataques conocidos, si encuentran alguna actividad sospecho emiten una alerta.

- IPS: *(*Intrusion Prevention System) (sistema de prevención de intrusiones) es un software que se utiliza para evitar ataques e intrusiones, su actuación es de tipo preventiva, el análisis se realiza en tiempo real para determinar si se va a producir un incidente.

6.2.3 Análisis y vulnerabilidades. Enfocado en el análisis de vulnerabilidades los cuales cuenta con los siguientes ítems:

- Escaneo de red LAN.
- Escaneo de red wifi.
- Firewall.
- Usuarios y contraseñas.
- Cifrado.
- Spyware.
- Software.
- Páginas web.
- Antivirus.

Con la respectiva identificación de cada uno de los puntos se propondrá un conjunto de soluciones y recomendaciones con el fin de cerrar esas brechas de seguridad detectadas y de esta manera minimizar el impacto de futuras amenazas a la infraestructura de la organización, por ejemplo, la utilización de mecanismos seguros de comunicación como la VPN es fundamental para el desarrollo del trabajo desde casa, sugerencias para cambiar los puertos y contraseñas por defecto o la implementación de doble autenticación para acceder a los servicios digitales.

6.2.4 Concientización: Es fundamental para la seguridad de la información, ya que, en sí, se trata de la sensibilización de los usuarios, actualizando los conocimientos se puede afrontar las amenazas que surgen cada día, para ellos es necesario realizar la formación del personal por medio de los siguientes ítems con el fin de generar una cultura para la ciberseguridad:

- **Capacitación Virtual:** Por medio de la plataforma de preferencia como *teams,* Skype, o la acordada, un experto en temas de seguridad informática, realizará una capacitación virtual con el fin de informar, aconsejar y resolver todas las inquietudes que se presenten por parte de los clientes.

- **Capacitación Presencial:** Un experto en temas de seguridad realizará la visita a la sede del cliente donde podrá informar, aconsejar y resolver todas las inquietudes de los clientes.

- **Cursos Informativos (virtual):** Para acceder a estos cursos el cliente recibirá unas credenciales para poder acceder a una plataforma, que cuenta con cursos informativos orientados a la seguridad informática para clientes con que no tengan conocimiento.

- **Cursos Básicos (virtual):** Para acceder a estos cursos el cliente recibirá unas credenciales para poder acceder a una plataforma, que cuenta con cursos informativos orientados a la seguridad informática para los clientes que cuenten con un conocimiento básico.

6.2.5 Contingencia. Inspección de los planes de contingencias para fortalecerlos, o desarrollarlos con el fin de conservar la continuidad del negocio, los servicios y los procesos de tecnologías de las comunicaciones y la información, ante alguna emergencia o siniestro que pueda representar la interrupción parcial o total, se consideran todos los componentes del sistema y los recursos auxiliares como:

- Seguridad y migración a la nube.
- Copias de seguridad.
- Suministro de energía eléctrica.
- Documentación.
- Hardware.
- Pólizas.
- Red.

6.2.6 Anuncios. El CSIRT ofrecerá información sobre temas de ciberseguridad obtenida y recopilada de reconocidas fuentes distribuidas de la siguiente manera:

- **Boletín de vulnerabilidades:** Se incluirán temas y tips acerca de la forma de actuar para prevenir fallos en los sistemas informáticos.

- **Ciberseguridad al día**: Semanalmente se brindará información sobre los temas actuales de la ciberseguridad.

- **Malware al día:** Semanalmente se brindará información sobre los temas actuales referentes a malware, virus y demás amenazas que circulan en las redes.

6.2.7 Mejores prácticas: Aplicar las siguientes metodologías que incluyen las mejores prácticas y procesos para fortalecer los procedimientos orientados a la seguridad informática y de la información de los clientes, un profesional del área acompañará al cliente en todo el proceso de inicio a fin:

- Metodología de análisis y gestión de riesgos de los sistemas de información, que incluye el proceso de la valoración de los activos utilizando MAGERIT, realizada por personal especializada con experiencia. Una parte fundamental dentro de la gestión de la seguridad de la información es conocer y controlar los riesgos a los cuales está expuesta la información de la compañía.

- Aplicación de los controles a las falencias evidenciadas por medio de la norma ISO/IEC 27002:2013, esta incluye los controles que buscan mitigar el impacto o la posibilidad de ocurrencia sobre los deferentes riesgos a los que se expone la organización.

- Aplicación de la norma ISO 27032, enfocada en el uso de buenas prácticas en materia de la seguridad de la información, teniendo en cuenta las herramientas necesarias para gestionarla, adicionalmente cuenta con los ejes de la seguridad de redes, seguridad de internet y sobre la protección de infraestructuras críticas de la información para el cliente.

6.2.8 Servicios reactivos del CSIRT. En CCSIRT Policía[82], indican que los servicios reactivos son las respuestas que se dan de manera inmediata cuando ocurren los incidentes cibernéticos que buscan la estrategia para reaccionar de manera adecuada, acertada y en el menor tiempo posible con el fin de reducir el impacto y que el servicio del cliente pueda reanudarse. En el Cuadro 5 están plasmados los servicios ofrecidos por el CSIRT, están determinados por gestión de incidentes en el que se presentan las principales actividades y en CSIRT donde se encuentran las actividades complementarias:

[82] CCSIRT POLICIA. Servicios reactivos [en línea]. Colombia. [consultado: 25 de junio 2021]. Disponible en: https://cc-csirt.policia.gov.co/servicios/servicios-reactivos

Cuadro 5. Servicios reactivos

Catálogo de servicios reactivos	
Gestión de incidentes.	- Respuesta remota. - Análisis y asesorías. - Respuesta en sitio. - Servicio forense.
CSIRT	- Determinar posibles causas del incidente - Coordinación - Reportes

Fuente: CNN CERT. Servicios reactivos [en línea]. 2011. Pág. 25. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

6.2.8.1 Respuesta remota. Si el cliente lo requiere y es posible se puede realizar la gestión por la vía virtual, para este proceso es necesario que algún encargado o responsable del área de tecnología de la empresa solicitante acompañe todo el proceso para facilitar la operación porque eventualmente se necesitará información, datos, permisos con el fin de mitigar o solucionar la vulnerabilidad detectada.

6.2.8.2 Análisis y asesorías. Cualquier cliente (pymes o mediana empresa) puede solicitar la colaboración del CSIRT en el momento que sea víctima de un ataque, el equipo realiza la asistencia contactando a la organización o a los implicados con el incidente, el implicado debe presentar todos los datos necesarios para poder sugerir medidas con el fin de restablecer el servicio y la seguridad en el sistema atacado.

Es importante aclarar que el CSIRT mantendrá bajo confidencialidad cualquier tipo de información relevante que sea necesario saber para actuar eficazmente. Para solicitar el incidente será necesario realizar una llamada o en su diferencia ingresar una solicitud / incidente por medio de un aplicativo web, con el fin de que el CSIRT pueda iniciar la gestión.

6.2.8.3 Respuesta en sitio. Si el cliente lo requiere o si la situación lo amerita se asiste a la sede del cliente de manera presencial para realizar el respectivo análisis, la gestión y brindar la solución, el acompañamiento por parte de algún miembro del área de tecnología por parte del cliente es clave para facilitar la operación. Teniendo en cuenta que la atención se realiza a nivel nacional, es posible que existan algunos casos donde el personal que se movilice hasta el sitio del cliente se pueda retrasar (por distancias extensas o motivos ajenos) por lo que el CSIRT, recomienda inicialmente optar por la respuesta remota si el impacto del incidente es muy crítico.

6.2.8.4 Servicio forense. El CSIRT contará con el servicio forense especializado con el fin de apoyar, orientar y solucionar algunas actividades como:

- Recuperación de información y particiones eliminadas de medios digitales, bien sea por virus, fallas eléctricas, daños físicos o cifrado de *ramsomware.*
- Recuperación y examinación de datos de los dispositivos electromagnéticos.
- Diseño de procedimientos en una presunta escena del crimen informático.
- Realización de análisis de evidencias legales.
- Generación de informes forenses informáticos sobre el proceso de investigación.

- El servicio forense aplica para sistemas operativos, redes, la nube y dispositivos móviles.

6.2.8.5 Determinar posibles causas del incidente. El equipo del CSIRT recopilara toda la información que el cliente suministre junto con el diagnóstico inicial, luego se realizara el seguimiento para poder determinar la posible causa que genero el incidente de ciberseguridad y/o los responsables, cuando la investigación finalice y la incidencia se halla controlado se confirmará la causa que desencadenó la falla o el agujero de seguridad y al mismo tiempo se indicara de qué forma se podrá tratar.

6.2.8.6 Coordinación. El equipo del CSIRT podrá facilitar el contacto con otro tipo de entidades o departamentos de seguridad a cargo del manejo de investigaciones legales y judiciales, así mismo con otro tipo de entidades que puedan estar involucrados en el incidente, también incluirá comunicación con proveedores de internet (ISP), y comunicación con CSIRT internacionales dependiendo los casos.

6.2.8.7 Reportes. El equipo del CSIRT, generará un reporte luego de que el incidente esté controlado y resuelto, en donde se podrá visualizar información como el origen, la causa, el riesgo presentado, los daños si aplica, las recomendaciones para evitar que vuelva a ocurrir el incidente, el tiempo, las estadísticas, las conclusiones y la solución definitiva bien sea para eliminar la causa y/o fortalecer los mecanismos de ciberseguridad de la organización.

Para la gestión de los incidentes se tendrán presente los siguientes ítems:

6.2.9 La evaluación: Teniendo en cuenta la fuente de MINTIC [83] , para evaluar un incidente de seguridad se deben tener presente los niveles de impacto y la clasificación de los activos de información de la organización. Niveles de impacto:

- **Alto Impacto:** Este tipo de incidente afecta los activos de información los cuales son considerados con impactos críticos y que influyen directamente en los objetivos de la organización.

- **Medio Impacto:** Este tipo de incidente afecta los activos de información los cuales son considerados con impactos moderados y que influyen directamente en los objetivos de la organización.

- **Bajo impacto:** Este tipo de incidente afecta los activos de información los cuales son considerados con impactos insignificantes y que no influyen directamente en los objetivos de la organización.

6.2.10 Clasificación de los incidentes: De acuerdo con los servicios ofrecidos en el Cuadro 6 se encuentra plasmada la clasificación de los incidentes importante para la categorización:

Cuadro 6. Clasificación de incidentes

Clasificación de incidentes		
Clasificación	**Tipo de incidentes**	**Detalle**
Disponibilidad	Dos	Denegación del servicio, incluye denegación distribuida.
	Interrupciones del servicio	Cuando el servicio es cortado por alguna causa ajena.
	Configuración	Cuando la configuración es errónea y es necesaria la orientación.

[83] MINTIC. Guía para la gestión y clasificación de incidentes de seguridad [en línea]. Pág.15 [consultado: 29 de junio 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Continuación:

Información	Escaneo de red	Solicitudes e intentos de analizar y obtener información de la red para visualizar vulnerabilidades.
	Análisis de paquetes	La visualización del tráfico de redes y posible alteración.
	Acceso no autorizado (revelación de información)	Cuando acceden a la información sin consentimiento de la organización.
	Modificación no autorizada	Cuando acceden y alteran la información sin el consentimiento de la organización.
	Ingeniería social	Obtención de información sin el uso de la tecnología.
Infección	Malware	Cuando el sistema ha sido infectado por cualquier tipo de amenazas como virus, ramsonware, spyware, etc.
Contenido inapropiado	SPAM	Cuando llegan correos en cantidades desbordadas de manera inesperada.
	Contenido discriminatorio / sensible	Orientado al contenido difamatorio, a la violencia, racismo, pornografía infantil, incitación al odio.
Intrusión	Credenciales	Cuando han intentado o ingresado utilizando ataques como fuerza bruta.
	Aplicaciones	Cuando han intentado o ingresado a las aplicaciones utilizando ataques como inyecciones SQL.
	Privilegios	El sistema ha sido comprometido por alguna cuenta con privilegios.
	Ataque desconocido	Algún ataque o acceso desconocido hacia la red.
Fraude	Derechos de autor	Divulgación de información sin ninguna autorización por ejemplo en Taringa.
	Suplantación	Técnica usada para hacerse pasar por el titular y obtener beneficios.
	Phishing	Técnica para llevar a la víctima a revelar información o datos importantes.

Continuación:

Forense	Recuperación de información	Recuperación de Información borrada accidental o intencionalmente.
	Investigación legal	Cuando se requiere una investigación en la organización que requiera obtención y análisis de las evidencias digitales que permitan fundamentar una pretensión ante los tribunales.
Capacitación	Concientización	Charlas, actualización y trasferencia del conocimiento sobre el estado actual de la ciberseguridad y amenazas actuales.
	Cursos	Cursos básicos o específicos a elección del cliente.
Otros	Otros	Cualquier tipo de incidente que no esté presente.

Fuente: CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciber incidentes [en línea]. Pág.14. Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

6.2.11 Tiempos de respuesta y la priorización: La atención especializada, adecuada y eficiente se establece por el nivel de prioridad del incidente, para brindar la solución se cuentan con las variables de prioridad, criticidad de impacto, impacto actual e impacto futuro.

El nivel de prioridad: Este valor depende de la importancia que le ha otorgado la organización (cliente) y la relación con los sistemas afectados, en el Cuadro 7 se encuentran establecidos los niveles de criticidad, su ponderación y el detalle que explica el criterio a tener en cuenta para seleccionar el nivel que aplique a determinada situación del incidente:

Cuadro 7. Nivel de criticidad del impacto

Nivel de criticidad	Ponderación	Detalle
Superior	1,00	Critico (sistemas que impactan totalmente el negocio).
Alto	0,75	Impacta el área de tecnología.
Medio	0,50	Sistema que apoya varias dependencias.
Bajo	0,25	Sistema que apoya una dependencia.
Inferior	0,10	Impacta estaciones de trabajo no críticos.

Fuente: CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciber incidentes [en línea]. Pág.20. Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

- **Criticidad del impacto:** Es conformado por las variables impacto actual e impacto futuro las cuales están definidas:

- **Impacto actual:** Depende en gran medida del daño causado por el incidente.

- **Impacto futuro:** Depende en gran medida del daño que puede causar el incidente si este no es tratado.

  En el Cuadro 8 se visualizan los niveles de impacto (donde superior es el más crítico e inferior el menos crítico), la ponderación que se aplica a cada caso y el detalle que describe de forma general cada tipo de impacto para cada ítem:

Cuadro 8. Nivel de impacto actual y futuro

Nivel de impacto	Ponderación	Detalle
Superior	1,00	El impacto es alto en uno o más componentes del sistema.
Alto	0,75	El impacto es moderado en más de un componente del sistema.
Medio	0,50	El impacto es alto en un componente del sistema.
Bajo	0,25	El impacto es moderado en un componente del sistema.
Inferior	0,10	El impacto es leve en un componente del sistema.

Fuente: CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciber incidentes [en línea]. Pág. 22. Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

La prioridad estaría compuesta por la siguiente fórmula: **Nivel de prioridad** = (impacto actual * 2,5) + (impacto futuro * 2,5) + (criticidad del impacto * 5), el resultado es comparado con el siguiente cuadro, que define la priorización del incidente, en el Cuadro 9 están reflejados los niveles de priorización y su respectivo valor donde superior tiene la mayor ponderación e inferior tiene la menor ponderación:

Cuadro 9. Nivel de priorización

Nivel de priorización	Valor
Superior	7,50 – 10,00

Continuación:

Alto	5,00 – 7,49
Medio	3,75 - 04,99
Bajo	2,50,- 3,74
Inferior	0,0 – 2,49

Fuente: INCIBECERT. Guía Nacional Gestión de Ciber incidentes [en línea]. Pág.31. Disponible en: https://www.incibecert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

6.2.12 El tiempo de respuesta. Es el tiempo en que un incidente de acuerdo con su criticidad e impacto debe ser atendido por el equipo del CSIRT, en el Cuadro 10 se puede visualizar de forma detallada el nivel de prioridad y su respectivo tiempo de respuesta donde la prioridad superior deberá ser atendida en máximo 10 minutos y la prioridad inferior deberá ser atendida en máximo 4 horas:

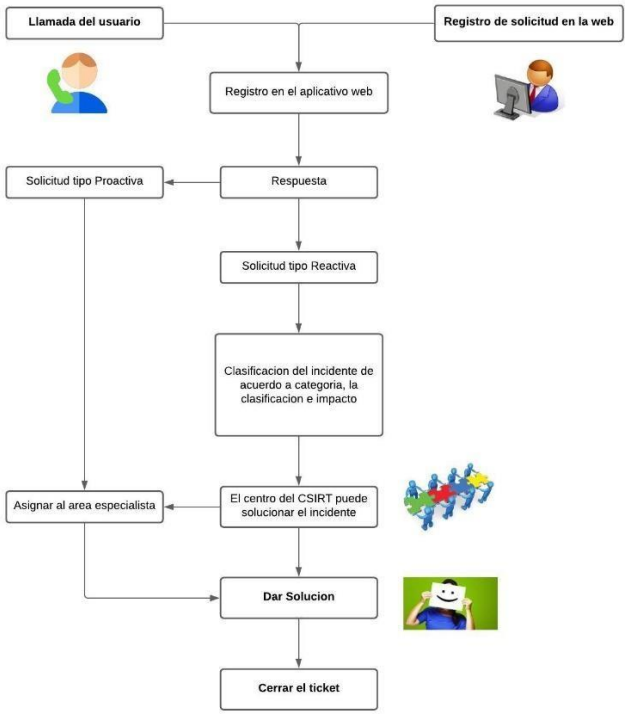
Cuadro 10. Tiempo de respuesta

Prioridad	**Tiempo de respuesta**
Superior	10 minutos.
Alto	20 minutos.
Medio	1 hora.
Bajo	2 horas.
Inferior	4 horas.

Fuente: INCIBECERT. Guía gestión de Ciber incidentes [en línea]. Pág.27. Disponible en: https://www.incibecert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

6.2.13 Procedimiento para solicitar un incidente. Para solicitar el incidente el cliente tiene dos opciones la primera: puede acceder a la página web: https://CSIRTpymesymedianas.com.co. Ingresar las credenciales de usuario y clave que son asignadas al cliente, posteriormente deben ingresar todos los datos solicitados para generar un número de ticket. La segunda opción para solicitar el incidente consiste en llamar a la línea de teléfono indicada, uno de los técnicos atenderá su incidente/solicitud, en este proceso al igual que el anterior se deben suministrar algunos datos claves para finalizar el proceso y generar un número de ticket. La atención será 24 * 24 los 7 días por la semana, el servicio siempre opera para los clientes, la Figura 12 contiene el proceso de atención a los incidentes por medio del flujo que se inicia en la notificación por parte del usuario:

Figura 12: Proceso de atención para los incidentes



Fuente: Elaboración propia

6.3 FORMULAR POLÍTICAS Y PROCEDIMIENTOS OPERACIONALES DEL CSIRT PARA QUE SEA ADOPTADO Y APLICADO POR EL PERSONAL.

6.3.1 Políticas y controles de tratamiento de información. Las políticas y controles para el tratamiento de la información son las siguientes:

- Será de total obligación el respectivo celo y reserva en el tratamiento de la información bien sea física o digital que se tenga que gestionar en las instalaciones del cliente por parte del equipo del. CSIRT.

6.3.2 Clasificación de Información: Para la clasificación de la información es indispensable poder conocer el tipo y el responsable de la misma, existen diferentes medios y formatos donde puede estar almacenada la información:

- Bases de datos.
- Dispositivos de almacenamiento (Discos duros, USB).
- Tipo electrónicos.
- Correo electrónico.
- Formato físico o papel.

Existen cuatro (4) niveles para la clasificación de la información:

- Confidencial: Cuando la información es secreta, no es conocida y tiene un valor comercial.

- Restringido: Cuando la información solo es accesible para ciertas personas.

- Uso interno: Cuando la información es accesible para todos los miembros de alguna organización.

- Público: Cuando la información es accesible para cualquier persona que pertenezca o no a la organización.

6.3.3 Protección de datos. Al momento en que un incidente es generado por un cliente, se obtendrán algunos datos privilegiados del cliente, así mismo al momento de que algún miembro del CSIRT deba acceder a las instalaciones físicas del cliente, es posible que deba realizar algún tipo de interacción con algún elemento que contenga información sensible, por lo que es de vital importancia aclarar que:

- Los datos del cliente pueden ser recopilados al momento de generar un incidente o en otro tipo de circunstancias que se requieran, pueden contener, nombres, responsables, dirección, teléfonos, correos, IP, y otros, todos estos datos serán totalmente reservados, no serán publicados por ningún motivo hacia terceros.

6.3.4 Retención de Información. Para el proceso de retención de la información se enfocará en el registro dejado en los sistemas para cerrar los tickets de incidencias, estas contienen la descripción del diagnóstico, solución y evidencias que puedes ser desde firmas de los clientes hasta fotografías.

6.3.5 Destrucción de Información. Para la destrucción de información se deberá seguir el siguiente procedimiento cuando la situación lo amerite con el fin de garantizar la total confidencialidad de los datos sabiendo que en la actualidad existen herramientas potentes para la recuperación de información:

- **Información no sensible:** Haciendo referencia a toda esa información que no posee un valor significativo se podrá eliminar de la manera tradicional, sin necesidad de recurrir a herramientas especializadas.

- **Información sensible:** Si llegado al caso se debe eliminar alguna información que posee algún valor de tipo confidencial se deberá eliminar de forma segura utilizando un software llamado *eraser* con el fin de garantizar que esa información no sea recuperada con algún método.

6.3.6 Divulgación de la información. El CSIRT tendrá como política reservar cualquier tipo de información relacionada con los sistemas informáticos del cliente, no será compartida a terceros en ninguna circunstancia, por el otro lado a nivel interno la divulgación de la información se dará de acuerdo con el contexto de manera responsable. Para garantizar la confidencialidad de la información en la sede del CSIRT contra los proveedores se dispondrá de un formato el cual deberá ser leído y firmado antes de iniciar cualquier tipo de actividad.

6.3.7 Acceso a la información. Para el acceso a la información, se establecerán roles de los cuales cada integrante del equipo será parte teniendo presente su función, las bases de datos donde se almacena información de los clientes no podrá ser accedida a todos los usuarios. Así mismo se adaptarán los niveles de crear, editar, eliminar y visualizar. La información que sea tipo confidencial será cifrada totalmente para establecer un mayor nivel de seguridad.

Para el teletrabajo en caso de que el funcionario deba acceder a la red institucional el procedimiento a seguir una vez autorizado el acceso será única y exclusivamente mediante VPN. Teniendo presente que los integrantes del equipo atenderán incidentes a nivel nacional y en muchas ocasiones deberán atender incidentes de manera presencial o de acuerdo con la situación que lo requiera. La seguridad física también hace parte de las políticas del CSIRT, es necesario establecer mecanismos de autenticación y registro como los sistemas biométricos para el cuarto de servidores con el fin de evitar que personas sin autorización puedan ingresar.

6.3.8 Uso apropiado de los sistemas del CSIRT. El CSIRT contará con sistemas y herramientas que están destinadas a prestar un servicio a los clientes, por lo tanto, su uso debe ser exclusivo para todas esas actividades relacionadas, la responsabilidad de los integrantes del CSIRT tiene un alto impacto por lo que se recalcara siempre, un uso apropiado de los recursos permite evitar incidentes en el proceso y facilita el alcance de los objetivos, brindando eficiencia y seguridad. Por niveles de seguridad:

- Cuando un funcionario del CSIRT se retire de la organización, su usuario deberá ser deshabilitado en cada aplicación o herramienta en la que operaba por ejemplo el correo, el usuario, el acceso a las bases de datos, a las carpetas compartidas etc.

- Cuando un funcionario se retire del CSIRT, deberá brindar la información institucional al jefe directo, así mismo informar sobre el estado de todas las actividades que ejercía.

- No estará permitido el ingreso a todas las páginas web.

- La instalación de software está prohibida, solo se podrá disponer algunas máquinas de prueba para tal fin.

- El uso de las licencias de software será única y exclusivamente para los dispositivos que pertenecen al CSIRT.

- Se implementará el uso de wifi para funcionarios, sin embargo, la red estará oculta y su activación se realizará por solicitud y por medio de la dirección MAC, no existirá red inalámbrica para visitantes.

- El aseo y el orden en los puestos de trabajo también es responsabilidad de los funcionarios.

- El servicio de correo institucional será única y exclusivamente para los temas laborales.

- Cada funcionario será responsable de la integridad de la información almacenada en su ordenador asignado, será habilitado una herramienta como *One drive* para realizar la respectiva copia de seguridad.

- Los equipos escritorios no tendrán puertos USB habilitados.

6.3.9 Definición de incidentes de seguridad y política de eventos. Para la definición de incidentes de seguridad se tendrán en cuenta el impacto que genera con respecto a la seguridad de la información, aquí se incluye la confidencialidad, integridad y disponibilidad.

La política de eventos estará enfocada en la mejora continua, se llevará a cabo el respectivo análisis entendiendo que en la guía ISO/IEC 73 [84], define evento como un acontecimiento que cambiaría un conjunto particular de circunstancias, es un tipo de cambio que no presenta resultados negativos, Se abordará cada caso particular con el fin de fortalecer las políticas con el fin de mantener la operatividad y la seguridad tanto en la organización del CSIRT como en el servicio que se les presta a los clientes.

6.3.10 Gestión de incidentes. La gestión de incidentes se llevará a cabo de la siguiente manera: el procedimiento se inicia con la revisión de los casos que se encuentren registrados en la plataforma o sistema de gestión de incidentes, posteriormente se tipifica, se asigna al área correspondiente para su respectiva solución.

[84] PMG-SSI. Diferencia entre evento e incidente [en línea]. [consultado: 10 de julio 2021]. Disponible en: https://www.pmg-ssi.com/2016/09/iso-27001-diferencia-entre-evento-e-incidente/

En el Cuadro 11, se encuentran documentadas las cinco (5) fases desde que se recibe un incidente hasta que se finaliza con su respectiva descripción y el responsable:

Cuadro 11. Procedimiento gestión de incidentes

No	Fase	Descripción	Responsable
1	Asignar	Se verifican los incidentes que se encuentren alojados en el aplicativo de mesa de ayuda, con este sistema se podrá observar la prioridad, es necesario que los integrantes del equipo puedan escalar los tickets rápidamente.	Técnico de soporte de primer nivel.
2	Atender	Cada grupo de nivel de soporte incluyendo los especialistas recibirán el ticket con el fin de revisarlo, analizarlo y atenderlo: Revisarlo: Identifica si corresponde a su área, si por ejemplo llegara un ticket de informática forense a un ingeniero nivel 1, entonces deberá devolverlo, notificar para que sea asignado al especialista correspondiente. Analizarlo: Una vez verificado que corresponde al área o especialidad, se procede a revisar todos los detalles y la información que contenga el ticket para tener una idea inicial y de ser necesario alistar las herramientas necesarias. Atenderlo: De acuerdo con el tipo de caso se contactará con el cliente para saber la forma en que se atenderá el caso (virtual o en sede) y de este modo atender el cliente. En algunos casos es posible que la magnitud del incidente exija que sea atendido por dos o más ingenieros o especialistas.	Ingenieros nivel 1, 2, y especialistas.

Continuación:

3	Solucionar	Una vez se realice la asistencia vía remota o en sitio y se solucione el incidente se procederá con la respectiva documentación del caso indicando el proceso y todos los detalles importantes, preferiblemente dejar una evidencia como una fotografía.	Ingenieros nivel 1, 2, y especialistas.
4	Confirmar	Los tickets tendrán un total de 48 horas luego de brindar solución para cerrarse totalmente, es decir que si en menos de 48 horas la solución planteada no ha sido suficiente se podrá retomar el caso.	Ingenieros nivel 1, 2, y especialistas.
5	Finalizar	Luego de las 48 horas el cliente recibirá un correo donde se notificará el cierre del ticket donde incluye la documentación y una encuesta para medir el nivel de calidad en el servicio.	Aplicación.

Fuente: Elaboración propia

El estado de los tickets consta de seis (6) tipos, en el Cuadro 12 se encuentra la descripción correspondiente de su definición y de su funcionamiento, el cliente debe conocer esta información por que se verá reflejada al momento de hacer algún seguimiento:

Cuadro 12. Estado de los tickets

Estado	**Descripción**
Nuevo	Indica que el incidente se ha registrado exitosamente por parte del cliente, se debe asignar.

Continuación:

En curso	Significa que el ticket ha sido asignado al área que corresponde para su gestión y solución.
Esperando cliente	Este estado aplicará únicamente cuando no se haya establecido comunicación con el cliente, es decir cuando el cliente no responde a los medios de contacto suministrados como el número de teléfono o correo.
Solucionado	Cuando se ha resuelto el incidente, se ha documentado y opcionalmente se ha dejado evidencia en el ticket.
Cerrado	Cuando pasan 120 horas luego del estado solucionado sin que el cliente lo reporte como reincidente automáticamente el ticket queda en estado cerrado, esto quiere decir que no se podrá volver a tratar y quedara cerrado de forma definitiva.
Reincidente	Cuando el estado del ticket se encuentra en solucionado, pero antes de 120 horas el cliente reporta que la solución propuesta no ha bastado o no cumple en su totalidad con la satisfacción del cliente, por lo que el incidente quedara activo nuevamente.

Fuente: Elaboración propia

La priorización de los incidentes estará configurada en el sistema utilizado para la gestión de tickets, es decir al momento en que el cliente ingrese toda la información para la creación del ticket, el sistema automáticamente calculara la prioridad y el tiempo para el cumplimiento de la respuesta SLA.

Respecto a la información que se solicitará a los clientes se tendrá en cuenta algunos datos de la organización, como la ubicación y el teléfono de contacto, así mismo el tipo de ticket, los impactos que está provocando y todos los detalles posibles por medio de un espacio de texto libre. En el Cuadro 13 se visualiza el formato para un incidente o solicitud:

Cuadro 13. Datos relevantes del incidente o solicitud

Nombre de la organización:		**Logo del CSIRT**
Persona contacto:		
Número de teléfono contacto:		
Correo:		
Ciudad:		
Dirección:		
Tipo:	Incidente / solicitud	
Tipificación:		
Impacto Actual:		
Impacto Futuro:		
Criticidad del sistema:		
Detalles:		

Fuente: Elaboración propia

Para diligenciar correctamente el anterior formato se deben tener en cuenta las siguientes precisiones para cada campo:

- **Nombre de la organización:** Se ingresará el nombre de la organización que solicita el ticket.

- **Persona contacto:** Se ingresa el nombre del cliente, quien será el puente para el contacto con la organización.

- **Número de contacto:** Se ingresa el número de contacto, celular, teléfono o ambos.

- **Correo:** Se ingresa el correo institucional de la organización.

- **Ciudad:** Se diligencia la ciudad en la que reside el cliente.

- **Dirección:** Se diligencia la dirección y el barrio de la ubicación de la organización.

- **Tipo:** Se ingresa incidente o solicitud teniendo en cuenta lo siguiente:

  - **Incidente:** (Si se refiere al servicio reactivo).
  - **Solicitud:** (Si se refiere al servicio proactivo).

- **Tipificación:** Aquí se debe seleccionar la tipificación propuesta dependiendo del tipo de ticket ingresado en el campo anterior, es decir puede ser incidente o solicitud:

- **Incidente:** Sí en el campo anterior "tipo" fue seleccionado incidente, entonces se visualizará la tipificación que corresponde como se muestra en el Cuadro 14:

Cuadro 14. Tipificación de incidentes

Disponibilidad	Dos.
	Interrupciones del servicio.
	Configuración.
Información	Escaneo de red.
	Análisis de paquetes.
	Acceso no autorizado (revelación de información).
	Modificación no autorizada.
	Ingeniería social.
Infección	Malware.

Continuación:

Contenido inapropiado	SPAM.
	Contenido discriminatorio / sensible.
Intrusión	Credenciales.
	Aplicaciones.
	Privilegios.
	Ataque desconocido.
Fraude	Derechos de autor.
	Suplantación.
	Phishing.
Forense	Recuperación de información.
	Investigación legal.
Otros	Otros

Fuente: CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciber incidentes [en línea]. Pág. 14. Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

- **Solicitud:** Si en el campo anterior “tipo” fue seleccionado solicitud, se podrá visualizar la tipificación correspondiente tal como en el Cuadro 15:

Cuadro 15. Tipificación para el tipo de solicitud

Forense	Recuperación de información.
	Investigación legal.
Capacitación	Concientización.
	Cursos.
Diagnostico	Análisis y asesorías.

Continuación:

Otros	Otros.

Fuente: Elaboración propia

- **Impacto actual:** Se seleccionará una opción sobre el nivel que más represente la situación en el momento actual para la organización donde superior es la opción más crítica e inferior la opción menos crítica, en el Cuadro 16 están descritas las opciones:

Cuadro 16. Nivel de impacto actual

Nivel de impacto	Detalle
Superior	El impacto es alto es uno o más componentes del sistema.
Alto	El impacto es moderado en más de un componente del sistema.
Medio	El impacto es alto en un componente del sistema.
Bajo	El impacto es moderado en un componente del sistema.
Inferior	El impacto es leve en un componente del sistema.

Fuente: Elaboración propia

- **Impacto futuro:** Se seleccionará una opción sobre el nivel que más represente la situación a futuro de acuerdo con los niveles de impacto para la organización, todos los niveles se detallan en el Cuadro 17, donde el nivel que cuenta con más prioridad es superior y el de menor es inferior:

Cuadro 17. Nivel de impacto futuro

Nivel de impacto	Detalle
Superior	El impacto es alto es uno o más componentes del sistema.
Alto	El impacto es moderado en más de un componente del sistema.
Medio	El impacto es alto en un componente del sistema.
Bajo	El impacto es moderado en un componente del sistema.
Inferior	El impacto es leve en un componente del sistema.

Fuente: Elaboración propia

- **Criticidad del sistema:** Se ingresa alguna de las siguientes opciones de acuerdo con la mejor opción que represente la situación para la empresa, en el Cuadro 18 se encuentran los niveles de criticidad y el respectivo detalle:

Cuadro 18. Nivel de criticidad

Nivel de criticidad	Detalle
Superior	Crítico (sistemas que impactan totalmente el negocio).
Alto	Impacta el área de tecnología.
Medio	Sistema que apoya varias dependencias.
Bajo	Sistema que apoya una dependencia.
Inferior	Impacta estaciones de trabajo no críticos.

Fuente: Elaboración propia

- **Detalles:** Espacio donde el cliente podrá ingresar toda la información necesaria que considere relevante para la gestión del caso. Este apartado tendrá una opción para anexar documentos o imágenes adicionales que puedan ser importantes para atender el caso. Finalmente, una vez terminado el proceso de generación del ticket se dará en la opción de enviar y se genera un número de ticket, estos son únicos e irrepetibles, por ejemplo, así:

  - Si el ticket es de tipo incidente será: INC_00001.
  - Si el ticket es de tipo solicitud será: SOL_00001.

- **Encuesta de satisfacción:** Una vez el incidente o solicitud quede en estado de cerrado, entonces al correo suministrado por el cliente llegará una breve encuesta para calificar los niveles de servicio y calificar el nivel de satisfacción, en el Cuadro 19, se establece un modelo en el que se abordan dos (2) preguntas de selección y una (1) abierta:

Cuadro 19. Encuesta de satisfacción

Reciba un cordial saludo por parte del CSIRT, queremos valorar tu opinión acerca del servicio recibido:	
1. Califique en la siguiente escala su nivel de satisfacción con respecto al servicio brindado.	
Muy satisfecho	
Satisfecho	
Poco satisfecho	
Nada satisfecho	
2. ¿El tiempo de respuesta fue adecuado por parte del equipo del CSIRT?	
Muy Rápido	
A tiempo	
Muy demorado	
3. Ingrese libremente alguna recomendación o felicitación que usted considere.	

Fuente: Elaboración propia

6.3.11 Cooperación. La cooperación es una estrategia muy importante para el funcionamiento del CSIRT, será clave mantener una relación de tipo contractual o de cooperación con otros organismos nacionales o internacionales con el propósito de adoptar nuevas medidas de ciberseguridad, conocer nuevas amenazas, escalar incidentes que contengan características especiales, este tipo de acuerdos fortalece estas relaciones de confianza y facilita el cambio de información y de servicios. El director del CSIRT será el encargo de realizar estas actividades que contemplan la comunicación con las autoridades competentes y los organismos nacionales e internacionales de acuerdo con el tipo de incidente y de los protocolos acordados para seguirlos.

El esfuerzo para poder elevar el nivel de ciberseguridad en muchos casos no es suficiente con el trabajo individual como CSIRT, contar con todo el apoyo adicional tanto a nivel local como internacional es la mejor forma para combatir la ciberdelincuencia.

Este CSIRT tendrá el reto de establecer aliados a nivel nacional e internacional con el fin de fortalecer los servicios y de la misma manera poder colaborar en la lucha del cibercrimen, por ejemplo, a trabajar de la mano con el colCERT quien asesora y coordinar a los CSIRT´S a nivel público y privado para responder a los incidentes informáticos.

6.3.12 Establecer los manuales de funciones para los perfiles del equipo de trabajo del CSIRT. El Manual de Funciones constituye el documento formal que compila las diferentes descripciones de puestos de trabajo de una organización[85]. Para alcanzar los objetivos propuestos es necesario contar con el talento humano que permita desarrollar las diferentes funciones necesarias, a continuación, en el Cuadro 20, se describen los requisitos, perfiles y roles de trabajo para la conformación del grupo CSIRT para pequeñas y medianas empresas:

Cuadro 20. Cargos manuales de funciones

Tipo de integrante	Descripción
Director	El líder del equipo es el principal responsable de los protocolos de respuesta, análisis de incidentes y actualizaciones en los procedimientos de respuesta.
Coordinador	Encargado de coordinar y supervisar todos los incidentes que son reportados al CSIRT con el fin de que estos queden solucionados en los tiempos de respuesta establecidos y así mismo administrar el equipo con el fin de mantener la operación activa.
Especialistas	Serán encargados de solucionar los diferentes incidentes nivel II que le sean asignados de acuerdo con sus competencias y habilidades.
Abogados	Su labor estará orientada en representar al CSIRT en materia de temas judiciales.
Profesionales	Serán los encargados de solucionar los diferentes incidentes nivel I que le sean asignados de acuerdo con sus competencias y habilidades.
Técnicos	Serán el apoyo en el primer momento en que se genere una incidencia reportada por el cliente, documentara la incidencia y la asignara por el conducto establecido.

Fuente: Elaboración propia

[85] AITECO. Manual de funciones [en línea]. [consultado: 26 de julio 2021]. Disponible en: https://www.aiteco.com/manual-de-funciones/

Cuadro 21. Manual de funciones Directivo

I- IDENTIFICACIÓN	
Nivel: Denominación del Empleo: Dependencia: Posición:	Directivo PROFESIONAL ESPECIALIZADO Dirección General 001
II- PROPÓSITO PRINCIPAL	
Desarrollar las actividades necesarias para el control de las políticas y ejecución de los proyectos relacionados con las operaciones del CSIRT para pequeñas y medianas empresas.	
III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS	
1. Gestionar los procesos de contratación de servicios de acuerdo con las necesidades que surjan. 2. Coordinar la gestión de proyectos sobre el análisis de la planeación, seguimiento, ejecución, evaluación y mejora continua con base a los objetivos del CSIRT. 3. Verificar el uso y cumplimiento del uso de estándares internacionales y buenas prácticas del CSIRT. 4. Entablar comunicación con otros CSIRT con los cuales exista algún tipo vinculación de cooperación con el fin de reportar o coordinar algún incidente o hecho que la situación lo amerite. 5. Comunicar a la dirigencia las estadísticas de los incidentes atendidos y demás detalles que sean solicitados. 6. Asegurarse de que el CSIRT goce de los recursos y presupuestos adecuados para llevar a cabo todos los objetivos propuestos.	
IV- CONOCIMIENTOS BÁSICOS O ESENCIALES	
1. Conocimientos generales en seguridad informática. 2. Conocimientos en herramientas y mecanismos para la seguridad informática. 3. Conocimientos de normatividad y estándares internacionales de buenas prácticas. 4. Conocimientos y habilidades para liderar grupos y manejo de personal.	

Continuación:

V – COMPETENCIAS COMPORTAMENTALES		
COMUNES	**POR NIVEL JERÁRQUICO**	**ESPECÍFICAS**
1. Aprendizaje Continuo. 2. Compromiso con la organización. 3. Trabajo en Equipo.	1. Aporte profesional. 2. Comunicación efectiva.	1. Adaptación al cambio. 2. Capacidad de gestión.

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título de postgrado en la modalidad de maestría en: - Maestría de seguridad informática. - Gerente Certificado de Seguridad de la Información (CISM) - Tarjeta Profesional - ITIL V3	Veinticinco (25) meses de experiencia profesional relacionada.

Fuente: Elaboración propia

Cuadro 22. Manual de funciones Coordinador

<table>
<tr><th colspan="3">I- IDENTIFICACIÓN</th></tr>
<tr><td colspan="2">Nivel:
Denominación del Empleo:
Dependencia:
Posición:</td><td>Profesional
PROFESIONAL ESPECIALIZADO
Área de tecnología
002</td></tr>
<tr><th colspan="3">II- PROPÓSITO PRINCIPAL</th></tr>
<tr><td colspan="3">Coordinar todas las actividades relacionadas con el proceso de atención y solución a los incidentes solicitados por parte de los clientes.</td></tr>
<tr><th colspan="3">III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS</th></tr>
<tr><td colspan="3">1. Coordinar la respuesta de los incidentes generados por los diferentes clientes en los tiempos establecidos.
2. Realizar seguimiento al estado de los incidentes y asegurarse que estos queden solucionados y documentados.
3. Elaborar estadísticas y análisis de los tickets gestionados.
4. Mantener y asegurar la continuidad del servicio.
5. Participar en el plan de mejora continua de los procesos y la operatividad del servicio.</td></tr>
<tr><th colspan="3">IV- CONOCIMIENTOS BÁSICOS O ESCENCIALES</th></tr>
<tr><td colspan="3">1. Conocimientos generales en seguridad informática.
2. Conocimientos en ITIL.
3. Conocimientos en herramientas y gestión de mesa de ayuda.
4. Conocimientos de normatividad y estándares internacionales de buenas prácticas.
5. Conocimiento básico de Ingles.</td></tr>
<tr><th colspan="3">V – COMPETENCIAS COMPORTAMENTALES</th></tr>
<tr><th>COMUNES</th><th>POR NIVEL JERÁRQUICO</th><th>ESPECÍFICAS</th></tr>
<tr><td>1. Aprendizaje Continuo.
2. Compromiso con la organización.
3. Trabajo en Equipo.
4. Trabajo bajo presión.</td><td>1. Aporte profesional.
2. Comunicación efectiva.</td><td>1. Adaptación al cambio.
2. Capacidad de gestión.</td></tr>
</table>

Continuación:

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título de postgrado en la modalidad de especialización en: - Especialista seguridad informática. - Certificación ISO/IEC 27032 - Certificación ECIH - Tarjeta profesional	Veinticuatro (24) meses de experiencia profesional relacionada.

Fuente: Elaboración propia

Cuadro 23. Manual de funciones Especialista Nivel II

<table>
<tr><th colspan="3">I- IDENTIFICACIÓN</th></tr>
<tr><td colspan="2">Nivel:
Denominación del Empleo:
Dependencia:
Posición:</td><td>Profesional
PROFESIONAL ESPECIALIZADO
Área de tecnología
002</td></tr>
<tr><th colspan="3">II- PROPÓSITO PRINCIPAL</th></tr>
<tr><td colspan="3">Asumir la gestión, análisis y respuesta de las amenazas que involucran la infraestructura de TI de los clientes, cumpliendo con los tiempos establecidos del servicio.</td></tr>
<tr><th colspan="3">III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS</th></tr>
<tr><td colspan="3">1. Prestar asistencia especializada de nivel II para las solicitudes proactivas o reactivas generadas por los clientes bien sea de forma presencial o virtual con el fin de brindar soluciones.

2. Realizar la respectiva documentación de los casos que sean atendidos, incluyendo evidencias en la solución.

3. Mantener reserva absoluta sobre la información y sistemas que correspondan a los clientes atendidos en donde la operación lo haya requerido.

4. Investigar y mantenerse actualizado sobre las nuevas amenazas cibernéticas como el malware con el fin de idear mecanismos de defensa que contrarresten los posibles impactos.

5. Transferir y compartir el conocimiento con el fin de que el equipo de trabajo posea las condiciones necesarias para enfrentar y resolver las amenazas que surjan en los clientes.</td></tr>
<tr><th colspan="3">IV- CONOCIMIENTOS BÁSICOS O ESENCIALES</th></tr>
<tr><td colspan="3">1. Conocimientos generales en seguridad informática.
2. Conocimientos en herramientas para análisis de vulneración (pentest).
3. Conocimientos en herramientas y mecanismos para la seguridad informática.
4. Conocimientos de normatividad y estándares internacionales de buenas prácticas.</td></tr>
<tr><th colspan="3">V - COMPETENCIAS COMPORTAMENTALES</th></tr>
<tr><th>COMUNES</th><th>POR NIVEL JERÁRQUICO</th><th>ESPECÍFICAS</th></tr>
<tr><td>1. Aprendizaje Continuo.
2. Compromiso
3. Trabajo en Equipo.</td><td>1. Aporte profesional.
2. Comunicación efectiva.</td><td>1. Adaptación al cambio.
2. Capacidad de gestión.</td></tr>
</table>

Continuación:

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título de postgrado en la modalidad de especialización en: - Especialista en seguridad informática. - Certificación Ethical Hacker (CEH) - Certificación ISO 27001:2013 - Certificación ECIH	Cuarenta y ocho (48) meses de experiencia profesional relacionada.

Fuente: Elaboración propia

Cuadro 24. Manual de funciones especialista nivel I

I- IDENTIFICACIÓN	
Nivel: Denominación del Empleo: Dependencia: Posición:	Profesional PROFESIONAL ESPECIALIZADO Área de tecnología 010
II- PROPÓSITO PRINCIPAL	
Orientar al cliente en la adopción de las buenas prácticas y en la implementación de las metodologías de análisis y gestión de riesgos que sean solicitados por los clientes del CSIRT.	
III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS	
1. Prestar asistencia especializada para las solicitudes proactivas generadas por los clientes bien sea de forma presencial o virtual con el fin de brindar soluciones. 2. Realizar la respectiva documentación de los casos que sean atendidos, incluyendo evidencias en la solución. 3. Mantener reserva absoluta sobre la información y sistemas que correspondan a los clientes atendidos en donde la operación lo haya requerido. 4. Investigar y mantenerse actualizado sobre las nuevas amenazas cibernéticas como el malware con el fin de idear mecanismos de defensa que contrarresten los posibles impactos. 5. Transferir y compartir el conocimiento con el fin de que el equipo de trabajo posea las condiciones necesarias para enfrentar y resolver las amenazas que surjan en los clientes. 6. Documentar medidas para los clientes, con el fin de evitar que sean víctimas de ciber ataques, estafas o robos.	
IV- CONOCIMIENTOS BÁSICOS O ESENCIALES	
1. Conocimientos generales en seguridad informática. 2. Conocimientos en metodología de análisis y gestión de riesgos MAGERIT. 3. Habilidades de comunicación.	

Continuación:

V - COMPETENCIAS COMPORTAMENTALES		
COMUNES	**POR NIVEL JERÁRQUICO**	**ESPECÍFICAS**
1. Aprendizaje Continuo. 2. Compromiso con la organización. 3. Trabajo en Equipo. 4. Adaptación al cambio. 5. Trabajo bajo presión.	1. Aporte profesional. 2. Comunicación efectiva.	1. Adaptación al cambio. 2. Capacidad de gestión.

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título de postgrado en la modalidad de especialización en: - Especialista de seguridad informática - Certificación Ethical Hacker (CEH) - Certificación ISO 27001:2013	Veinticuatro (24) meses de experiencia profesional relacionada.

Fuente: Elaboración propia

Cuadro 25. Manual de funciones profesional especializado forense

I- IDENTIFICACIÓN	
Nivel: Denominación del Empleo: Dependencia: Posición:	Profesional PROFESIONAL ESPECIALIZADO Área de tecnología 003
II- PROPÓSITO PRINCIPAL	
Asumir la gestión, análisis y respuesta a los incidentes orientados al servicio de informática forense por medio de las solicitudes de los clientes.	
III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS	
1. Prestar asistencia especializada de informática forense de manera presencial o remota, resolviendo las necesidades del cliente. 2. Realizar la respectiva documentación de los casos que sean atendidos, incluyendo evidencias en la solución. 3. Mantener reserva absoluta sobre la información y sistemas que correspondan a los clientes atendidos en donde la operación lo haya requerido. 4. Investigar y mantenerse actualizado sobre las nuevas amenazas cibernéticas como el malware con el fin de idear mecanismos de defensa que contrarresten los posibles impactos. 5. Transferir y compartir el conocimiento con el fin de que el equipo de trabajo posea las condiciones necesarias para enfrentar y resolver las amenazas que surjan en los clientes. 6. Poseer conocimiento en las leyes Colombianas referente a los delitos informáticos y realizar diseños de procedimientos sobre presuntas escenas de crimen informático. 7. Participar en el plan de mejora continua de los procesos y la operatividad del servicio.	
IV- CONOCIMIENTOS BÁSICOS O ESENCIALES	
1. Conocimientos generales en seguridad informática. 2. Conocimientos en herramientas forenses. 3. Conocimiento en la nube. 4. Conocimientos de normatividad y leyes relacionadas con los delitos informáticos. 5. Buenas habilidades de comunicación y escritura.	

Continuación:

V - COMPETENCIAS COMPORTAMENTALES		
COMUNES	**POR NIVEL JERÁRQUICO**	**ESPECÍFICAS**
1. Aprendizaje Continuo. 2. Compromiso con la organización. 3. Trabajo en Equipo. 4. Adaptación al cambio. 5. Trabajo bajo presión.	1. Aporte profesional. 2. Comunicación efectiva.	1. Adaptación al cambio. 2. Capacidad de gestión.

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título de postgrado en la modalidad de especialización en: - Especialista seguridad informática. - Certificación GIAC Security Essentials (GSEC) - Tarjeta profesional - Certificación CDFE	Veinticuatro (24) meses de experiencia profesional relacionada.

Fuente: Elaboración propia

Cuadro 26. Manual de funciones especialista en leyes

<table>
<tr><th colspan="3">I- IDENTIFICACIÓN</th></tr>
<tr><td colspan="2">Nivel:
Denominación del Empleo:
Dependencia:
Posición:</td><td>Profesional
PROFESIONAL ESPECIALIZADO
Jurídica
004</td></tr>
<tr><th colspan="3">II- PROPÓSITO PRINCIPAL</th></tr>
<tr><td colspan="3">Representar legal y judicialmente al CSIRT en los procesos solicitados bien sea a nivel de accionante o demandado.</td></tr>
<tr><th colspan="3">III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS</th></tr>
<tr><td colspan="3">1. Conocer profundamente las leyes Colombianas relacionadas a los delitos informáticos, con el fin de aplicarlos en las situaciones que lo ameriten.
2. Mantenerse actualizado sobre el cambio o actualizaciones de leyes que tengan relación con los delitos informáticos.
3. Compartir y dar a conocer las actualizaciones de las leyes colombianas que puedan impactar los procesos que se realizan.
4. Proyectar actos administrativos que sean necesarios de acuerdo con la situación.
5. Representar al CSIRT en actuaciones judiciales, extrajudiciales o administrativas que sean asignadas.</td></tr>
<tr><th colspan="3">IV- CONOCIMIENTOS BÁSICOS O ESENCIALES</th></tr>
<tr><td colspan="3">1. Conocimientos en leyes informáticas.
2. Redacción de documentos legales.
3. Normatividad vigente del sector.
4. Manejo de paquete de office.
5. Desarrollo de procesos judiciales.</td></tr>
<tr><th colspan="3">V - COMPETENCIAS COMPORTAMENTALES</th></tr>
<tr><th>COMUNES</th><th>POR NIVEL JERÁRQUICO</th><th>ESPECÍFICAS</th></tr>
<tr><td>1. Aprendizaje Continuo.
2. Compromiso con la organización.
3. Trabajo en Equipo.
4. Trabajo bajo presión.</td><td>1. Aporte profesional.
2. Comunicación efectiva.</td><td>1. Adaptación al cambio.
2. Capacidad de gestión.</td></tr>
</table>

Continuación:

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título profesional en: - Derecho - Tarjeta profesional abogado	Veinticuatro (24) meses de experiencia profesional relacionada.

Fuente: Elaboración propia

Cuadro 27. Manual de funciones profesional universitario

I- IDENTIFICACIÓN	
Nivel: Denominación del Empleo: Dependencia: Posición:	Profesional PROFESIONAL UNIVERSITARIO Área de tecnología 005
II- PROPÓSITO PRINCIPAL	
Atender y gestionar los incidentes que sean solicitados por los clientes con el fin de poderlos resolver efectivamente cumpliendo con los tiempos establecidos del servicio.	
III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS	
1. Prestar asistencia profesional de nivel I para las solicitudes proactivas o reactivas generadas por los clientes bien sea de forma presencial o virtual con el fin de brindar soluciones. 2. Realizar la respectiva documentación de los casos que sean atendidos, incluyendo evidencias en la solución. 3. Mantener reserva absoluta sobre la información y sistemas que correspondan a los clientes atendidos en donde la operación lo haya requerido. 4. Investigar y mantenerse actualizado sobre las nuevas amenazas cibernéticas como el malware con el fin de idear mecanismos de defensa que contrarresten los posibles impactos. 5. Realizar capacitaciones, charlas y orientación al cliente en temas de seguridad informática que sean asignadas. 6. Participar en el plan de mejora continua de los procesos y la operatividad del servicio	
IV- CONOCIMIENTOS BÁSICOS O ESENCIALES	
1. Conocimientos generales en seguridad informática. 2. Conocimientos en herramientas para análisis de vulneración (pentest). 3. Conocimientos en herramientas y mecanismos para la seguridad informática. 4. Conocimientos de normatividad y estándares internacionales de buenas prácticas. 5. Habilidades de comunicación.	

Continuación:

V - COMPETENCIAS COMPORTAMENTALES		
COMUNES	**POR NIVEL JERÁRQUICO**	**ESPECÍFICAS**
1. Aprendizaje Continuo 2. Compromiso con la organización. 3. Trabajo en Equipo. 4. Adaptación al cambio. 5. Trabajo bajo presión.	1. Aporte profesional. 2. Comunicación efectiva.	1. Adaptación al cambio. 2. Capacidad de gestión.

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título profesional en uno de los siguientes núcleos básicos del conocimiento: - Ingeniero de sistemas. - Ingeniero de redes o telecomunicaciones.	Veinticuatro (24) meses de experiencia profesional relacionada.

Fuente: Elaboración propia

Cuadro 28. Manual de funciones técnico

I- IDENTIFICACIÓN	
Nivel: Denominación del Empleo: Dependencia: Posición:	TÉCNICO TÉCNICO PROFESIONAL Área de tecnología 0006
II- PROPÓSITO PRINCIPAL	
Recibir y realizar la primera asistencia a los incidentes que han sido solicitados por los clientes, gestionarlos y escalarlos al nivel encargado para la solución cumpliendo con los tiempos establecidos del servicio.	
III- DESCRIPCIÓN DE FUNCIONES ESPECÍFICAS	
1. Realizar el registro de los incidentes reportados por los clientes ya sea por el aplicativo o por vía telefónica con el fin de clasificar, priorizar y escalar a los niveles encargados para la solución del ticket. 2. Mantener el seguimiento a los tickets y asegurarse de que sean resueltos en los tiempos establecidos. 3. Prestar asistencia técnica para las solicitudes reactivas generadas por los clientes los cuales no requiera mayor esfuerzo técnico. 4. Generar estadísticas y reportes relacionados con los tickets recibidos. 5. Investigar y mantenerse actualizado sobre las nuevas amenazas cibernéticas como el malware con el fin de idear mecanismos de defensa que contrarresten los posibles impactos. 6. Participar en el plan de mejora continua de los procesos y la operatividad del servicio.	
IV- CONOCIMIENTOS BÁSICOS O ESENCIALES	
1. Conocimientos generales en seguridad informática. 2. Conocimientos en herramientas para análisis de vulneración (pentest). 3. Conocimientos en herramientas y mecanismos para la seguridad informática. 4. Conocimientos de normatividad y estándares internacionales de buenas prácticas.	

Continuación:

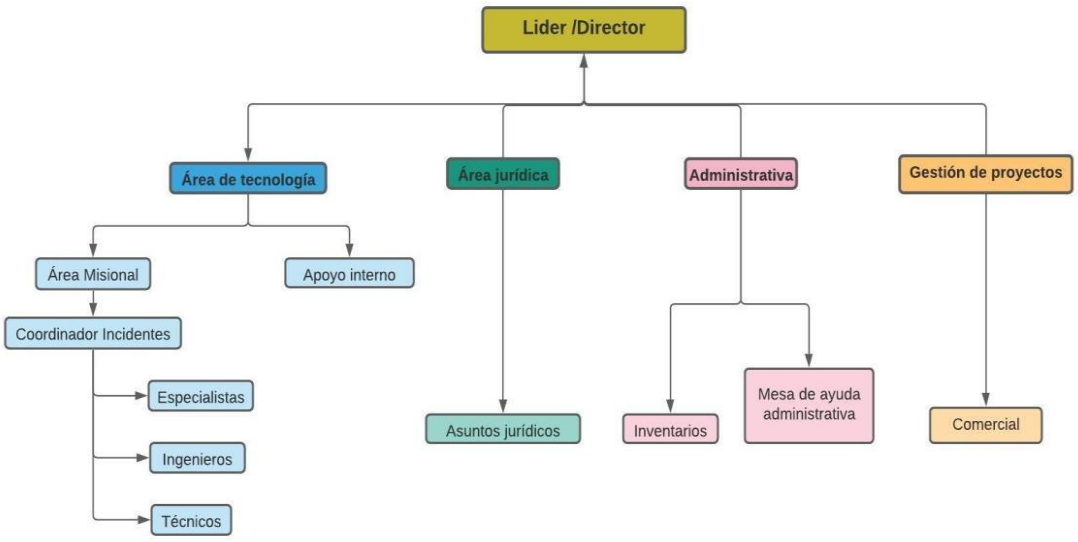
V - COMPETENCIAS COMPORTAMENTALES		
COMUNES	**POR NIVEL JERÁRQUICO**	**ESPECÍFICAS**
1. Aprendizaje Continuo. 2. Compromiso con la organización. 3. Trabajo en Equipo. 4. Adaptación al cambio. 5. Trabajo bajo presión.	1. Aporte profesional. 2. Comunicación efectiva.	1. Adaptación al cambio. 2. Capacidad de gestión.

VI - REQUISITOS DE FORMACIÓN ACADÉMICA Y EXPERIENCIA	
FORMACIÓN ACADÉMICA	**EXPERIENCIA**
Título técnico en: - Técnico profesional de sistemas.	Dieciocho (18) meses de experiencia técnica relacionada.

Fuente: Elaboración propia

6.3.13 Modelo organizacional. El modelo organizacional para el CSIRT de pequeñas y medianas empresas estará conformado por los elementos más importantes para la ejecución de la operación contemplada en este diseño documental. En la Figura 13 están plasmadas las áreas de tecnología, jurídica, administrativa y de gestión de proyectos cada una cumplen un papel fundamental para la operación y prestación del servicio, el director es el responsable de coordinar y garantizar que el CSIRT opere adecuadamente:

Figura 13. Modelo organizacional CSIRT



Fuente: Elaboración propia

Misión: Prestar servicio de atención de incidentes cibernéticos para todas las pequeñas y medianas empresas del territorio nacional.

Visión: Reducir el riesgo de que nuestros clientes comprometan sus activos por medio de ataques cibernéticos, nuestro personal está especializado en concientizar, informar, orientar y dar lo mejor de sí, para garantizar tranquilidad y satisfacción al cliente.

6.3.14 La organización. Este CSIRT ha sido patrocinado por la empresa platino sistemas, quien ha planificado su construcción y funcionamiento para el año 2022, teniendo en cuenta que la cobertura del servicio es a nivel nacional, los departamentos a excepción de Bogotá, la cobertura inicialmente será vía remota, si es necesario una visita presencial a la infraestructura del cliente, el CSIRT contará con un grupo de ingenieros en cada municipio para garantizar la atención. La sede quedará ubicada en la ciudad de Bogotá y el servicio de cobertura estará disponible para todo el territorio nacional.

Para alcanzar este objetivo se hace necesario contar con las dependencias adecuadas en el modelo y estructura organizacional:

- **Área de tecnología:** El área misional es la encargada de gestionar todos los incidentes que se generan por parte de los clientes, bien sea a nivel proactivo o reactivo por medio del equipo que conforma el área utilizando y siguiendo los mecanismos procedimentales. El área de apoyo interno estará conformada por un pequeño grupo de profesionales que brinde el apoyo de soporte para los incidentes internos con el fin de que el área misional se enfoque exclusivamente a los clientes.

- **Área jurídica:** Tienen la misión de representar de forma judicial al CSIRT en los procesos que se requieran bien sea de manera accionante o demandado, adicionalmente mantendrá actualizados y al día la información de las normas constitucionales que tengan relación con la operación del CSIRT.

- **Área administrativa:** Es la oficina encargada de realizar la administración de los bienes en la sede del CSIRT, así como llevar el inventario y gestionar una mesa de ayuda de administrativa para resolver los incidentes relacionados con la infraestructura**.**

- **Gestión de proyectos:** Se encarga de toda la planeación, seguimiento y evaluación de todos los proyectos enfocados al cumplimiento de los objetivos establecidos, así mismo de acordar contratos, establecer alcances, definir vigencias, aprobar nuevos proyectos con el cliente.

- **Talento humano y finanzas:** El área de talento humano estará a cargo de la empresa platino sistemas quien proveerá al CSIRT con todo el talento humano necesario para su funcionamiento. Así mismo sucederá con el área de finanzas que operará desde platino sistemas, responsable de administrar todo el tema financiero pertinente.

7. CONCLUSIONES

- La taxonomía de ataques cibernéticos refleja un panorama actual de la tipificación de las amenazas más conocidas a nivel mundial, esto quiere decir que pueden existir muchas otras que aún no han sido descubiertas, pero con la constante evolución de la tecnología surgirán nuevas amenazas. Esta información es clave para el CSIRT porque genera una idea más específica sobre el tipo de medidas que se pueden adoptar para mitigar y minimizar las ciber amenazas.
- El catálogo del servicio es el documento principal que el cliente visualiza para generar una expectativa del servicio, esta herramienta facilita y agiliza la comunicación con el cliente, los servicios (proactivos y reactivos) definidos para el CSIRT y brinda toda la información necesaria para que las pymes y medianas empresas puedan adquirir los servicios.
- El CSIRT debe operar bajo unas políticas y procedimientos operacionales que orienten a los integrantes de la organización, estas guías, establecen los parámetros necesarios para llevar a cabo los procesos y actividades de acuerdo con el cumplimiento de las funciones definidas anteriormente, con el fin de cumplir los objetivos del servicio. Los manuales de funciones son instrumentos que contienen las descripciones de los perfiles de trabajo que conforman la organización, cada empleado cumple un papel muy importante dentro del CSIRT, por medio de los manuales de funciones establecidos el CSIRT podrá reunir el mejor talento humano para ofrecer un servicio eficiente y de calidad al cliente.
- Muchas de las pymes y medianas empresas en Colombia no cuentan con una adecuada asesoría en materia de ciberseguridad porque la mayor parte de estos servicios son costosos y orientados a grandes empresas, este diseño documental tiene el propósito de orientar administrativamente un

CSIRT con los servicios de soporte enfocados a este sector importante para la economía nacional y que no deben olvidarse porque muchas de ellas son muy vulnerables a los ataques cibernéticos. El uso de la tecnología es un beneficio que las organizaciones han aprovechado, sin embargo, en materia de ciberseguridad aún hace falta mucho camino por recorrer para llegar a un nivel óptimo, por medio de los servicios ofrecidos por el CSIRT las pymes y medianas empresas serán beneficiadas con el fin de que adquieran mejores prácticas de ciberseguridad.

8. RECOMENDACIONES

El alcance de este proyecto se orientó a la parte administrativa, por lo que a partir de este documento será necesario complementarlo con la parte técnica que se enfoca en su infraestructura (servicios, servidores, redes, seguridad, conectividad, hardware y software) esta parte es necesaria para que el proyecto se pueda ejecutar de forma real.

Este proyecto a largo plazo debe ir madurando, es decir, ampliando su catálogo de servicios para las empresas, inicialmente un CSIRT puede estabilizarse después de uno o dos años, así mismo el CSIRT deberá ir evolucionando de acuerdo con las nuevas tecnologías y amenazas, sin embargo, siempre enfocado en su principal objetivo y conservando su esencia que es brindar servicio a las pequeñas y medianas empresas de Colombia.

Un CSIRT debe estar conformado por los mejores profesionales y expertos en los temas de ciberseguridad, pero más allá del conocimiento y la experiencia, la ética profesional y la honestidad son elementos indispensables que no se pueden plasmar en los manuales de funciones, la ética profesional se ve reflejada en el actuar de los integrantes del grupo, sin embargo, si alguno carece de valores sus actos van a causar una mala imagen para el CSIRT, es necesario que esta parte se tenga en cuenta por medio de los procesos de selección.

Es de suma importancia elaborar, implementar, mantener y actualizar un plan de contingencia y continuidad de negocio a nivel corporativo porque ninguna organización está exenta de sufrir algún ataque informático que comprometa de manera total o parcial el funcionamiento del negocio, el CSIRT deberá contar con todas las precauciones y un alto nivel de ciberseguridad, ya que un ataque cibernético puede manchar la imagen del CSIRT produciendo perdida de la confiabilidad.

Las organizaciones ya no pueden considerar la seguridad informática como un proceso aislado o secundario ante las demás, en los últimos años los efectos de la pandemia generó el proceso de la transformación digital, potenciado el uso de dispositivos informáticos para diferentes fines, ocasionado un incremento potencial de ataques informáticos que pueden vulnerar la información de las organizaciones, por medio de la capacitación y la concientización el CSIRT debe encargarse de informar y transmitir a las organizaciones sobre los riesgos y peligros que representa no contar con las medidas adecuadas de ciberseguridad.

BIBLIOGRAFÍA

ABC. Ciberataques. [en línea]. [consultado 02 de octubre 2020]. Disponible en: https://www.abc.es/tecnologia/redes/abci-eugene-kaspersky-ciberataque-contra-hospitales-atentado-terrorista-202004230204_noticia.html

AITECO. Manual de funciones [en línea]. [consultado 26 de julio 2021]. Disponible en: https://www.aiteco.com/manual-de-funciones/

ALCALDIA DE BOGOTA. Ley 1581 de 2012 [17 de octubre de 2012]. Por la cual se dictan disposiciones generales para la protección de datos personales [en línea]. [consultado 29 de septiembre 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

ASUNTOS LEGALES. Ciberdelitos en aumento [en línea]. [consultado 03 de abril 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

ASUNTOS LEGALES. Plagio penas de prisión y multas [en línea]. [consultado 11 de junio 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/por-hacer-plagio-puede-pagar-hasta-ocho-anos-de-prision-y-multas-de-hasta-1000-salario-minimos-2907914

AVENIA DELGADO Carlos, Fundamentos de seguridad informática. Información [en línea]. [consultado 24 de septiembre 2020]. Pág. 10, 2017. Disponible en: https://digitk.areandina.edu.co/bitstream/handle/areandina/1367/Fundamentos%20de%20seguridad%20inform%C3%A1tica.pdf?sequence=1&isAllowed=y

BIBLIOTECA DE SEGURANCA. Ámbitos del CSIRT y buenas prácticas Nacional [en línea]. [consultado 07 de octubre 2020]. Disponible en: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2016/09/2016-Buenas-Practicas-CSIRT.pdf

BLOG SEGURIDAD ANDREA. [en línea]. [consultado 23 de mayo 2021]. Disponible en: https://blogseguridadandrea.wordpress.com/2016/11/13/4-1-tipos-de-ataques/

CC-CSIRT. Servicios reactivos [en línea]. [consultado 21 de junio 2021]. Disponible en: https://cc-csirt.policia.gov.co/servicios/servicios-reactivos

CCIT ORG. Ciberseguridad pymes Colombia [en línea]. [consultado 10 de noviembre de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CCIT. Cibercrimen [en línea]. [consultado 20 de septiembre 2020]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CCN CERT. Ataques de denegación de servicio y recomendaciones [en línea]. [consultado 25 de mayo 2021]. Disponible en: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/10067-ataques-de-denegacion-de-servicio-distribuido-recomendaciones-y-buenas-practicas.html

CCN CERT. Creación de un CERT CSIRT [en línea]. [consultado 11 de octubre 2020]. Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf

CCN CERT. El papel de un CERT [en línea]. [consultado 07 de octubre 2020]. Disponible en: https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/657-el-papel-de-un-cert-gubernamental/file.html

CIBERSEGURIDAD BLOG. 25 ataques informáticos y como retenerlos [en línea]. [consultado 06 de mayo 2021]. Disponible en: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

CINCO DIAS. El 70% de los ciberataques son directo a las pymes [en línea]. [consultado 29 de septiembre 2020]. Disponible en: https://cincodias.elpais.com/cincodias/2020/02/23/pyme/1582491990_626988.html

COLABORACIÓN DNP. CONPES 3854. Política nacional de seguridad digital [en línea]. [consultado 04 de diciembre de 2020]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

COMPARITECH. Cybersecurity by country. [en línea]. [consultado 23 de septiembre 2021]. Disponible en: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

DEFINICIONA. Virtualidad [en línea]. [consultado 25 de septiembre 2020]. Disponible en: https://definiciona.com/virtualidad/

DELOITTE. Ciberseguridad enfocada a las pymes. [en línea]. 2019. Makros Cyber Security Expert. [consultado 04 de octubre 2020]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/risk/CyberMonth2019/guia-ciberseguridad-para-pymes-2019.pdf

DINERO. Guía de ciberseguridad para el 2019 [en línea]. [consultado 15 de octubre 2020]. Disponible en: https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

EL TIEMPO. Principales ataques de cibercriminales en Colombia [en línea] [consultado 02 de octubre de 2020]. Disponible en:

https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-ataques-de-cibercriminales-en-colombia-371096

ENCYCLOPEDIA.KASPERSKY. Las principales vulnerabilidades del software son un verdadero riesgo [en línea]. [consultado 15 de mayo 2021]. Disponible en: https://encyclopedia.kaspersky.es/knowledge/software-vulnerabilities/

FACTOR CAPITAL HUMANO. Pymes estrategias integrales para la ciberseguridad [en línea]. [consultado 27 de septiembre 2020]. Disponible en: https://factorcapitalhumano.com/emprendedores/pymes-necesitan-estrategias-integrales-de-ciberseguridad/2018/05

FUNCION PUBLICA. Decreto 1377 de 2013 [27 de junio 2013]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015 [en línea]. [consultado 28 de septiembre 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

FUNCION PUBLICA. Decreto 2573 de 2014 [13 de diciembre 2014]. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea. [en línea]. [consultado 28 de septiembre 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60596

FUNCION PUBLICA. Decreto 2693 de 2012 [21 de diciembre 2012]. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia [en línea]. [consultado 05 de diciembre 2020]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51198

FUNCION PUBLICA. Decreto 2693 de 2012 [en línea] [consultado 05 de diciembre 2020]. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

FUNCION PUBLICA. Ley 1266 de 2018 [31 de diciembre 2018]. Hábeas data [en línea]. [consultado 25 de septiembre 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=3448

GB ADVISORS. Secuestro de sesión [en línea]. [consultado 25 de mayo 2021]. Disponible en: https://www.gb-advisors.com/es/secuestro-de-sesion-aprende-evita-acceso-autorizado-datos/

GEEKS. Que es la recuperación ante desastres [en línea]. [consultado 13 de mayo 2021]. Disponible en: https://geeks.do/que-es-la-recuperacion-ante-desastres-como-servicio-o-draas/

GHASSAN Dreibli. Pymes como blanco para los ciber delincuentes [en línea]. [consultado 29 de septiembre 2020]. Disponible en: https://www.elespectador.com/noticias/tecnologia/las-pymes-como-blanco-para-los-ciberdelincuentes/

GODADDY. Amenazas informáticas que toda pyme debe conocer [En línea]. [consultado 14 de mayo 2021]. Disponible en: https://co.godaddy.com/blog/7-amenazas-informaticas-toda-pyme-debe-conocer/

GODADDY. Man in the middle [en línea]. [consultado 20 de mayo 2021]. Disponible en: https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/

HORNET SECURITY. Seguridad informática [en línea]. [consultado 25 de septiembre 2021]. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/malware/

HORNETSECURITY. Knowledge Malware [en línea]. [consultado 29 de mayo 2021]. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/malware/

INCIBE. Decálogo de ciberseguridad en empresas una guía de aproximación para empresarios [en línea]. [consultado 04 de octubre 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

INCIBE. IDS e IPS [en línea]. [consultado el 13 de junio 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

INCIBE. Taxonomía de ciber ataques [en línea]. [consultado 06 de mayo 2021]. Disponible en: https://www.incibe-cert.es/taxonomia

INFOBAE. Ciberataques en Colombia 2020 [en línea]. [consultado 05 de marzo 2021]. Disponible en: https://www.infobae.com/america/colombia/2021/02/25/2020-fue-el-ano-que-colombia-tuvo-mas-ciberataques/

INFORMATICA FANDOM. Eficiencia [en línea]. [consultado 23 de septiembre 2020]. Disponible en: https://informatica.fandom.com/wiki/Eficacia_y_eficiencia

INFORMATICA JURIDICA. Derechos de autor [en línea]. [consultado 9 de junio 2021]. Disponible en: http://www.informatica-juridica.com/trabajos/colombia-y-los-derechos-de-autor-en-internet/

IONOS. Servidor caído: riesgos, efectos y prevención [en línea]. [consultado 07 de junio 2021]. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/servidor-caido-que-hacer/

ISO 27000. Concepto ataque [en línea]. [consultado 23 de septiembre 2020]. Disponible en: https://www.iso27000.es/glosario.html

ISO 27000. Concepto impacto [en línea]. [consultado 23 de septiembre 2020]. Disponible en: https://www.iso27000.es/glosario.html

IT DIGITAL SECURITY. Que es un ataque dirigido [en línea]. [consultado 02 de junio 2021]. Disponible en: https://www.itdigitalsecurity.es/reportajes/2017/08/que-hace-diferente-a-un-ataque-dirigido

ITROQUE. 11 tipos de ataques reconocimiento [en línea]. [consultado 19 de mayo 2021]. Disponible en: http://itroque.edu.mx/cisco/cisco1/course/module11/11.2.2.2/11.2.2.2.html

KASPERSKY Threats What is DDoS Attacks [en línea]. [consultado 28 de mayo 2021]. Disponible en: https://www.kaspersky.es/resource-center/threats/ddos-attacks

KASPERSKY. Ataques dirigidos [en línea]. [consultado 30 de mayo 2021]. Disponible en: https://www.kaspersky.es/blog/ataques-dirigidos-que-conseguirian-sin-un-objetivo/104/

LA REPÚBLICA. Aumento de cibercrímenes [en línea]. [consultado 27 de septiembre 2020]. Disponible en: https://www.larepublica.co/empresas/en-tiempos-de-covid-19-empresas-deben-protegerse-ante-aumento-de-cibercrimenes-3041263

LA REPÚBLICA. Fraude una amenaza para la ciberseguridad [en línea]. [consultado 05 de mayo 2021]. Disponible en: https://www.larepublica.co/internet-economy/fraude-una-amenaza-para-la-ciberseguridad-3151358

LA REPUBLICA. Reto que deben enfrentar las empresas en el mundo por el COVID [en línea]. [consultado el 28 de octubre 2020]. Disponible en: https://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083

LATAM KASPERSKY. Resource Center What is Malware [en línea]. [consultado 28 de mayo 2021]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

LATINPYMES. Pymes vulnerables [en línea]. [consultado 30 de septiembre 2020]. Disponible en: https://www.latinpymes.com/pymes-vulnerables-a-ciberataques/

MEDUX. Why do Services outages happen: The importance of network monitoring [en línea]. [consultado 08 de agosto 2021]. Disponible en: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

MICROGESTIO. Riesgos de la seguridad informática [en línea]. [consultado 04 de mayo 2021]. Disponible en: https://microgestio.com/blog/content/riesgos-de-la-seguridad-informatica/1213

MINTIC. Guía para la gestión y clasificación de incidentes de seguridad. Gestión de incidentes. [en línea]. [consultado 29 de junio 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MINTIC. Ley 1273 de 2009 [en línea]. [consultado el 23 de mayo 2021]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MUY COMPUTER. Ransomware una gran amenaza [en línea]. [consultado 24 de julio 2021]. Disponible en: https://www.muycomputer.com/2020/07/15/ransomware-una-gran-amenaza/

NETDATANETWORKS. Ciberataques en Colombia [en línea]. 2020. [consultado 01 de diciembre 2020]. Disponible en: https://blog.netdatanetworks.com/ciberataques-en-colombia-recomendaciones-para-hacerle-frente

OAS. Riesgo cibernético sector financiero [en línea]. 2019. [consultado 14 de octubre 2020]. Disponible en: https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

PC ACTUAL. Que es un Hacker [en línea]. [consultado 17 de mayo 2021]. Disponible en: https://www.pcactual.com/noticias/trucos/espia-conviertete-hacker-2_3708

PMG-SSI. CIA [en línea]. [consultado 03 de junio 2021]. Disponible en: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

PMG-SSI. Diferencia entre evento e incidente [en línea]. [consultado 10 de julio 2021]. Disponible en: https://www.pmg-ssi.com/2016/09/iso-27001-diferencia-entre-evento-e-incidente/

PROTEJETE WORDPRESS. Seguridad de la Información y protección de datos [en línea]. [consultado 03 de junio 2021]. Disponible en: https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

PUBLICATIONS IASB. Reporte riesgos avances y el camino a seguir de ciberseguridad América latina y el caribe [en línea]. [consultado 05 de octubre 2020]. 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 /

PYMAS. Ciberseguridad pymes Colombia [en línea]. [consultado 28 de octubre 2020]. Disponible en: https://www.pymas.com.co/ideas-para-crecer/ayuda-legal/ciberseguridad-pymes-colombia

RED HAT. Topics Security What is Malware [en línea]. [consultado 29 de mayo 2021]. Disponible en: https://www.redhat.com/es/topics/security/what-is-malware

REDESZONE. Vulnerabilidades software [en línea] [consultado 14 de mayo 2021]. Disponible en: https://www.redeszone.net/noticias/seguridad/vulnerabilidades-software-importantes-2020/

RETINA EL PAÍS. Nube de cifras ciberseguridad: las cifras de los ataques informáticos [en línea]. [consultado el 02 de octubre 2021]. Disponible en: https://retina.elpais.com/retina/2020/07/17/tendencias/1594958904_685745.html

REVISTABYTE. Ciberseguridad pymes [en línea] [consultado 03 de mayo 2021]. Disponible en: https://revistabyte.es/ciberseguridad/pymes-ciberataques/

ROMERO CASTRO Martha, Introducción a la seguridad informática y al análisis de vulnerabilidades. 2018 [en línea]. [consultado 23 de septiembre 2020]. Disponible en:https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad inform%C3%A1tica.pdf

RYTE WIKI. Tipos de hijacking o secuestro [en línea]. [consultado 25 de mayo 2021]. Disponible en: https://es.ryte.com/wiki/Hijacking#Hijacking_de_sesi.C3.B3n

SEARCHDATACENTER. Equipo de respuestas frente a incidencias de seguridad informática [en línea]. [consultado 04 de octubre 2020]. Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informativa-CSIRT

SECRETARIA SENADO. Ley 1273 de 2009 [05 de enero 2009]. Por la cual se crea un nuevo bien jurídico “de la protección de la información y de los datos [en línea]. [consultado 03 de diciembre 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SEGU-INFO. Ataques de modificación [en línea]. [consultado 02 de junio 2021]. Disponible en: https://www.segu-info.com.ar/ataques/ataques_modificacion

SERVICETONIC. Servicio [en línea]. [consultado 25 de septiembre de 2020]. Disponible en: https://www.servicetonic.com/es/itil/3-itil-conceptos-y-principios/

SIC. Ley 1273 2009 [en línea]. [consultado el 23 de mayo 2021]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

SITES GOOGLE. Principios en la seguridad informática, confidencialidad, integridad y disponibilidad [en línea]. [consultado 08 de octubre 2020]. Disponible en: https://sites.google.com/site/seguridadinformaticacmj/introduccion

SITES OAS. Buenas Prácticas CSIRT [en línea]. [consultado 04 de noviembre 2020]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

SOFTWAREONE. Las causas comunes no disponibilidad en los sistemas [en línea] [consultado 13 de mayo 2021]. Disponible en: https://www.softwareone.com/es-co/blog/articles/2020/02/17/las-6-causas-mas-comunes-de-la-no-disponibilidad-en-los-sistemas

STATICS SECURELIST. Intrusión y detección en Colombia, principales amenazas [en línea]. [consultado el 01 de octubre 2020]. Disponible en: https://statistics.securelist.com/es/country/colombia/intrusion-detection-scan/month

TIP BOGOTA. CONPES 3701 2011. Lineamientos de política para ciberseguridad y ciberdefensa [en línea]. [consultado el 04 de diciembre 2020]. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

UJAEN. Diseño documental [en línea]. [consultado 06 de noviembre de 2020]. Disponible en: http://www.ujaen.es/investiga/tics_tfg/dise_documental.html

USS. Seguridad informática pymes [en línea] [consultado 04 de octubre 2020] disponible en: https://uss.com.ar/corporativo/medidas-de-seguridad-informatica-pyme/

VPN MENTOR. Historia del Ransomware [en línea]. [consultado 24 de julio 2021]. Disponible en: https://es.vpnmentor.com/blog/historia-de-la-amenaza-conocida-como-ransomware-pasado-presente-y-futuro/

WELIVESECURITY. Gusano Morris [en línea]. [consultado 10 de octubre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2018/11/05/malware-anos-80-recordando-virus-informatico-brain-gusano-morris/

WELIVESECURITY. Vulnerabilidades reportadas en el año 2020 [en línea]. [consultado 01 de octubre 2020]. Disponible en: https://www.welivesecurity.com/la-es/2021/02/16/record-vulnerabilidades-reportadas-en-2020/

ANEXOS

ANEXO A. Breve Historia del ramsomware

El primer incidente del *ransomware* conocido a nivel mundial fue hace casi más de dos décadas, respecto a la aparición que existe actualmente, para el año 2005 la transformación de internet empezó a facilitar la propagación del malware, más adelante en 2011 surgió una nueva forma de *ransomware.* El Troyano *WinLock* se considera el primer ejemplo de lo que pasó a ser conocido como *ransomware Locker* o bloqueador. En lugar de cifrar los archivos del dispositivo de la víctima, simplemente hacía que fuera imposible acceder al dispositivo, posteriormente surgieron los llamados virus de la policía, una variación sobre el tema del software de imitación que engañaba a las víctimas consiguiendo que pagaran suscripciones falsas. Para la segunda mitad del 2013 surgió una nueva variante de *ransomware* de cifrado que marcó un antes y un después en la lucha de la seguridad cibernética. *CryptoLocker* su funcionamiento consistía en enviar un mensaje a las víctimas informando de que todos sus ficheros estaban cifrados y amenazaba con borrarlos si no se pagaba un rescate en un plazo de tres días, aunque en 2014 dejó de funcionar su relevo fue *CryptoWall*, empleando el mismo cifrado de clave RSA pública-privada generado tras la pantalla de la red Tor y distribuido mediante estafas de *phishing*. *CryptoWall* también confirmó el creciente rol que estaba teniendo Bitcoin en los ataques de *ransomware*. Para el 2014, la criptomoneda era el método de pago elegido**.** Otro paso importante en la historia del *ransomware* fue el desarrollo de las versiones dirigidas a dispositivos móviles**.** Al principio, el objetivo exclusivo de estas eran los dispositivos Android, utilizando el código abierto su sistema operativo. Mas tarde afecto a dispositivos Apple, El 12 de mayo de 2017, el gusano *ransomware* paso a ser conocido en todo el mundo como *WannaCry* sus primeras víctimas fueron en España, y en cuestión de horas ya se había propagado a cientos de ordenadores en decenas de países aprovechando vulnerabilidades de los sistemas, infectándolos y causando miles de pérdidas para

organizaciones de toda clase.[86] El *Ransomware* fue la principal amenaza informática en el primer semestre de 2020, según los datos de la firma de seguridad S21sec.[87]

Ilustración 1: Representación del *ransomware*

Fuente: MUY COMPUTER. Ransomware [en línea]. 2020. Disponible en: https://www.muycomputer.com/2020/07/15/ransomware-una-gran-amenaza/

[86] VPN MENTOR. Ransomware pasado, presente y futuro [en línea]. 2020. [consultado 24 de julio 2021]. Disponible en: https://es.vpnmentor.com/blog/historia-de-la-amenaza-conocida-como-ransomware-pasado-presente-y-futuro/

[87] MY COMPUTER. Ransomware una gran amenaza. [en línea]. 2020. [consultado: 24 de julio 2021]. Disponible en: https://www.muycomputer.com/2020/07/15/ransomware-una-gran-a

ANEXO B. Educación de ciberseguridad en Australia

En Australia quieren implementar asignaturas obligatorias de ciberseguridad tanto en la educación primaria como en secundaria, una estrategia acorde a la realidad donde el mundo gira al torno de la tecnología, virtualidad y del acceso a la red internet, pero que realmente no solamente están involucrados los adultos sino que al contrario los niños y niñas desde muy pequeños empiezan a interactuar con estos dispositivos, a pesar de que hoy en día tienen una habilidad impresionante para utilizarlos, es posible que puedan tener riesgos y experiencias poco recomendables para su edad, por tal motivo Australia quiere pensar en el futuro e incluir la ciberseguridad para el conocimiento de su próxima generación, sin duda un gran paso, el conocimiento es esencial para estos tiempos donde prácticamente hay que interactuar con la tecnología para una cosa o la otra, el eslabón más débil de la ciberseguridad inicia por el desconocimiento de los usuarios, entonces si se fortalece este eslabón será más difícil que los ciberdelincuentes puedan llevar a cabo sus ataques, los niños y los más jóvenes permanecerán más seguros cuando interactúen en la red. Claramente no serán temas complejos, para los niños de primaria los temas serán básicos, pero en secundaria los temas serán un poco más serios demostrando lo vulnerables que podemos estar en la red, al visitar páginas o abrir enlaces de correos desconocidos.

Esta estrategia se debería replicar en todos los países del mundo porque al final todos los niños y jóvenes son los más beneficiados para afrontar el uso de estas tecnologías.[88]

[88] COMPUTER HOY. Australia quiere enseñar ciberseguridad a los niños de todos los colegios [en línea]. 2021. [consultado 05 de mayo 2021]. Disponible en: https://computerhoy.com/noticias/life/plan-estudios-australia-quiere-ensenar-ciberseguridad-todos-colegios-institutos-858009

ANEXO C: Modelo de acta de confidencialidad a terceros

ACTA DE CONFIDENCIALIDAD CSIRT V1

NOMBRE DE LA ENTIDAD:
REPRESENTANTE LEGAL:
NÚMERO DE IDENTIFICACIÓN:

Por medio del contrato celebrado entre la entidad y el CSIRT se acuerda:

El contratista está obligado a no divulgar a terceras partes, la Información confidencial que le sea suministrada por parte del CSIRT, y/o revelar dicha información ya sea en forma escrita, oral, visual, medios magnéticos, fotografías o en cualquier otra forma tangible.

En el caso de que el contratista deba utilizar la Información confidencial para el desarrollo de alguna actividad acordada estará obligado a mantener reserva absoluta y no revelar ningún tipo de información.

El Contratista se compromete totalmente a custodiar y reservar la información y gestión de los datos suministrados por el CSIRT en las redes y bases de datos (físicas y/o electrónicas).

Para el manejo de información que incluya datos personales, el contratista estará obligado a cumplir las disposiciones constitucionales legales y constitucionales sobre la protección del derecho fundamental lo dispuesto en el artículo 15 de la Constitución Política y la ley 1581 de 2012.

Si el contratista incumple de manera parcial o total con las obligaciones establecidas en la presente acta, será responsable de los daños y perjuicios que dicho incumplimiento llegase a ocasionar al CSIRT.

La vigencia de la presente será indefinida y permanecerá vigente mientras exista relación contractual.

Suscrita a los XX días del mes de XXXX de XXXX, en Bogotá D.C.

Firma:
REPRESENTANTE

Fuente: Elaboración propia