IMPLEMENTACIÓN DIRECTIVA Y ORGANIZACIONAL DE CIBERSECURITY-CERT

GABRIEL FERNANDO GUZMÁN RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2020

IMPLEMENTACIÓN DIRECTIVA Y ORGANIZACIONAL DE CIBERSECURITY-CERT

GABRIEL FERNANDO GUZMÁN RODRÍGUEZ

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

Tutor
Milton Javier Mateus

Asesor de proyecto
Cesar Enrique Silva

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Neiva, 09 de diciembre de 2020

DEDICATORIA

Dedico este trabajo a mis excompañeros del Laboratorio De Informática Forense, pertenecientes al Centro Cibernético Policial, de la Policía Nacional de Colombia, por su gran apoyo y amistad.

AGRADECIMIENTOS

Agradezco al Centro Cibernético Policial, de la Policía Nacional de Colombia, especialmente al personal perteneciente al área del Laboratorio De Informática Forense, ya que pude compartir muchas experiencias sobre la labor que se desempeña en el campo de la investigación de delitos cibernéticos y el forense digital, donde me apoyaron incondicionalmente en mi formación y trayectoria laboral, mientras pertenecí a esta prestigiosa entidad, desde donde me inspiraron a continuar con el desarrollo de este trabajo.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

ACTIVOS DIGITALES: cualquier recurso en forma digital que se puede poseer, o que representa contenido que se puede poseer, y por tanto, tiene asociado un derecho de uso.

BEC: Técnicas en donde los delincuentes cibernéticos consiguen datos privados de compañías, directores y personal que labora en las empresas, con el fin de enviar correos falsos donde se suplante personas con poder de decisión, buscando que otros empleados de menor rango realicen transacciones financieras o de mercancías a persona ajenas a la entidad.

CRYPTOJACKING: tomar control del hardware de la víctima, la cual se obtiene a través de la visita a un sitio web, con el fin de realizar el proceso de minería de criptomonedas.

CSIRT: Equipo de Respuesta ante Incidencias de Seguridad Informáticas.

DDOS: Técnica que logra bloquear un servicio web, con el fin que no sea accesible a sus usuarios y clientes.

HARDWARE: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático

INCIDENTES CIBERNÉTICOS: todo evento contra un sistema de información que produce la violación de una política de seguridad explícita o implícita, poniendo en riesgo la confidencialidad, integridad y disponibilidad del mismo.

INFORMÁTICA FORENSE: se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o privada.

MALWARE programa informático capaz de afectar un sistema informático sin la autorización de su dueño.

PYMES: comprenden las micros, pequeñas y medianas empresas operadas por una persona natural o jurídica bajo alguna forma de organización.

RAMSONWARE: modalidad delictiva que utiliza malware y diferentes programas informáticos, con el fin de lograr el cifrado de los archivos de una máquina, para

posteriormente pedir recompensa económica, a fin de entregar la solución de acceso a los datos.

SIM SWAPPING: busca tener en control de abonaos telefónicos de personas, a través de engaños a proveedores de servicio de telefonía móvil, requiriendo la activación de tarjetas SIM, de manera irregular.

SOFTWARE: conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora

TAXONOMÍA: estructura de organización de la información que está formada por un conjunto de categorías y subcategorías, gracias a las cuales podemos unir entidades (cosas) que comparten alguna característica común.

VULNERABILIDADES: incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la incapacidad para reponerse después de que ha ocurrido un desastre.

RESUMEN

El objetivo principal que se quiere conseguir con la puesta en marcha del presente proyecto, es la organización documental de un CSIRT, que sirva como soporte a empresas, que en el mercado no encuentran una opción que se acomode a su presupuesto, en la posibilidad de tener asesoría y protección de sus activos de información. Se realiza la delimitación del ámbito de actuación del CSIRT basado en el contexto y panorama actual de Ciberseguridad en Colombia, estableciendo los servicios que prestará, desde la actuación reactiva, preventiva y proactiva. Se desarrollan las tablas de cargos y perfiles necesarios en el funcionamiento del CSIRT y se define la estructura organizacional, de políticas y manuales de procedimientos operacionales estandarizados, para funcionamiento eficiente de la organización.

PALABRAS CLAVE: Administrativo, CERT, Ciberseguridad, CSIRT, directivo, incidente, información, seguridad, vulnerabilidad.

ABSTRACT

The main objective that is to be achieved with the implementation of this project, is the documentary organization of a CSIRT, which serves as support to companies, that in the market we do not find an option that suits their budget, in the possibility of have advice and protection of your information assets. The delimitation of the CSIRT's scope of action is made based on the current context and panorama of Cybersecurity in Colombia, establishing the services it will provide, from reactive, preventive and proactive action. The charge tables and profiles necessary in the operation of the CSIRT are defined and the organizational structure, policies and manuals of standardized operational procedures are defined for the efficient operation of the organization.

KEY WORDS: Administrative, CERT, CSIRT, Cybersecurity, incident, information, manager, security, vulnerability.

INTRODUCCIÓN

La Ciberseguridad en Colombia ha afectado la economía tanto de empresas como de personas naturales, pero esto solo es la punta de iceberg de lo que será el futuro, ya que se evidencian sofisticaciones técnicas importantes en la vida del ser humano que involucran la inteligencia artificial, el internet de las cosas y el Big Data, lo que abrirá un abanico de posibilidades casi infinitas para los ataques cibernéticos.

Con este trabajo se pretende iniciar la primera fase de la implementación de un CSIRT sectorial para ayudar a las empresas que no cuenta con los recursos económicos suficientes para formar su propio equipo de respuesta a incidentes, apoyándolo con el ofrecimiento de los servicios requeridos. En este primer momento se busca desarrollar la documentación necesaria para el funcionamiento de Cibersecurity-CERT.

Este propósito se construirá a través de la investigación del contexto colombiano, identificando la situación de la cibercriminalidad del país, con el fin de analizar la viabilidad del proyecto, llegando a relacionar los elementos documentales necesarios para su inicio.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Cibersecurity de Colombia LTDA, es una empresa colombiana que presta servicios de seguridad para la protección de la Información. Su propósito para el año 2021 es consolidarse como un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT.

Este buscará crear y gestionar las funciones de respuesta a incidentes cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes, teniendo presente el nivel de servicio contratado, los cuales pueden ser de respuesta a incidentes o de gestión a vulnerabilidades. Con el fin de iniciar el desarrollo del proyecto, se hace necesario identificar los aspectos administrativos importantes para su funcionamiento, como son la delimitación de su ámbito de actuación, la definición de servicios a prestar, los perfiles profesionales necesarios y sus políticas organizacionales.

Por tal motivo la empresa Cibersecurity de Colombia LTDA, requiere el diseño documental de sus aspectos directivos, los cuales son necesarios para posteriormente desarrollar de manera acertada, su diseño técnico, lo que permitirá dar avance a la creación final del CSIRT.

Según el informe presentado por las autoridades que atienden y estudian el Cibercrimen en Colombia, a través del documento tendencias Cibercrimen 2018-2019, Durante el año 2019 se presentó un aumento del 54% de los casos reportados por incidentes en el ciberespacio, donde se revelo un incremento preocupante en ataques con malware a pequeñas y medianas empresas (PYMES), reportando en 2018 una cifra de 99 denuncias y en la siguiente anualidad se llegó a 705 querellas, demostrando que la tendencia de la delincuencia está en concentrar sus energías en defraudar esta población económica[1].

Lo más grave del aumento en la tendencia en ataque a PYMES, se evidencia cuando se enumeran las causales de preferencia de los delincuentes cibernéticos para tratar de obtener beneficio de estas entidades, las cuales van desde los pocos recursos económicos con los que cuentan estas empresas para adquirir infraestructura necearía que mejore la seguridad de la información tanto en hardware y software, la falta de personal con conocimientos en seguridad

[1] Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

informática, el desconocimiento de las medidas básicas de protección en la red y la inexistencia de entes dedicados especialmente al estudio de medidas preventivas para esta población, ya que los costos para creación de equipos que prevengan y den respuesta a estos incidentes es muy alto.

Igualmente, las consecuencias de un ataque a una pequeña empresa, no es más alentador, ya que, según el reporte de las autoridades, el 60% de los negocios que sufren un hecho delictivo contra su información, no logran sobrevivir a este más de 6 meses[2].

Una de las iniciativas más similares, a la propuesta que se quiere desarrollar, es la de INTECO-CERT[3], la cual fue implementada en España, con el objetivo de apoyar con un CSIRT, que brindara seguridad y confianza a las PYMES y ciudadanos del país, cuando estos utilizaran las tecnologías de la información para el comercio electrónico y la convivencia en la Red, logrando grandes beneficios a estos dos sectores, los cuales anteriormente se sentían solos y vulnerables al momento de usar las nuevas fuentes de comunicación.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se diseñan e identifican los requerimientos administrativos, en la creación de un equipo de respuesta a incidentes, enfocado a PYMES?

Se evidencia la necesidad de crear un equipo de respuesta a incidentes tecnológicos que colabore con la protección y educación de las PYMES y empresas que no cuenten con el recurso económico suficiente para tener un personal propio en estas funciones.

La mala gestión de la seguridad de los datos de cualquier empresa, implicaría responsabilidades legales y económicas importantes, pero más grave sería si la organización encargada de esta tarea, demuestra falta de profesionalismo en el diseño y gerenciamiento de su mismo funcionamiento.

[2] Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[3] Rivas, J. (2008, diciembre 19). INTECO-CERT, centro de respuesta antes incidentes en TI para pymes. Pymes y Autonomos. https://www.pymesyautonomos.com/tecnologia/inteco-cert-centro-de-respuesta-antes-incidentes-en-ti-para-pymes

2 JUSTIFICACIÓN

El motivo principal del desarrollo de este proyecto, es el de poder brindar las pautas administrativas y legales para el diseño y organización de un CSIRT comercial, desde su aspecto directivo, que, al ser llevado a la realidad, puede brindar la oportunidad de competitividad a todos los actores económicos en crecimiento, teniendo chance de contratar los servicios mínimos de reacción y asesoría en el ámbito de la Ciberseguridad.

Con el resultado de este trabajo se busca poner un grano de arena en el desarrollo económico de empresas que en el futuro se verán vulnerables y susceptibles de desaparecer, gracias a la falta de conocimiento de los factores de amenazas en el contexto del manejo de las tecnologías de la información.

Al identificar en ciertas regiones de Colombia, se desconocen muchos temas de seguridad de la información, se ve la gran necesidad de personas capacitadas en la prevención y respuesta ante delitos cibernéticos, ya que generalmente el personal de TI, que atiende estos hechos termina eliminando los registros dejados por los ataques, lo que impide su acertado diagnóstico y tratamiento.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar la documentación e identificación de los requerimientos administrativos de Cibersecurity-CERT, con el fin de establecer los aspectos organizacionales, necesarios para el desarrollo de las actividades propias de este CSIRT.

3.2 OBJETIVOS ESPECÍFICOS

- Delimitar el ámbito de actuación del CSIRT basado en el contexto y panorama actual de Ciberseguridad en Colombia.

- Establecer los servicios que prestará el equipo CSIRT, desde la actuación reactiva, preventiva y proactiva, teniendo en cuenta la descripción de los ataques más relevantes presentados en Colombia.

- Desarrollar las tablas de cargos y perfiles necesarios en el funcionamiento del CSIRT.

- Definir la estructura organizacional, las políticas y manuales de procedimientos operacionales estandarizados del CSIRT, para tener como guía en la actuación del equipo.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En Colombia está en curso hace unos años una problemática que no parece amenazante para la seguridad digital del estado, las personas y empresas; pero este puede ser solo la punta del iceberg de lo que viene en el futuro, pareciera que el gobierno tomara las medidas adecuadas para la defensa de los activos digitales de todos, pero se nota que la reacción está llegando un poco tardía para las PYMES (pequeñas y medianas empresas) y gobiernos municipales de pocos recursos económicos, por eso se debe gestionar la necesidad de que esta respuesta pueda llegar desde el ámbito privado, ofreciendo un servicio de calidad y muy profesional a través de los CSIRT.

Según Raúl Kats (2018), en su libro el "ecosistema y la economía digital en américa latina", es notable que la región muestra un crecimiento exponencial en la utilización de las tecnologías de la información, para apoyar todo tipo de negocio, donde ya existen compañías que su mayor activo son la información y la tecnología con la que se gestionan[4], de la cual Colombia no podía ser la excepción. Este gran progreso en el cambio de nichos de negocios y manera de adminístralos y venderlos, no llega solo, ya que con esto también vienen las maneras de la delincuencia de buscar tener su participación de estas grandes ganancias. Una prueba de esto es el aumento del 54% de los incidentes tecnológicos en el año 2019 comparado con el año 2018[5], cifra que se evidencia muy alta si se destaca que la mayoría de estas conductas no son denunciadas por algunas personas, las cuales no le dan importancia, al igual que empresas que por vergüenza al mal prestigio y desconfianza de sus clientes, asume las perdidas, dejando más expuesta a otras compañías, por falta de información del incidente ocurrido, dando la oportunidad a más ataques.

En este sentido las grandes compañías y empresas estatales vienen tomando medidas integrales, creando unas políticas de Ciberseguridad mas estandarizas y acordes a las amenazas, donde crean equipos y cargos donde se va a desarrollar

[4] Kats, R. (2018). El ecosistema y la economía digital en américa latinas. Madrid, ESPAÑA: Editorial Planeta. (pp. 266 – 267). Recuperado de https://books.google.com.co/books?id=Axt5CgAAQBAJ&printsec=frontcover&dq=panorama+actual+de+CiberSeguridad+en+Colombia&hl=es-419&sa=X&ved=0ahUKEwjVzcCO7pXmAhXGq1kKHcYACI4Q6AEIYjAI#v=onepage&q=seguridad&f=false

[5] Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

esta tan importante labor[6]. El problema surge ya con las PYMES (pequeñas y mediana empresas), las cuales consideran que el gasto es demasiado alto al momento de implementar soluciones más completas, llegando al punto de que no le dan la importancia necesaria. Desafortunadamente gracias a este enfoque dado al valor de los datos, las PYMES son el principal objetivo de ataque para los Ciberdelincuentes que quieren tener beneficios financieros.

La nueva era de la criminalidad siempre evoluciona con su entorno, especialmente en el momento de la moda de la informática, que se encuentra en todos los entornos de las sociedades, desde ámbitos personales, hasta los negocios, por esta razón los grandes delincuentes están pasando de ser bandas de atracadores fuertemente armados dispuesto a dar su vida por su botín, a ingenieros, matemáticos, psicólogos entre otros profesionales que harán sus mismas fechorías, pero detrás de una pantalla de computador[7].

De lo que no son conscientes algunas empresas, especialmente pequeñas, es que dependiendo del ataque informático en el que se vean expuestos, este puede llevar a un negocio hasta la quiebra, ya que, así como es costosa la implementación de medidas de seguridad digital, igualmente es muchísimo mayor el impacto económico que genera un incidente[8].

En el marco de la situación de políticas públicas, para lograr enfrentar los retos de seguridad digital en Colombia, se evidencia un gran avance y apoyo por parte del estado, iniciando con la puesta en marcha del documento CONPES 3701 de 2011, donde se inicia realmente la organización de las entidades encargadas de la protección de los Ciudadano ante las amenazas del crimen digital y la defensa del país en cuanto a ataques internos o externos desde el contexto del ciberespacio[9].

Según Cortés (2015), en su artículo “Estado actual de la política pública de Ciberseguridad y Ciberdefensa en Colombia”, nuestro estado es uno de los

---

[6] Consejo Nacional de Política Económica y Social [Conpes]. (Julio 14 de 2011). Docu-mento Conpes 3701. Lineamientos de Políti-ca para Ciberseguridad y Ciberdefensa. Re-cuperado el 25 de octubre de 2014 de min-tic: http://www.mintic.gov.co/portal/604/articles3510_documento.pdf

[7] Caballero, D. (2019). Matemáticos, ingenieros, informáticos: los criminales del futuro que amenazan a las empresas. Recuperado de https://www-abc-es.cdn.ampproject.org/c/s/www.abc.es/economia/abci-matematicos-ingenieros-informaticos-criminales-futuro-amenazan-empresas-201911240248_noticia_amp.html?fbclid=IwAR3NUZO-0WtaFEIF83F_GaOwA2gg5BeXU1bG1TEI3Ca0ZdrURUqfv6pVfBI

[8] Mosquera, V. A. (2019). Ciberseguridad en Colombia. Bogotá, COLOMBIA: Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

[9] Robles, P.H. (2018). Panorama Actual De La Seguridad Informática O De La Ciberseguridad, A Nivel Del País Y Las Tendencias Actuales Y Futura A Nivel Global: Universidad nacional abierta y A Distancia. Recuperado de https://core.ac.uk/download/pdf/187433111.pdf

ejemplos de la región, pero que igualmente deja expreso que el reto es grande, ya que también tenemos uno de los más altos indicen de crecimiento del delito informático[10].

A pesar que a nivel gubernamental se enumeran grupos especializados para enfrentar los más grandes retos en Ciberseguridad, donde por ejemplo se cuenta el Centro Cibernético Policial (CCP), que se encarga de la gestión de los incidentes de criminalidad digital, a través del CAI virtual, sus laboratorios de informática forense, unidades de investigación de delitos tecnológicos y de análisis de malware, se denota que ellos también son responsables de los delitos que a pesar de no ser de índole digital, tiene una relación cuando utilizan estos medios cibernéticos para ser cometidos, este es el caso de la evidencia de documentos digitales, conversaciones de mensajería instantánea, información almacenada en celulares, entre otros. Al tener tanto campo de acción es muy difícil poder llegar a corresponder de manera eficiente a casos de criminalidad específicos, como son los delitos en modalidades de MALWARE, BEC, DDOS, SIM SWAPPING, CRYPTOJACKING o RAMSONWARE[11]. Lo problemático del asunto es que estas son modalidades delictivas con tendencia a aumentos vertiginosos y que afectan especialmente a ciudadanos del común y PYMES, los cuales no cuentan con el apoyo tecnológico y educativo para prevenir estos flagelos.

Según los manifestado por Robles(2018), en su monografía “Panorama Actual De La Seguridad Informática o De La Ciberseguridad, A Nivel Del País Y Las Tendencias Actuales Y Futura A Nivel Global”, se puede concluir que en la implementación del CONPES 3701 de 2011, se han realizado grandes avances especialmente en temas de creación de entidades responsables de cada aspecto de la seguridad digital, como son el CCP, colCERT, CCOC (Comando Conjunto Cibernético), el CSIRT PONAL, entre otras, pero también se evidencio uno de los temas que más preocupan, que es la falta cooperación y sinergia entre estas entidades[12]. Otro reto que enfrenta Colombia será la comunicación y educación de los ciudadanos en temas de Ciberseguridad, ya que de eso dependerá también el

[10] Cortes, B.R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia: Revista Derecho, Comunicación y Nueva Tecnologías. Recuperado de https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics227.pdf

[11] Vega, S.F. (2018). Métodos De Ataques Y Prevención De La Ingeniería social En Las alcaldías Del Huila En Colombia: Universidad nacional abierta y A Distancia. (pp. 63 – 74). Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/18701/1075273452.pdf?sequence=1&isAllowed=y

[12] Robles, P.H. (2018). Panorama Actual De La Seguridad Informática O De La Ciberseguridad, A Nivel Del País Y Las Tendencias Actuales Y Futura A Nivel Global: Universidad nacional abierta y A Distancia. Recuperado de https://core.ac.uk/download/pdf/187433111.pdf

crecimiento económico de la nación, puesto que todos deberán aprender a utilizar para bien, la apertura de la información digital del estado[13].

Dentro del CONPES 3854, se define a Colombia como uno de los estados reconocidos por su liderazgo en temas de avance en Ciberseguridad a nivel internacional, donde se cuenta con herramientas importantes para la reacción a incidentes como son ocho CSIRT con membrecías del Foro de equipos de seguridad y respuesta de incidentes (FIRST), pero se sabe que no es suficiente, ya que se puede notar que la mayor capacidad de respuesta se encuentra enfocada en las organizaciones más grandes y de infraestructura critica para el Gobierno. El problema está en las pequeñas empresas y municipios del país que no cuenta con los recursos para implementar un mecanismo de defensa y reacción mínimamente eficiente.

Gracias a que se cuenta con conceptos y metodologías de implementación de CSIRT más acorde a las necesidades de cada actor de la sociedad, se puede estudiar y verificar varias implementaciones, como ejemplo, la descrita por ENISA, que según su documento “Cómo Crear Un CSIRT Paso A Paso”, se encuentra muy claro desde el concepto más básico, hasta el diseño que requiere cada contexto[14].

Debido a las limitaciones de PYMES Y entidades públicas de municipios pequeños, nace la iniciativa de creación de un CSIRT Comercial, llamado así según lo dispuesto por la OEA (2002), en su artículo, “Buenas Prácticas para establecer un CSIRT nacional”, el cual será de gran apoyo para todo negocio que tenga necesidades específicas de protección y conocimiento de la Ciberseguridad. Este será de gran apoyo no solo en aspectos reactivos, sino también en la educación de las personas integrantes de los negocios, lo que ayudará a prevenir incidentes graves y pérdidas que menoscaben la económica nacional, llevando a prevenir la quiebra de muchos colombianos[15].

[13] OCDE (2016) Evaluar el impacto del gobierno digital en Colombia. Recuperado de: https://www.oecd.org/countries/colombia/evaluar-el-impacto-del-gobierno-digital-en-colombia-9789264284272-es.htm

[14] Enisa, « Cómo crear un CSIRT paso a paso» Enisa, 2006. [En línea]. Recuperado de: https://www.enisa.europa.eu › publications › at_download › fullReport. [Último acceso: 02 12 2019].

[15] OEA (2002) Buenas Prácticas para establecer un CSIRT nacional. Recuperado de: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

4.2 MARCO CONCEPTUAL

4.2.1 Definición de CSIRT. Es un equipo de especialistas en temas de seguridad informática, encargados de atender incidentes en la seguridad de la infraestructura tecnológica, especialmente de informática, para las empresas que requieran de sus servicios. Estos equipos están conformados por personal técnico y profesional en diferentes campos de la gestión de la seguridad de tecnologías e infraestructura para el tratamiento de los datos[16].

4.2.2 Tipos de CSIRT. Las definiciones de los tipos de CSIRT están muy aclaradas en el concepto elaborado por la OEA, donde deja descrito los tipos de equipos que se pueden crear, teniendo siempre presente, el objetivo, los clientes a atender, las capacidades de talento humano y la logística.

Se relacionan los CSIRT más relevantes según la OEA, teniendo en cuenta a los tipos de clientes que se pretende servir.

"CSIRT DE INFRAESTRUCTURAS CRÍTICAS: En algunos casos, hay CSIRTs establecidos específicamente para la protección de los activos de información críticos y la infraestructura crítica de la nación, sin importar si es operado por el sector público o privado, o para la administración de transporte, la generación de energía, las comunicaciones u otros procesos. Dado que las instituciones que dependen de este tipo de CSIRT pueden pertenecer a más de una comunidad (por ejemplo, tanto militar como de infraestructura crítica), es vital establecer protocolos de interacción con otros equipos involucrados.

CSIRT DE PROVEEDORES: Son CSIRT que prestan servicios relacionados con productos específicos de un fabricante, desarrollador o proveedor de servicios. El propósito de este tipo de CSIRT es mitigar el impacto de las vulnerabilidades o problemas de seguridad relacionados con sus productos. Los ejemplos incluyen HP CSIRT (Hewlett Packard), Banelco CSIRT (Banelco Bank), o Adobe PSIRT (Adobe) entre otros.

CSIRT DEL SECTOR DE PEQUEÑAS: Y MEDIANAS EMPRESAS (PYME) Su tamaño y su naturaleza a menudo no les permiten a las PYME implementar equipos de respuesta a incidentes individuales. Por lo tanto, hay una necesidad de crear CSIRT que entiendan y respondan a las necesidades de esta comunidad de negocios; por ejemplo, en España se encuentra el INTECO-CERT Corporation, que se centra en ayudar a las PYME y a los ciudadanos.

[16] Ibid.

CSIRT COMERCIALES: Por diversas razones, incluyendo limitaciones de recursos humanos o muchas otras, algunas empresas optan por externalizar los servicios de CSIRT en lugar de internamente crear y gestionar las funciones de respuesta a incidentes. Esto ha dado lugar a un mercado robusto para CSIRT comerciales, que ofrecen servicios pagos de respuesta a incidentes para clientes. La relación entre un CSIRT comercial y su cliente a menudo se rige por acuerdos de nivel de servicio (SLA por sus siglas en inglés), que son necesarios para establecer lineamientos de respuesta a incidentes y asegurar que la información se maneja de acuerdo a las necesidades del cliente"[17].

4.2.3 Servicios de un CSIRT. Dentro de los tipos de servicio que puede prestar un CSIRT, se observa que la OEA los divide en tres categorías como son los Servicios proactivos, Servicios reactivos y Servicios de valor agregado.

- **"Servicios proactivos**.

Proactivos primer nivel: Uno de los servicios más básicos que ofrece un CSIRT es el monitoreo y las alertas, implica la implementación de sistemas que ayudan a detectar eventos de seguridad, realizan correlación de eventos, producen informes automatizados y escanean en búsqueda de vulnerabilidades en la comunidad objetivo. Para llevar a cabo estas funciones, el CSIRT puede desarrollar sus propias soluciones internas o emplear herramientas y sensores comerciales de fuente abierta o de terceros. La información producida por las iniciativas de monitoreo y alerta impulsará la toma de decisiones estratégicas y mejorará los procesos de respuesta a incidentes.

Proactivos segundo nivel: Un CSIRT más desarrollado ofrecerá servicios de vigilancia y de alerta más avanzados. Estos hacen un seguimiento a los sistemas y a las infraestructuras de la comunidad objetivo en mucha más profundidad, pero por lo general proporcionan el mismo tipo de alertas y correlación de incidentes, como el monitoreo y alerta de primer nivel. Un seguimiento más de cerca de los sistemas de cliente permite la detección temprana de eventos de seguridad, vulnerabilidades o artefactos maliciosos. Para llevar a cabo este tipo de monitoreo en profundidad, en general se requiere de la interconexión del sistema o la instalación de sensores de seguridad en la infraestructura de la comunidad.

- **investigación y desarrollo**

Investigación y desarrollo primer nivel: Estos servicios les permiten al CSIRT y a su comunidad mantenerse al tanto de los avances en el campo de la seguridad

[17] OEA (2002) Buenas Prácticas para establecer un CSIRT nacional. Recuperado de: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

de la información y de la respuesta a incidentes. En concreto, se les permitirá estar al día sobre las alertas, las amenazas en evolución, los vectores de ataque que emergen, las mejores prácticas y nuevas normas en los servicios, así como sobre el mantenimiento y la operación de dispositivos, las estrategias de defensa y varios otros temas.

Investigación y desarrollo segundo nivel: A medida que madura un CSIRT, va desarrollando capacidades más robustas de I+D. Con la información que recopila y genera, el CSIRT puede realizar auditorías de seguridad y evaluaciones en sus propios sistemas o en los del grupo objetivo. Esto puede incluir el análisis de la infraestructura o la aplicación, la revisión de las políticas de seguridad, el análisis de vulnerabilidades, las pruebas de penetración y el cumplimiento de los estándares o normas internacionales.

A MEDIDA que la tecnología evoluciona, las amenazas y las vulnerabilidades cambian. El CSIRT debe poder detectar amenazas o vulnerabilidades emergentes inherentes a las nuevas tecnologías y distribuir información relevante que pueda mejorar los niveles de seguridad.

Investigación y desarrollo tercer nivel: Los CSIRT más avanzados continuarán desarrollando las capacidades de I+D, por ejemplo, el análisis de los códigos maliciosos, a fin de poder determinar la naturaleza, el comportamiento y el propósito de un artefacto específico.

- **Servicios reactivos**.

Gestión de incidentes: El servicio de gestión de incidentes se compone de varias fases: la notificación y la recepción de un incidente, clasificación o TRIAGE, respuesta, análisis y resolución. El CSIRT debe primero determinar el tipo, el impacto potencial y la gravedad de un incidente, seguido de cerca por la designación de un equipo de respuesta que diseñe un plan de acción que restaurará los servicios o los sistemas a su funcionamiento normal o que mitigará el impacto de un evento de seguridad cibernética. En ciertos casos, esto requerirá que el personal del CSIRT visite el sitio del evento de seguridad. Muchos actores suelen participar en respuestas a incidentes cibernéticos, incluyendo, pero no limitado a los ISP, otros CSIRT, proveedores de tecnología, agencias del orden público, actores internacionales, equipos legales, departamentos de prensa y diferentes áreas de una organización afectada. El CSIRT coordina las actividades de respuesta y las comunicaciones de los distintos grupos de interés para optimizar esfuerzos y reducir los tiempos de resolución de incidentes. Para lograr esto, el CSIRT debe conocer las necesidades y los requerimientos de cada una de las partes interesadas con el fin de gestionar positivamente la interacción entre ellos.

Respuesta a vulnerabilidades: Esto comprende una variedad de procesos de gestión de vulnerabilidades, incluyendo parches, la aplicación de contramedidas y otras estrategias de mitigación. A medida que están disponibles nuevos parches para las vulnerabilidades detectadas, el CSIRT debe notificar a todas las partes interesadas y distribuir parches o describir las técnicas para la aplicación de contramedidas, mientras coordina y confirma que se están tomando las medidas adecuadas.

Respuesta a artefactos maliciosos: Un artefacto malicioso es un archivo o un objeto en un sistema que está involucrado en un ataque a una red o sistema, o se utiliza para evadir los controles de seguridad o medidas. La gestión de los artefactos maliciosos requiere extraerlos de un sistema afectado o informar a las partes interesadas sobre cómo hacer la gestión"[18].

4.3 MARCO LEGAL

Para el gobierno de Colombia se hace imperativo la creación de equipos de respuesta a incidentes sectorial, ya que estos apoyaran la labor de seguridad en el entorno digital de los ciudadanos del país.

Las normatividades a tener en cuenta en la creación y gestión del CSIRT se encuentran en:

- **CONPES 3854 del 11 de abril de 2016.** Teniendo en cuenta esta necesidad de aportar a la protección de todos los sectores sociales y económicos de la nación, en la protección de sus datos e infraestructuras tecnológicas, el gobierno decide impulsar y promover en la estrategia "E4.4. Fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas" descrita en el CONPES 3854, la cual apoya la creación y promueve mejoras de CSIRT sectoriales.

  Se identifica como misión de los CSIRT que "tendrán la capacidad de reacción ante incidentes especializados por sector y con capacidad real de interacción con los diferentes fabricantes, agencias de ley y otras agencias del gobierno. Adicionalmente, definirán prácticas adecuadas de gestión de seguridad en cada sector, asesorarán y acompañarán a las diferentes empresas"[19].

[18] OEA (2002) Buenas Prácticas para establecer un CSIRT nacional. Recuperado de: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[19] Consejo Nacional de Política Económica y Social [Conpes]. (Abril 11 de 2016). Docu-mento Conpes 3854. Política Nacional De Seguridad Digital. Recuperado el 15 de Noviembre de 2020 de dpn: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Por último, se establece que anualmente el coordinador nacional de seguridad digital, realizara convocatorio de socialización de todos los CSIRT en Colombia, donde se mostrara por cada uno de estos, el estado de las modalidades de ataque conocidos y se desarrollara un documento que apoyara en la mejora continua de la seguridad nacional digital.

- **Normas de apoyo.** Con el fin de facilitar y asegurar una labor pertinente por parte del equipo, deben ser identificadas y tenidas en cuentas las siguientes normas.

- **Constitución Política de Colombia. En su artículo 15**, a la letra dice: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".[20]

- **Ley 599 del 2000 "Código Penal Colombiano.** En su Título VII Bis, Capitulo I. se manifiestan los delitos de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos: En esta parte de la norma se tipifican los delitos que generalmente cometen los

[20] Constitución política. (s. f.). Recuperado 16 de noviembre de 2020, de http://www.secretariasenado.gov.co/index.php/constitucion-politica

delincuentes cibernéticos, describiendo las modalidades que más se presentan en Colombia.[21]

- **Ley 1581 de 2012 Protección de Datos Personales**. En su Título IV. Derechos y condiciones de legalidad para el tratamiento de datos. Norma que se expide para proteger a los dueños de datos personales, con el fin de que estos no sean usados ni tratados sin su debido consentimiento. Gracias a esta norma se deja claro cuáles son los tipos personales que pertenecen a un usuario y como estos debe ser protegidos por quien los tiene bajo su responsabilidad.[22]

- **Ley 1273 de 2009 "De la Protección de la información y de los datos**. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Con la adhesión de estos artículos al código penal colombiano, se busca proteger el bien jurídico tutelado de los datos, de todas las personas en el país, imponiendo una pena de prisión, que buscara disuadir y castigar a los delincuentes cibernéticos o a cualquier ciudadano que trasgreda el uso indebido de sistemas informáticos y la información privada que este contenida en ellos.[23]

- **LEY 1928 DE 2018.** adhesión al Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Es un tratado internacional, que vincula en materia penal, a los estados adheridos al mismo, donde se tipifican herramientas para perseguir los delitos relacionados con la transgresión de sistemas informáticos y los datos privados contenidos en estos, igualmente deja claro las pautas de

[21] Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_0599_2000]. (s. f.). Recuperado 16 de noviembre de 2020, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html
[22] Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. (s. f.). Recuperado 16 de noviembre de 2020, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
[23] Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (s. f.). Recuperado 16 de noviembre de 2020, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

cooperación entre los estados miembros, para la investigación de delitos informáticos. [24]

- I**SO/IEC 27000.** estándares mejores prácticas recomendadas en Seguridad de la información. Es un compendio de estándares internacionales, que guían a cualquier entidad en la creación, implementación, mejora y mantenimiento de un sistema de gestión de seguridad de la información.[25]

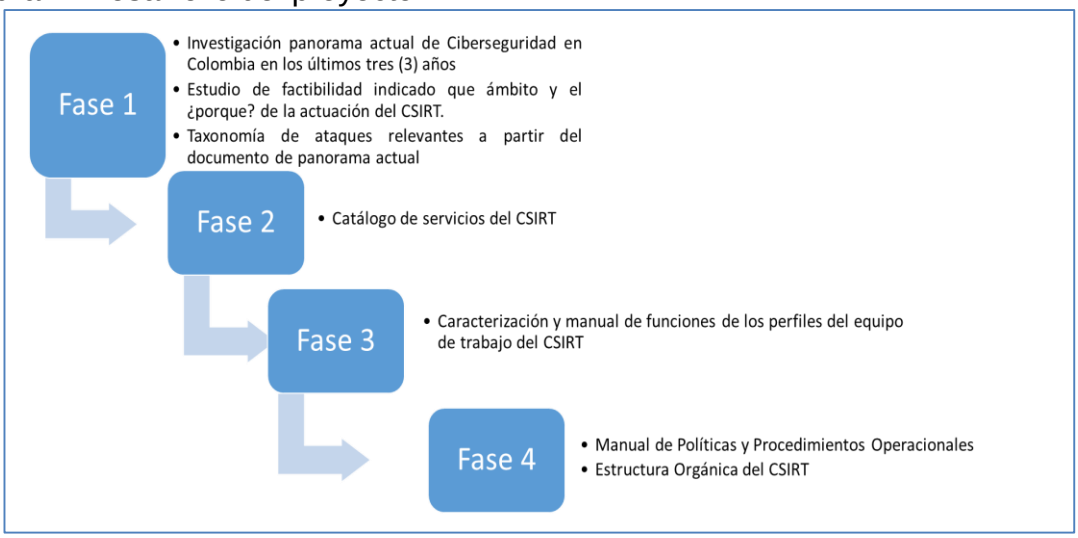
- **Ley 527 de agosto 18 de 1999**. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. es la norma que brinda es estatus de legalidad al documento electrónico y deja claro las pautas para que este tenga esta naturaleza y como se debe demostrar su no repudio.[26]

[24] Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_1928_2018]. (s. f.). Recuperado 16 de noviembre de 2020, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html
[25] ISO/IEC 27000:2018. ISO. Recuperado 16 de noviembre de 2020, de https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73906.html
[26] Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_0527_1999]. (s. f.). Recuperado 16 de noviembre de 2020, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

5 DISEÑO METODOLÓGICO

El presente proyecto es de carácter aplicado, por lo cual su fundamentación está relacionada con la resolución de un problema propuesto desde el contexto imaginado de una compañía de seguridad informática, que requiere se documente la implementación de una CSIRT comercial desde la parte directiva.

Figura 1. Desarrollo del proyecto



Fuente: “elaboración propia”

5.1 FASE 1: DELIMITAR EL ÁMBITO DE ACTUACIÓN DEL CSIRT BASADO EN EL CONTEXTO Y PANORAMA ACTUAL DE CIBERSEGURIDAD EN COLOMBIA.

Para lograr cumplir el objetivo de la fase uno, se deben realizar las siguientes actividades:

5.1.1 Investigación panorama actual de Ciberseguridad en Colombia.

a. Se realizará una revisión bibliográfica de los autores más reconocidos a nivel nacional e internacional, en temas de ciberseguridad y ciberdelincuencia, entre los que se encuentran, la Policía Nacional de Colombia, el centro cibernético Policial, Fiscalía General de la Nación, la Organización de estados Americanos OEA, donde se logren establecer cifras y análisis del contexto nacional en la materia.

b. Se diseñarán gráficos estadísticos, que muestren de manera descriptiva, los resultados de la investigación de la tendencia de denuncias y reportes de incidente informáticos hechos a las autoridades del país.

c. Con la investigación bibliográfica recolectada y los gráficos a diseñar, según lo dispuesto en el punto anterior, se elaborará y se expondrá a través de un análisis criminológico descriptivo, la situación de los ataques más relevantes en Colombia y su tendencia en los últimos años.

5.1.2 Estudio de factibilidad indicado el ámbito de actuación del CSIRT.

a. Se realiza revisión bibliográfica, que permita determinar los tipos de CSIRT, que se pueden diseñar, enfocando la lectura en entidades que sean pertinentes en el tema como son el Centro de Investigación en Matemáticas de zacateca México, la Agencia Europea de Seguridad de las Redes y de la Información ENISA y la Organización de Estados Americanos OEA.

b. Desde la identificación de los tipos de CSIRT que existen en el mundo, sus requerimientos para ser implementados y el análisis de situación actual de Colombia en el tema, se buscara delimitar el ámbito de actuación de la organización a crear.

5.1.3 Taxonomía de ataques relevantes a partir del documento de panorama actual.

a. Tomando como referencia el análisis del panorama actual de la ciberdelincuencia en Colombia y la bibliografía a estudiar, se listarán los tipos de ataques que son utilizados en Colombia, las herramientas, las vulnerabilidades más explotadas, los tipos de víctimas preferidos y la tipificación penal de las actividades que se relacionan al Cibercrimen.

b. Se realizará un gráfico que relacione y explique, la manera como todos los elementos descritos en el punto anterior, convergen para la existencia y crecimiento de la problemática del Cibercrimen.

5.2 FASE 2: ESTABLECER LOS SERVICIOS QUE PRESTARÁ EL EQUIPO CSIRT

Con el fin de poder cumplir el objetivo, de establecer los servicios que se deben prestar a la comunidad, teniendo en cuenta, las funcionalidades del CSIRT y la situación de la ciberseguridad en Colombia, se realizara lo siguiente:

5.2.1 Diseñar Catálogo de servicios del CSIRT.

a. Tomando como referencia las citas planteadas en la presente investigación y el resultado del desarrollo de los puntos antes nombrados, se identificaran los servicios pertinentes con los que iniciara el CSIRT.

5.3 FASE 3: DESARROLLAR LAS TABLAS DE CARGOS Y PERFILES NECESARIOS EN EL FUNCIONAMIENTO DEL CSIRT

5.3.1 Definir el manual de funciones de los perfiles del equipo de trabajo.

a. Teniendo como referencia, el catálogo de servicios y el ámbito de actuación del equipo, los cuales se identificaran según lo previsto en los puntos anteriores, se buscara diseñar los cargos necesarios para cumplir con las actividades del CSIRT.

5.4 FASE 4: DEFINIR LA ESTRUCTURA ORGANIZACIONAL, LAS POLÍTICAS Y MANUALES DE PROCEDIMIENTOS OPERACIONALES ESTANDARIZADOS DEL CSIRT.

5.4.1 Diseñar el manual de Políticas y procedimientos Operacionales.

a. Se realiza revisión bibliográfica, que permita identificar las políticas y procedimientos mínimos y obligatorios para el funcionamiento de un CSIRT, teniendo como referentes algunos manuales y guías internacionales que ayuden a la implementación de un equipo de respuesta a incidentes, como son los documentos de la Agencia Europea de Seguridad de las Redes y de la Información ENISA[27] y la Organización de Estados Americanos OEA.[28]

[27] Enisa, « Cómo crear un CSIRT paso a paso» Enisa, 2006. [En línea]. Recuperado de: https://www.enisa.europa.eu › publications › at_download › fullReport. [Último acceso: 02 12 2019].

[28] OEA (2002) Buenas Prácticas para establecer un CSIRT nacional. Recuperado de: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

b. Teniendo como insumo para el desarrollo de estas políticas y procedimientos, la investigación bibliográfica que se desarrollara, la información del tipo de CSIRT que se quiere implementar y sus servicios a ofertar, se buscara desarrollar unos mecanismos de seguridad de los datos y su gestión acordes a las necesidades y recursos.

5.4.2 Definir la estructura orgánica para el CSIRT

a. Tomando como insumo la información bibliográfica citada en el desarrollo de la presente investigación y la información obtenida del desarrollo del tipo de CSIRT, servicios a prestar y cargos necesarios, se desarrollara el organigrama, donde se identificaran las áreas necesarias para la puesta en marcha de la empresa.

6 DESARROLLO DE LOS OBJETIVOS

6.1 DELIMITACIÓN DE ACTUACIÓN CSIRT COMERCIAL

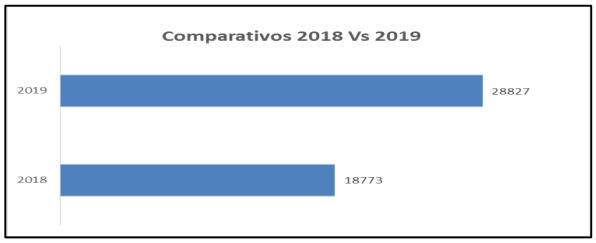
6.1.1 Panorama Actual De Ciberseguridad En Colombia. La necesidad de elaboración de este trabajo, se concentra en el diseño documental pertinente para la creación de un Centro de Respuesta a Incidentes Cibernéticos CSIRT, el cual prestará servicio de protección de la información a clientes en Colombia.

Los conceptos aquí definidos se encuentran relacionados en documentos, como el informe del balance de Cibercrimen en Colombia 2017, en el último documento de Tendencias de Cibercrimen en Colombia 2019-2020, desarrollado por un grupo de entidades gubernamentales y privadas expertas en el tema de Ciberseguridad en el País, igualmente se relacionan documentos que definen la manera más apropiada para la creación del portafolio de servicios de un CSIRT, desarrollado por instituciones académicas y organizaciones internacionales como son el Centro de Investigación en Matemáticas de zacateca México, la Agencia Europea de Seguridad de las Redes y de la Información ENISA y la Organización de Estados Americanos OEA, los cuales ayudaran a analizar el adelanto de la propuesta.

- ***Situación De Ataques cibernéticos Relevantes en Colombia.*** La información estadística analizada en este documento se divide en dos tipos, la primera es la información reportada a través del CAI virtual de la Policía Nacional de Colombia, sobre los incidentes informáticos presentados en Colombia y la segunda es el dato de denuncias interpuestas ante la Fiscalía General de la Nación, por delitos informáticos.

  En la figura 1, se muestran los casos reportados ante el CAI virtual de la Policía Nacional, donde debemos tener en cuenta, que muchas veces estos no son denunciados ante la fiscalía General de la Nación, como delito y solo sirven como referente de la problemática que se está presentando en el ciberespacio.

Figura 2. Comparativos incidentes en Ciberdelitos años 2018 y 2019



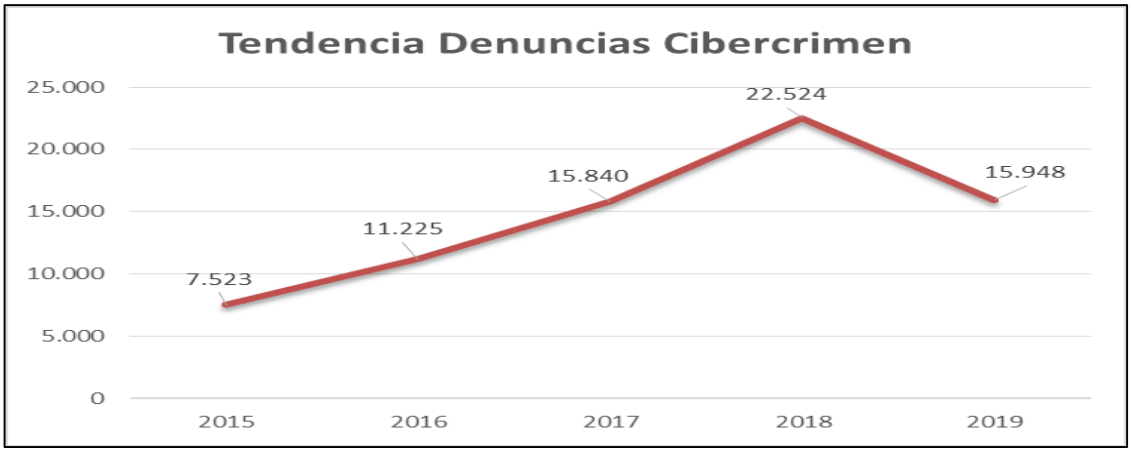
54%

Fuente: “elaboración propia”, con base en datos de: Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

El Cibercrimen en Colombia aumenta exponencialmente todos los años, ya que se denota un incremento del 54% de los incidentes recepcionados desde la plataforma del CAI virtual de la Policía Nacional, lo que nos deja ver la gran problemática que sufre la sociedad del país, donde se muestra que económicamente las afectaciones a las empresas y las personas son muy grandes.

El la figura 3 se puede observar la tendencia en los últimos 5 años, de denuncias interpuestas por casos que se tipifican como delito informático en el código penal colombiano en su artículo 269.

Figura 3. Tendencia denuncias de delitos informáticos

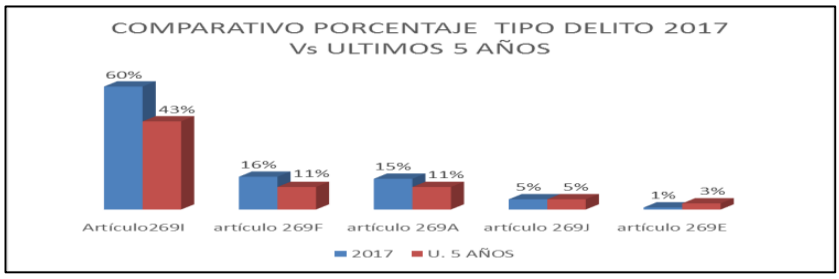


Fuente: “elaboración propia”, con base en datos de: Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

La tendencia de denuncia de los delitos informáticos, por parte de los colombianos tiene una aumento hasta el año 2018, pero para el año 2019 se denota un descenso en esta actividad, lo que se ve preocupante, si se evidencia que los incidentes reportados a la Policía van en aumento cada año y las personas no deciden denunciar estos hechos, dando oportunidad a los delincuentes a que puedan seguir operando, con estas modalidades maliciosas de manera más fácil a través de la impunidad y la poca investigación de los mismos.

En la figura 4, se observa el comparativo de los tipos penales más denunciados en Colombia sobre delitos informáticos, donde se denota tendencia de diminución de las infracciones que eran más denunciadas y aparece aumento de querellas en otros hechos, que poco se visibilizaban en las investigaciones penales.

Figura 4. Tendencia Tipos Penales de delitos informáticos

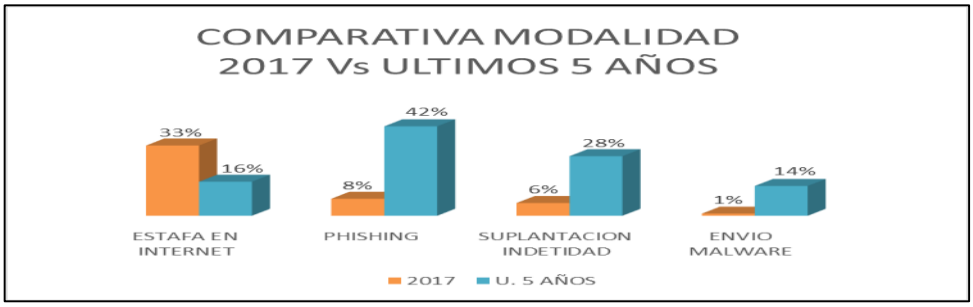


Fuente: “elaboración propia”, con base en datos de: Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Dentro de la información de denuncias en delitos informáticos tipificados en el código penal, se pueden evidenciar que históricamente las conductas más cometidas en el país, son: primero el articulo 269I Hurto por medios informáticos, el cual presenta la mayor participación, el segundo es el articulo 269F Violación de datos personales, el tercero es el artículo 269A Acceso abusivo a un sistema informático, el cuarto es el artículo 269J Transferencia no consentida de activos y el quinto es el artículo 269E Uso de software malicioso. Este último artículo presenta un aumento progresivo, lo que indica que los delincuentes cada vez se tecnifican más, para cometer sus ilícitos.

En la figura 5, se puede analizar la tendencia que se presenta en las modalidades de incidentes informáticos, que más afectan a los colombianos en los últimos 5 años, donde el Phishing y la suplantación de identidad siguen vigentes.

Figura 5. Comparativa modalidad de Ciberdelitos últimos años



Fuente: “elaboración propia”, con base en datos de: Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Las modalidades de delitos informáticos presentan algunas variaciones en sus tendencias, en este caso se muestra que para el año 2017 el mayor porcentaje lo registro la estafa por internet, pero la tendencia en los últimos años muestra que el phishing ha tomado prevalencia para la comisión de hechos delictivos, igualmente la suplantación de identidad y el envío de malware.

6.1.2 Factibilidad del ámbito de actuación del CSIRT.

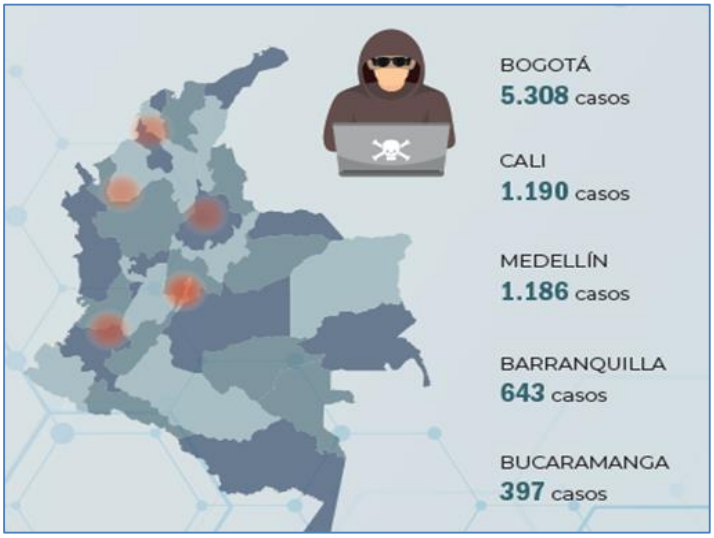
- **Nombre del CSIRT:**

Cibersecurity-CERT

- **Área de Actuación.** El área de atención del equipo de respuestas a incidente tecnológicos, será Colombia, por lo tanto, se tendrán en cuenta los sectores más afectados por la problemática de incidentes y delitos denunciados, según reporte anual de entidades encargadas a nivel gubernamental.

  En la figura 6 se evidencia un mapa de calor, donde vemos la problemática que se presenta en sitios específicos de Colombia, evidenciando muchos incidentes en las ciudades más densas e importantes del país.

Figura 6. Delitos Informáticos Por Ciudades



Fuente: Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Según el último informe de tendencias del Cibercrimen en Colombia (2019-2020), desarrollado por la Policía Nacional, en coordinación con las demás entidades

públicas y privadas expertas en el tema de seguridad digital, “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”[29].

- **Enfoque.** Cibersecurity-CERT es una organización de ámbito nacional, dedicada a apoyar la protección de la información y seguridad de la infraestructura tecnológica del sector comercial colombiano, especialmente en las pequeñas y medianas Empresas (PYMES), ofreciendo soluciones desde la prestación de servicios reactivos, proactivos y complementarios, que permitan garantizar un adecuado manejo de los datos y activos más importantes de los ciudadanos y compañías nacionales.

- **Colaboradores.** Se buscará apoyo de entidades privadas y públicas, las cuales estén comprometidas con el desarrollo y bienestar de la comunidad comercial colombiana a nivel nacional y local, entre estas CONFECAMARA y Cámaras de Comercio de cada Municipio del País, Grupos de investigadores de universidades, la asociación de organizaciones en seguridad tecnológica, entre otros.

- **Clientes.** Podrán ser clientes de la organización cualquier empresa a nivel nacional o local, de ámbito público o privado, teniendo prioridad en prestar servicios a más módico costo económico, y ajustados al contexto de la realidad de las PYMES.

- **Intervinientes.** Se buscará hacer convenios y adhesiones con miembros de organizaciones que apoyan y dan prestigio a la labor a desarrollar, los cuales estén relacionados con temas de seguridad informática y equipos de respuesta a incidentes, como son el Ministerio de las TIC, Forum of Incident Response and Security Teams (FIRST)[30], Centro Cibernético policial, Fiscalía General de la Nación, Fuerzas Militares, entre otros.

- **Ámbito de actuación.** El ámbito de operación de Cibersecurity-CERT, como CSIRT Comercial se basa en la atención de clientes comerciales, los cuales por limitaciones económicas o de infraestructura empresarial, no contemplen viable

[29] Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020. pág. 10

[30] First—Improving security together. (s. f.). FIRST — Forum of Incident Response and Security Teams. Recuperado 21 de julio de 2020, de https://www.first.org/

la creación de un Equipo de Respuesta ante Emergencias Informáticas interno, originando la necesidad de contratar estos servicios, teniendo en cuenta los requerimientos particulares de cada entidad.

6.1.3 Taxonomía De Ataques Relevantes En Colombia. Con el fin de comprender y entender la relación que tienen los diferente actores y elementos que facilitan los incidentes informáticos en el país, se listan y explican cada uno de estos, así:

- **"Tipos de ataques**. Las tendencias de los tipos de atasques identificados en Colombia, generalmente tienen un ámbito de actuación en todo el mundo lo que permite vincularlos a una compleja red de transferencia de conocimientos entre sus ejecutores:

  - BEC: esta técnica combina varias modalidades de engaño, que combinas de manera sistemática logran su objetivo, el cual es lograr el envío de dinero o mercancía de manera voluntaria por parte de la víctima. Entre estas modalidades se encuentran el Phishing, la suplantación de identidad, la ingeniería social, la inteligencia de fuentes abiertas y redes sociales (SOCMINT).

  - RANSOMWARE: Esta definición se usa como combinación de dos palabras en inglés, las cuales son Rasom, que significa rescate y ware lo que hace referencia a software, el objetivo de este método delictivo es el de secuestrar datos de un dispositivo electrónico, con el fin de pedir un beneficio económico, a cambio de devolver estas información, generalmente se requiere de modalidades como el Phishing, la ingeniería social, el envío de malware y el Fake WhatsApp.

  - DDOS. Este es un método más técnico que se enfoca en verificar las vulnerabilidades de sitios WEB, con el fin de buscar sobrepasar la capacidad de servicio para el cual fueron creados, buscando hacer que colapsen y no funcione. Este método es muy utilizado por activistas cibernéticos, que quieren protestar por algún ideal político o social, pero también puede ser usado por delincuentes para solicitar dadivas económicas a cambio de restablecer estos servicios. La inteligencia de fuentes abiertas (OSINT) y redes sociales (SOCMINT), son las modalidades más usadas para obtener datos que identifiquen los vectores de ataque y herramientas a usar.

  - MALWARE. Esta técnica es muy implementada con el fin de dañar sistemas de información o modificar su funcionamiento, con el fin de obtener datos o acceso a maquinas que siendo manipuladas pueden generar ganancias

económicas. Las maneras más comunes de infectar computadoras con este ataques, se hace a través del Phishing, la suplantación de identidad, la ingeniería social, la inteligencia de fuentes abiertas y la visita de sitios WEB infectados.

- SIM SWAPPING. El medio fundamental para lograr el objetivo principal de este ataque, se consigue gracias a la modalidad de la ingeniería social, que se hace a los proveedores de servicios de telefonía móvil, a los cuales engañan para que en una SIM nueva, se le ponga el número los datos del teléfono de la víctima, con lo cual tienen acceso a todos los mensajes, llamas y servicios de aplicaciones, ya con esto se inicia a realizar diferentes transacciones tanto de datos como de dinero.

- CRYPTOJACKING. Con el crecimiento del uso de las cryptomonedas, también se requiere de más cryptominería, que ponga a disposición este servicio, la cual en aspectos de hardware y procesamiento, demanda de una gran inversión económica, por lo que los delincuentes cibernéticos han decidido apoderarse de estos recursos a través programas maliciosos que redireccionan este valioso elemento a sus equipos, desde los computadores de las víctimas que son infectadas, consiguiendo evitar tener que comprar más máquina para realizar minería de monedas virtuales.

- **Herramientas**. Para lograr con éxito, cualquiera de los ataques informáticos relacionados anteriormente, estos además de utilizar modalidades que faciliten los mismo, también requieren de herramientas que se desarrollan teniendo en cuenta la necesidad del mismo:

  - Mulas Monetarias. Son persona que de manera consciente o mediante engaño, prestan sus cuentas bancarias para la consignación de dineros producto de delitos cibernéticos, el uso más común se da en casos de ataque tipo BEC, done el dinero que es obtenido mediante engaño a empresas, es distribuido en cuentas bancarias de Money Mules, como también se conocen en el medio de la seguridad estos individuos.

  - Cuentas Bancarias con Datos Simulados. Esta herramienta se está usando mayormente dentro de los ataques BEC, estas cuentas bancarias son abiertas con datos, donde simulan ser clientes de la empresa víctima o un directivo de la misma, con el fin de que los dineros girados mediante engaño lleguen a estos lugares.

  - Servidor malicioso. Cuando se inicia una ataque de Ransomware, el primer recurso que usa el delincuente es la configuración de un servidor malicioso,

desde donde se conecta a la maquina victima e instala los software necesarios para lograr el cifrado de los datos, con este paso generalmente el ciberdelincuente evade dar su posición geográfica, ya que estos servidores se encuentran normalmente, en países que no facilitan la cooperación entre autoridades, para la verificación de estos registros, que podrían darnos un rastro del lugar desde donde de origina este hecho.

- MALWARE. En algunos casos se puede referir a malware como un ataque, pero igualmente este también puede llegar a ser una herramienta para lograr concretar otro tipo de ataque. Dentro de los ataques que usan el malware como herramienta, se encuentran el Ransomware, el SIM Swapping y el Cryptojacking.

- Criptomoneda. Estos son tipos de moneda virtual, las cuales utilizan la tecnología blockchain, para el almacenamiento seguro de los datos de las cuentas y transacciones, pero igualmente se torna más complejo de rastrear para los investigadores de las entidades de justicia, lo que lo hace útil en los ataques de ransomware y DOS, ya que la usan como moneda exigida para la devolución de los datos secuestrados o restablecimiento de los servicios afectados.

- Redes BOTNETS. Esta es una herramienta que se prepara o se adquiere con antelación del ataque, esta es una red de computadoras infectadas con malware, el cual permite el control de sus funciones y capacidades para amplificar un ataque. Usualmente estas redes de equipos zombis se usan en ataques DDOS o de Malware.

- Redes Darknet. La red oscura es la parte de internet que no se encuentra indexado en los buscadores más conocidos de la red, pero además son sitios que son de acceso peligroso para una personas poco experimentadas para entrar en estos terrenos del ciberespacio, en estos se encuentra información ilegal que permite ampliar el arsenal de herramientas de un delincuente cibernético, pasando por la venta de malware, datos personales robados, información de tarjetas de crédito clonadas, pornografía infantil, drogas, entre otros.

- **Vulnerabilidades**. Se debe tener en cuenta que para realizar cualquier fraude, ya sea en la vida real o en la virtualidad, el primer paso del delincuente es la búsqueda de las fallas o errores que se cometen por el sistema que rodean al objetivo, en el caso del ciberespacio, generalmente confluyen vectores de ataque desde lo real y lo digital.

- Correo Electrónico. Este es uno de los puntos de ataque más utilizados, al momento de que los delincuentes requieran de autorización por parte de la víctima para acceder a sistemas o recursos ajenos, es muy común encontrar la vulneración de este elemento en casos de fraude BEC y RANSOMWARE.

- Persona confiada. En la modalidad de ingeniería social, el primer factor a identificar en el comportamiento de las víctimas, es un nivel de confianza y desconocimiento, al momento de utilizar sistemas informáticos, ya que esto abre una de las puestas más grandes para ataques como BEC, RANSOMARE, DDOS, MALARE Y CRIPTOJAKING.

- Sitios Web no asegurados. El hecho de que un sitio Web no cuente con mecanismo que aseguren un nivel mínimo de protección contra intentos de ingreso o espionaje, deja expuesta mucha información de una persona o compañía, generalmente esto se evalúa por los delincuentes a través de técnicas de evaluación de vulnerabilidades, los cuales le dará un contexto de otras herramientas que podría utilizar para conseguir un ataque positivo.

- WhatsApp. A pesar de que los dueños de esta aplicación, siempre buscan mejorar sus sistemas de seguridad, para evitar el daño a la privacidad de sus clientes, estos mecanismos se ven afectado por la confianza y falta de conocimiento de las personas que lo utilizan, lo que generalmente da la oportunidad a los ciberdelincuentes de utilizar este medio como parte del espionaje que se puede hacer, para obtener datos relevantes, que faciliten la utilización de modalidades de ingeniería social.

- Sistemas Vulnerables. Generalmente los sistemas que más se buscan quebrantar, son los de base de datos, ya que estos aseguran información muy valiosa para cualquier empresa, igualmente el objetivo de entrar a estos quipos es el de modificar datos que permitan engañar a la víctima y lograr que esta realice operaciones en beneficio de los atacantes.

- Teléfonos Móviles. El concepto de la telefonía cambio radicalmente, cuando estos aparatos pasan de ser un medio de comunicación por vos, a convertirse en un equipo de cómputo portátil y versátil; Pero este logro no fue gratuito, ya que esto provocó que para lograr que en un elemento tan pequeño se pueda realizar funciones similares a la de un ordenador, esto también redujo la seguridad del sistema operativo y por consiguiente es más fácil vulnerarlo, sumado a esto se evidencia el alto riesgo de pérdida y espionaje de datos, si se tiene en cuenta que en estos dispositivos se está guardando información muy privada de personas y compañías.

- **Tipos de víctimas.** Según el tipo de ataque, la modalidad y las herramientas que posean los delincuentes informáticos, así mismo estos evaluaran el tipo de victima que pueda presentar las mayores posibilidades de vulnerabilidades a explotar:

  - PYMES. La pequeña y mediana empresa, es una de las victimas más apetecidas en estos momento por los ciberdelincuentes, ya que estas poseen un capital financiero no despreciable, pero no suficiente para reconocer e implementar medidas de seguridad en sus sistemas informáticos, por lo cual presenta una oportunidad clara de obtener un beneficio económico apreciable, con un nivel de esfuerzo no muy exigente, tanto en tiempo como en herramientas de ataque.

  - Personas Naturales. Esta es la segunda víctima en donde más se concentran los criminales en el ciberespacio, ya que en Colombia se presenta una desconocimiento alto, por parte de las personas, sobre las medidas mínimas de seguridad para utilizar sistemas informáticos, ya sean equipos de telefonía móvil o computadores, lo que los hace muy vulnerables a ataques que involucren sus datos personales y cuentas bancarias.

  - Empresas de Gobiernos Locales. En estos casos se presenta una situación muy similar a lo que pasa con las PYMES, pero generalmente no es por falta de recursos, sino por falta de conocimiento de las medidas que existen en el mercado, que si están al alcance de esta población, agravando la situación cuando los delincuentes reconocen que estas entidades manejan recursos muchos más grandes.

  - Grandes empresas. Por ultimo en el país se presentan ataques a grades compañías, que a pesar que cuentan con algunas medidas de seguridad, están no son gestionadas de la mejor manera, esto debido al desconocimiento de los estándares mundiales en ciberseguridad que van evolucionando al mismo ritmo de la cibercriminalidad, para los atacantes estos fraudes son más complicados de llevar a cabo, pero dejan unos beneficios muchísimo mayores.

- **Tipificación Penal.** Debido al gran aumento de los delitos informáticos en el País y a su poca legislación para castigar a los autores de estos hechos, se decide en el año 2009, mediante la ley 1273, incluir en el código penal colombiano una nuevo bien jurídico a proteger, el cual busco tipificar los comportamientos que tiene relación con los ataque información y modalidades anteriormente se han nombrado.

- Hurto por Medios Informáticos. El que, superando medidas de seguridad informáticas, realice la conducta de Hurto, manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

- Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

- Acceso abusivo a un sistema Informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

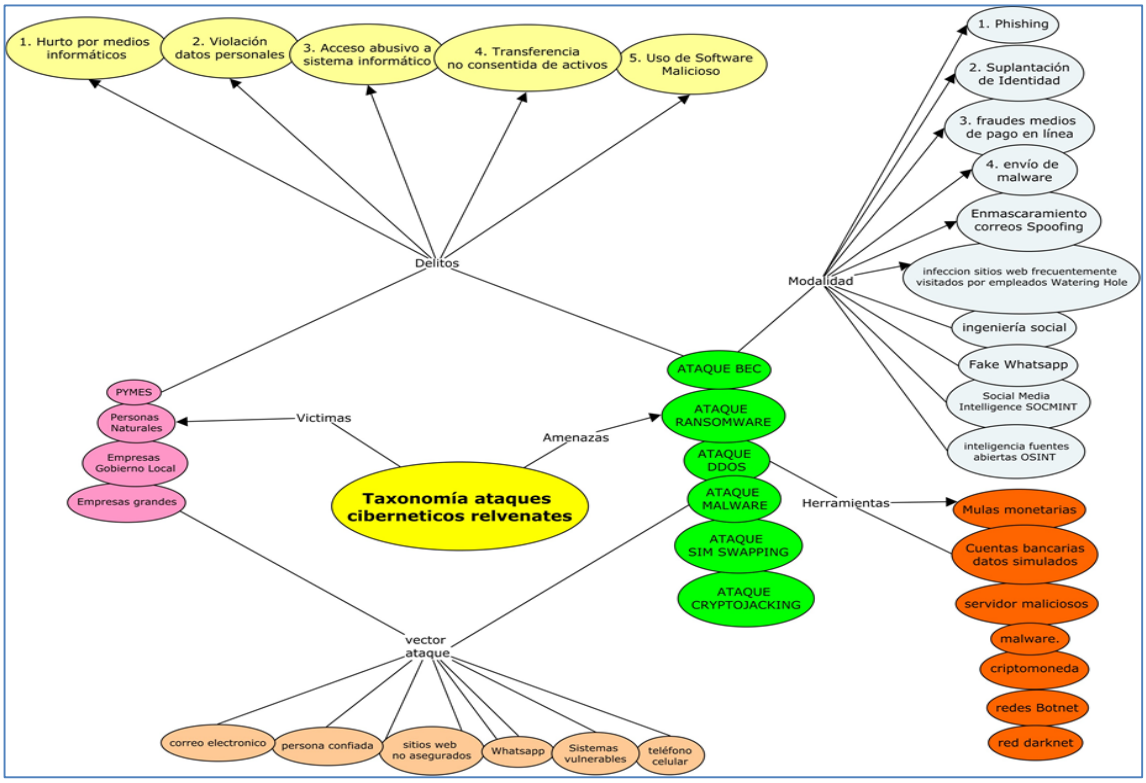
- Transferencia no consentida de Activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.

- Uso de Software Malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos."[31]

6.1.4 En la figura 7, vemos una explicación de los tipos de ataques, que son utilizados por los ciberdelincuentes en Colombia, al igual que las herramientas utilizadas, las vulnerabilidades más explotadas a sus víctimas preferidas y la tipificación penal, que se podría indilgar en caso de que produzcan capturas en las investigaciones.

[31] Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020. pág. 6

Figura 7. Taxonomía de ataques relevantes en Colombia



Fuente: “elaboración propia”, con base en datos de: Ceballos, A, Bautista, F, Mesa, L, ARGÁEZ, & Durán, A. (2019). Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia. Recuperado de http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

El delito cibernético tanto en Colombia, como en el resto del mundo, en los últimos años, ha generado una dinámica delictiva muy clara, la cual va modificándose gradualmente según las nuevas tecnologías que van apareciendo.

Dentro de las amenazas más preocupantes y constantes que se presentan en el país, se evidencian 6 tipos de ataques, los cuales, utilizando las modalidades de incidentes, herramientas maliciosas y analizando los vectores de ataque que son facilitados por las víctimas, logran mantenerse vigentes.

6.2 SERVICIOS CSIRT COMERCIAL

Teniendo en cuenta el panorama actual del país, donde se logra establecer la Taxonomía de ataques relevantes, el portafolio de servicios con el que se propone iniciar el CSIRT, los servicios a ofrecer se dividen en tres grupos, así:

6.2.1 Servicios Reactivos. Estos tipos de servicio son la base fundamental de la misión de un CSIRT, por tanto, generalmente son los primeros en implantarse:

- **Gestión de incidentes**. Es un servicio que le garantizará a la empresa, el manejo adecuado del lugar de los hechos en caso de un incidente informático, ya que este será fundamental en la mitigación de los daños a la infraestructura y los datos, al igual que en la pertinente recolección de evidencia digital, que se podrá utilizar en una futura investigación, reclamación o demanda legal.

- **Respuesta a vulnerabilidades**. La empresa tendrá una mayor percepción de seguridad en sus sistemas, al contar con la ayuda de investigadores, que estarán notificándolo de las últimas novedades en amenazas, que puedan poner en riesgo la integridad de sus activos de información.

- **Respuesta a artefactos maliciosos**. Dentro de las modalidades de ataques, que más ha aumentado en el ciberespacio y que afectan a empresas en Colombia, está el uso de software malicioso, el cual no es fácil de detectar por personas que no tengan experiencia en el tema. Con este servicio se busca atender la necesidad de encontrar este tipo de archivos en un sistema de información y poder determinar su funcionamiento básico.

6.2.2 Servicios Proactivos. Para la adopción de estos tipos de servicios, se toman más en cuenta la taxonomía y situación de riesgo que presentan los clientes que se atenderán, los cuales serán especialmente PYMES en Colombia:

- **Monitoreo y alertas (primer nivel).** Este servicio permite verificar y alertar sobre posibles afectaciones que pueda estar sufriendo la empresa que lo contrata, ofreciendo informes que den una expectativa del nivel de seguridad que presenta la compañía, lo que le permitirá una toma decisiones más acertaba para la gestión y protección de los datos, por parte de la gerencia. Igualmente permitirá saber que no se es víctima de un posible ataque en proceso.

- **Investigación y desarrollo (primer nivel)**. Al tener contratado este servicio dispondrá de información de investigaciones actuales sobre temas de últimas novedades en ataques y amenazas, donde estos se puedan apoyar de la tecnología que utiliza en el momento la empresa contratante.

6.2.3 Servicios Complementarios. Estos servicios son ajenos a la intervención de la infraestructura tecnología, ya que estos se enfocarán más a que el talento humano, este más informado de su responsabilidad en la seguridad informática:

- **Capacitación y educación**. Para este parte se le ofrecerán cursos específicos a las labores que se desarrollan en cada departamento de la empresa y el manejo de las tecnologías que se emplean, tanto desde el aspecto técnico y de prevención.

- **Concientización**. Se brindará charlas generales sobre el tema de ciberseguridad, dando el enfoque que el contexto que requiera, por ejemplo, seguridad empresarial, últimas amenazas en el ciberespacio, el teletrabajo seguro, seguridad de menores en la red, entre otras.

6.3 TABLAS DE CARGOS Y PERFILES NECESARIOS EN EL FUNCIONAMIENTO DEL CSIRT.

La presente tabla de cargos y perfiles, es desarrollada teniendo en cuenta el alcance y servicios que gestionara el mismo.

TABLA DE CARGO Y PERFIL **SERVICIO DE DIRECCIÓN**
I. IDENTIFICACIÓN DEL CARGO: Cargo: Director. Organigrama: Dirección
II. MISIÓN Apoyar la protección de la información y seguridad de la infraestructura tecnológica del sector comercial colombiano
III. FUNCIONES - Dirección estratégica del CSIRT. - Supervisión general de grupos de trabajo. - Verificación del personal a contratar - Asistencia a reuniones estratégicas con miembros y directivos de entidades externas e internas.
IV. EDUCACIÓN - Título Universitario en Tecnologías de la información u otro afín.

- Especialización o maestría en seguridad informática o de la información.

FORMACIÓN BÁSICA

- Deseable posgrado en gerencia en TI.
- Alguna Certificación en CISSP, CISM, CISA u homologable.

V. COMPETENCIAS

- Experiencia mínima de 9 años en cargos técnicos relacionados con le seguridad informática o de la información.
- Tres años mínimos en cargo de gerencia.
- Deseable experiencia en cargos o similares que involucre el servicio de respuesta a incidentes de TI.

VI. CONDICIONES DEL TRABAJO

- Mayor compromiso y disponibilidad para asumir los retos
- Sometido regularmente a ambientes de estrés y exigencia de toma de decisiones.

TABLA DE CARGO Y PERFIL
SERVICIO DE DIRECCIÓN

I. IDENTIFICACIÓN DEL CARGO:

Cargo: Gestor De Incidentes.

Organigrama: Operaciones

II. MISIÓN

Garantizar un adecuado y legal manejo del lugar de los hechos en caso de un incidente informático.

III. FUNCIONES

- Análisis, monitoreo, registro y respuesta a incidente
- Coordinación a las respuestas de incidentes.
- Colaboración interna para respuesta a incidentes.

IV. EDUCACIÓN

- Título Universitario en Tecnologías de la información u otro afín.
- Especialización o maestría en seguridad informática o de la información.

FORMACIÓN BÁSICA

- Deseable curso respuesta incidentes.
- Curso informática forense
- Certificaciones (CISSP, CISM, CISA o similar).

V. COMPETENCIAS

- Experiencia mínima de 5 años en cargos técnicos relacionados con la seguridad informática o de la información.
- Experiencia en operaciones en respuesta a incidentes.
- Deseable experiencia en metodologías de gestión ágiles

VI. CONDICIONES DEL TRABAJO

- Receptivo y metódico para la identificación incidentes y su respuesta.
- Sometido regularmente a ambientes de estrés y resolución rápida de problemas.

TABLA DE CARGO Y PERFIL
SERVICIO DE DIRECCIÓN

I. IDENTIFICACIÓN DEL CARGO:

Cargo: Analista/Investigador.

Organigrama: Investigación y desarrollo

II. MISIÓN

Notificar de las últimas novedades en amenazas, que puedan poner en riesgo la integridad de los activos de información de los clientes, al igual que producir investigaciones actuales sobre temas de últimas novedades en ataques y amenazas cibernéticas.

III. FUNCIONES

- Realizar investigaciones sobre necesidades de seguridad específicas.

- Desarrollar Boletines educativos e investigativos sobre riesgos cibernéticos y técnicas de prevención.
- Monitoreo de sistemas de información de los clientes.
- Verificar y alertar sobre posibles afectaciones que pueda estar sufriendo los sistemas de los clientes.

IV. EDUCACIÓN

- Título Universitario en Tecnologías de la información u otro afín.
- Conocimientos en varios lenguajes de programación.
- Estudios en seguridad informática.

FORMACIÓN BÁSICA

- Deseable curso respuesta incidentes.
- Curso informática forense
- Certificaciones (CISSP, CISM, CISA o similar).

V. COMPETENCIAS

- Experiencia mínima de 5 años en cargos técnicos relacionados con la elaboración de proyectos de seguridad en Ciberseguridad.
- Experiencia en investigación y desarrollo.
- Deseable experiencia en metodologías de gestión ágiles

VI. CONDICIONES DEL TRABAJO

- Receptivo y metódico para la identificación incidentes y su respuesta.
- Analítico y proactivo, con deseo de aportar al conocimiento de ciberseguridad.

TABLA DE CARGO Y PERFIL
SERVICIO DE DIRECCIÓN

I. IDENTIFICACIÓN DEL CARGO:

Cargo: Administrador De Sistemas.

Organigrama: Tecnologías de la información

II. MISIÓN

Administrar los sistemas de información del CSIRT, al igual que apoyar la respuesta a incidentes que requieran del conocimiento de sistemas de información y análisis de malware.

III. FUNCIONES

- Mantener y administrar los sistemas de información del CSIRT, siendo el responsable de la seguridad de los datos.
- Apoyar la respuesta a incidentes, donde se requiera conocimiento de sistema de información.
- Detección y análisis de software malicioso.

IV. EDUCACIÓN

- Título Universitario en Tecnologías de la información u otro afín.
- Conocimientos en varios lenguajes de programación.
- Cursos de análisis de malware y forense.

FORMACIÓN BÁSICA

- Deseable curso respuesta incidentes.
- Curso informática forense
- Certificaciones enfocados análisis de malware (CMU, SANS o similar).

V. COMPETENCIAS

- Experiencia mínima de 3 años cargo de administración de sistemas de información.
- Experiencia en análisis de malware.
- Deseable experiencia en trabajo con sistemas criptográficos.

VI. CONDICIONES DEL TRABAJO

- Receptivo y metódico para la identificación incidentes y su respuesta.
- Dispuesto a nuevos aprendizajes.
- Dinámico y polifacético al momento de enfrentar nuevos retos.

TABLA DE CARGO Y PERFIL
SERVICIO DE DIRECCIÓN

I. IDENTIFICACIÓN DEL CARGO:

Cargo: Representante Legal.

Organigrama: Servicios de apoyo

II. MISIÓN

Representar al CSIRT en eventos y prestar formación académica a los clientes, especialmente en la parte legal.

III. FUNCIONES

- Representar ante los clientes y eventos al CSIRT.
- Impartir cursos a clientes en seguridad informática.
- Concientizar clientes a través de charlas sobre la importancia de la seguridad informática.
- Asesorar al personal técnico operativo en los casos que se requiera.

IV. EDUCACIÓN

- Título universitario en Derecho.
- Especialización o maestría en seguridad informática o de la información.

FORMACIÓN BÁSICA

- Formación como docente.
- Curso informática forense
- Deseable Certificaciones (CISSP, CISM, CISA o similar).

V. COMPETENCIAS

- Experiencia mínima de 1 año en cargos de legislación de delitos informáticos.
- Experiencia en docencia o capacitador.

VI. CONDICIONES DEL TRABAJO

- Dinámico y paciente al momento de explicar temas de TI y legales.
- Facilidad para el dominio de diferentes tipos de públicos.

TABLA DE CARGO Y PERFIL
SERVICIO DE DIRECCIÓN

I. IDENTIFICACIÓN DEL CARGO:

Cargo: Gerente De Comunicaciones.

Organigrama: Servicios de apoyo

II. MISIÓN

Realizar marketing del CSIRT, dando a conocer sus servicios y ventajas.

III. FUNCIONES

- Desarrollo y publicación de documentos del CSIRT.
- Desarrollar y mantener actualizada el sitio web de la empresa.
- Manejo de las redes sociales y medios de comunicación.

IV. EDUCACIÓN

- Título Universitario en Tecnologías de la información u otro afín.
- Especialización o maestría en medios de comunicación.

FORMACIÓN BÁSICA

- Formación en desarrollo páginas web.
- Cursos en marketing digital.

V. COMPETENCIAS

- Experiencia mínima de 2 años en cargos relacionados con manejo de medios de comunicación.
- Experiencia en manejo de páginas web.
- Experiencia en marketing digital.

VI. CONDICIONES DEL TRABAJO

- Dinámico y activo en el uso de las redes sociales.
- Manejo adecuado de medios de comunicación.
- Prudencia en el manejo de los mensajes y ruedas de prensa.

TABLA DE CARGO Y PERFIL
SERVICIO DE DIRECCIÓN

I. IDENTIFICACIÓN DEL CARGO:

Cargo: Gerente Triage.

Organigrama: Operaciones

II. MISIÓN

Clasificación y asignación de incidentes de seguridad.

III. FUNCIONES

- Recepción de comunicaciones sobre eventos de seguridad.
- Clasificación de eventos de seguridad reportados.
- Asignación de casos al personal técnico.
-

IV. EDUCACIÓN

- Título Universitario en Tecnologías de la información u otro afín.
- Especialización o maestría en seguridad informática o de la información.

FORMACIÓN BÁSICA

- Formación atención a incidentes.
- Cursos sobre hacking ético o respuesta a incidentes.
- Certificaciones en Information Systems Audit and Control Association (ISACA) o Systems Security Certification Consortium (ISC).
-

V. COMPETENCIAS

- Experiencia mínima de 5 años en cargos relacionados con respuesta a incidentes.
- Experiencia en cargos de supervisión de persona técnico TI.

VI. CONDICIONES DEL TRABAJO

- Trabajo bajo presión.
- Altos conocimientos en diferentes áreas de seguridad TI.
- Manejo de personal técnico.

6.4 ESTRUCTURA ORGANIZACIONAL, LAS POLÍTICAS Y MANUALES DE PROCEDIMIENTOS OPERACIONALES ESTANDARIZADOS DEL CSIRT

6.4.1 MANUAL DE POLÍTICAS Y PROCEDIMIENTOS OPERACIONALES.

- **Política de Clasificación de Información.**

  Objetivo: Garantizar una adecuada clasificación de la información, con el fin de brindar una protección jerarquizada de los datos, sin importar el formato en que se encuentren registrados.

  Alcance: Es obligatorio para todo el personal del CSIRT.

Responsabilidades: Los responsables de la gestión de los datos deben cumplir los protocolos estipulados para garantizar su seguridad.

Administrador De Sistemas: se encargará de ingresar el tipo de activo en el inventario, teniendo en cuenta la clasificación que se asumirá.

Propietario de activo: es el jefe del área a la cual le compete la información el cual deberá realizar la clasificación y etiquetado de los activos.

Miembros del CSIRT: todas las personas integrantes del CSIRT, en todos los niveles deben dar un manejo adecuado a los datos a los cuales tiene acceso.

Criterios de clasificación de la información: los niveles de confidencialidad de los datos serán adoptados teniendo en cuenta el valor, la sensibilidad y las obligaciones legales de la información.

Nivel de Seguridad	Criterios	Restricción a acceso
Pública	Es de interés general y su conocimiento no producirá daño al CSIRT o a sus clientes.	Información disponible para todo el público.
Uso interno	El acceso no autorizado a los datos puede dañar de menor manera a la empresa, pero no causará daño en los clientes.	La información será disponible para todos los empleados y terceros autorizados según su competencia.
Restringida	El acceso no autorizado de la información podrá dañar considerablemente a la empresa, pero no tendría consecuencia en los clientes.	La información está disponible para un grupo específico de empleados y en algunas ocasiones a terceros autorizados.
Confidencial	El acceso no autorizado a los datos causaría un daño irreparable a la empresa y/o afectaría gravemente a algún cliente.	La información es de uso exclusivo de algunas personas del CSIRT.
Datos Sensibles	Son datos de afectación de la intimidad del dueño de los mismo o que su naturaleza afecten su	Información es de uso exclusivo de la empresa y disponible para el titular de la misma.

	dignidad al ser usados sin su permiso, los cuales pueden ser datos de su descendencia de raza o étnica, su posición política, la religión o filosofía de vida que practica, la adhesión sindical, a organizaciones de derechos humanos, sociales, o que impulsen provechos de cualquier partido político o que avalen las garantías y derechos de partidos de oposición, así como información referente a la a la vida sexual, los datos biométricos y la salud.[32]	

- **Política de protección de datos.** Teniendo como referencia la ley 1581 de 2012 y su decreto reglamentario 1377 de 2013, se desarrolla y adopta la presente política de protección de datos.

  Responsable del tratamiento de datos:

  CIBERSECURITY-CERT.
  "Protegemos sus Activos más importantes"
  Calle 14 Sur No. 14 - 23.
  Tel. PBX: (+57 1) 344 3700 Bogotá D.C., Colombia.
  Mail: servicio_cliente @ cibersecurity-cert.com.
  Sitio web: www.cibersecurity-cert.com

  Marco Legal: ley estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013

  Ámbito de aplicación: la presente política se aplicará a los datos registrados en las bases de datos y sistemas de información propios de la empresa.

[32] Ley 581 (2012). Secretaria Senado De La República. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Definiciones:

“a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

e) responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.[33]”

Principios:

a) Confidencialidad: todos los empleados de la empresa que tengan contacto con información, ya sea de su competencia, de las bases de datos o confiada a su poder debe seguir los lineamientos de seguridad de la información que prevenga la divulgación de misma.

b) Integridad: La información que sea procesada por todos los empleados debe ser conservada exacta evitando su eliminación o modificación.

c) Disponibilidad: se debe procurar por la disponibilidad de la información de manera eficiente, siempre verificando la autorización previa para dar acceso a esta.

[33] Ley 581 (2012). Secretaria Senado De La República. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Derechos De Los Titulares. “Los derechos de los titulares de la información son los siguientes:

a) Los Encargados o responsables del Tratamiento deben dar a Conocer, rectificar y actualizar los datos personales. Esta petición se puede realizar frente a datos de tipo inexactos, parciales, fraccionados, incompletos, que puedan inducir al error, o los que cuyo Tratamiento estén explícitamente prohibidos o no tengan autorización.

b) Puede pedirse prueba sobre la autorización que da el dueño del dato al responsable o encargado del tratamiento, para ejercer esta actividad.

c) ha recibir información por parte del encargado o responsable del Tratamiento, cuando se haga solicitud, donde indique el uso que se le dio a la información.

d) Denunciar o interponer quejas ante la Superintendencia de Industria y Comercio, por violaciones al articulado de la ley 1581 de 2012 y las demás normatividades que la adicionen, modifiquen o complementen.

e) Terminar el permiso y/o pedir la cesación, cuando en el proceso de tratamiento se viole los derechos, principios y garantías dadas por la constitución y la ley. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.”[34]

Autorización: Dependiendo del nivel de información y dueño o titular de la misma, se requerirá de este, consentimiento informado para su tratamiento. Este consentimiento se podrá realizar a través del titular o un apoderado y se manifestará mediante un escrito físico o digital que permita verificar la identidad de la persona, del cual se guardará como prueba.

Se deja claro que en cualquier momento el titular o dueño de los datos podrá solicitar que se termine el tratamiento de la información.

Tratamiento al que se someterán los datos: los datos de tipo no sensible serán administrados y utilizados específicamente para situaciones

[34] Ley 581 (2012). Secretaria Senado De La República. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

administrativas y operativas de la empresa, en ningún caso se pueden usar para situaciones personales.

Los datos sensibles solo pueden ser utilizados previa autorización del titular de los mismos, evitando la creación de bases de datos que revele esta información.

Registro base de datos: La empresa procederá al registro de las bases de datos ante la Superintendencia De Industria Y Comercio de Colombia, con el fin de dar cumplimiento a la normatividad del país.

- **Política de retención de información.**

Objetivo: establecer los periodos de retención de los datos, teniendo en cuenta su categoría y nivel.

Alcance: Es obligatorio para todo el personal del CSIRT.

Programa general: Se determinará una persona para cumplir la función de responsable de la protección de los datos, quien determinará los periodos de tiempo de los documentos, teniendo en cuenta su nivel de confidencialidad y categoría.

De igual manera se determinarán excepciones en la prolongación de la retención de datos, teniendo en cuenta, solicitudes externas de nivel judicial o necesidades de prolongación por parte de los integrantes de la empresa, a lo cual se deberá justificar de manera clara.

En caso de aparición de datos o información en diferentes tipos de presentación o contenedor (físico papel, dispositivos electrónicos de almacenamiento, entre otros), los cuales no esté definidos dentro las diferentes políticas referentes a los datos, se asumirá una retención de 6 años.

Preservación de los datos durante el tiempo de retención: durante la conservación de los datos se deberá tener en cuenta los espacios y contenedores, los cuales propenderán por garantizar la preservación de la información durante su retención, teniendo en cuenta los diferentes tipos de presentación de los mismo como son, información, digital, fisca en papel y los mismos activos de información donde se guarden lo registros.

Cumplimiento: la persona asignada como responsable de protección de datos, será el garante de que todos los departamentos y dependencia del

CSIRT, cumplan y ejecuten la política de manera correcta, asesorándolos en las actividades a desarrollar.

El cumplimiento es de carácter obligatorio y el incumplimiento de la misma debe ser notificado al responsable de protección de datos, con el fin de tomar las medidas pertinentes, que encausen un buen proceder.

- **Política de destrucción de información.**

Objetivo: Realizar la destrucción de datos o información, teniendo presente los criterios de retención y procedimientos adecuados para la eliminación de archivos, con el fin de beneficiar a la empresa en la obtención de más espacio de almacenamiento, reducir costos, aumentar la eficiencia y disminuir los riesgos en la seguridad de los datos.

Alcance: Es obligatorio para todo el personal del CSIRT.

Principios: se deberá tener en cuenta las observaciones hechas en la tabla de retención documental, donde se especifican los términos de preservación de los datos y la manera de destrucción teniendo en cuenta la condición en que se encuentren.

a) Se debe tener autorización para la eliminación de los datos, los cuales deben ser concedidos tanto por los clientes involucrados y propietarios de datos, como del responsable de seguridad de la información.

b) La eliminación se debe realizar con métodos que garanticen la seguridad de la destrucción de los datos, verificando que no se puede reconstruir o recuperar.

c) Se promover la eliminación oportuna de los archivos, sin presentar dilación al procedimiento, esto con el fin de evitar fugas de datos.

d) Todo procedimiento de destrucción de archivos debe ser documentado, donde quedaran claros todos los procedimientos efectuados a la información, siguiendo siempre los parámetros básicos creados por el CSIRT.

Procedimiento. Los siguientes son los pasos mínimos requeridos, para dar seguridad y legalidad a la actividad de destrucción de información, los cuales deben ser observados cada vez que se requiera:

a) Verificar los plazos exigidos en la Tabla de retención documental (TRD) del CSIRT, al igual que se debe velar por que la TRD, este aprobada y alienada con las normas del archivo nacional.

b) Se debe realizar un inventario de destrucción de documentos, el cual deberá ser adecuado a la necesidad de eliminación periódica y ordinaria de datos, dejando claro el lugar donde se encuentran los archivos a eliminar y sus posibles copias.

c) Teniendo en cuenta los tipos de soporte documental y contenedor de la información, se debe prepara el método más adecuado para garantizar una total y segura eliminación de los datos.

d) Teniendo presente que la autorización externa para la eliminación de datos, se debe contemplar en la aprobación de la TRD, por parte del archivo nacional, también es importante dejar claro el procedimiento y formatos de autorización interno necesarios para proceder a ejecutar la actividad.

e) La ejecución de la destrucción de datos del CSIRT, debe ser realizada por personas idóneas en dicho tema, teniendo en cuenta el contenedor o formato de los datos, de lo cual debe quedar documentado todo el proceso.

- **Política de divulgación de información.**

  Objetivo: Definir la manera en que se divulgara la información, el tipo de información que se puede dar a conocer, teniendo en cuenta las restricciones el receptor de los datos.

  Alcance: Es obligatorio para todo el personal del CSIRT.

  Declaración De La Política:

  Información Pública. Toda la información que sea púbica, está autorizada a ser difundida, pero siempre teniendo en cuenta, realizarlo a través de los canales creados para tal fin.

  Información de Uso interno. Estos datos solo pueden ser divulgados teniendo en cuenta la autorización del director, el cual permitirá su conocimiento a todos los empleados y terceros que es faculte.

Información Restringida. Los datos de esta categoría solo pueden ser divulgados a un área en específico de empelados y terceros, después de ser autorizados por la dirección.

Información Confidencial. Esta información solo la gestionará personal exclusivo el CSIRT, para lo que, en el momento de requerir divulgación distinta a estas personas, se requerirá de autorización del director, dejando acta de acuerdo de no divulgación firmada por quien entrega y recibe los datos.

Información Sensible. Esta información no puede ser divulgada, ya que está protegida por la ley.

Divulgación interna. Dentro de las dependencias del CSIRT, se agilizará la divulgación de la información, siempre y cuando no se tenga una restricción por su nivel de confidencialidad.

Aspectos Legales. Toda petición externa de información, debe ser canalizada por la dirección, con el fin de que sea verificado su cumplimiento legal.

Pedidos de información. Con el fin de mantener vigente y dinámico el trabajo del CSIRT, este deberá recibir y proporcionar información de otros equipos de respuesta, de una manera ágil y fluida, teniendo como principio, la entrega de datos necesarios para su análisis, teniendo siempre cuidado de estar cumpliendo las normas legales de cada caso. Se debe tener en cuenta que los procesos de información y tipo de datos debe estar autorizado por la Dirección.

Para las peticiones realizada por personal de prensa, se debe tener presente que ningún miembro del CSIRT está autorizado a divulgar información o a dar declaraciones referentes al trabajo que se genera en este, todo debe ser canalizado a través del representante de la empresa, con el fin de que el vea viable la entrega de los datos solicitados, teniendo en cuenta que esto debe ser consultado a la dirección.

- **Política sobre el acceso a la información.**

Objetivo: Facilitar los canales de acceso a la información, teniendo presente la responsabilidad con los datos de los clientes y su privacidad.

Alcance: Es obligatorio para todo el personal del CSIRT.

Comité de acceso a la información: se conformará el comité de acceso a la información, el cual estará precedido por el director, responsable de seguridad de la información, y jefes de área, los cuales tomaran la decisión sobre facilitar algunos datos que sean de niveles restrictivos para el peticionario, se establecerá y clasificaran los datos en los niveles de información y determinaran los procedimientos para el acceso a los datos.

Acceso permanente de información: a través de los medios previstos por el CSIRT, como es la página web de la empresa, canales telefónicos, redes sociales institucionales, se mostrará la mayor cantidad de información pública que pueda ser de interés para la comunidad en general, dentro de la que se encuentra, la estructura orgánica, servicios, numero de contacto, ultimas noticias sobre temas del equipo, normas, convenios, empleos, historia, entre mucha otra.

Excepciones: dentro de la información que no se pude publicar a través de los medios públicos y masivos de la empresa, se dejan fuera del alcance:

a) Todo dato que afecte la privacidad de clientes, empleados, o contratistas del CSIRT.

b) Datos sobre procesos de contratación y licitación que realice la empresa con empresas privadas.

c) Datos sujetos a la norma de secreto profesional de los involucrados en el CSIRT.

d) Información protegida con el derecho de propiedad intelectual.

e) Información judicial de casos especiales o individuales.

f) Otro tipo de información, que en el comité de acceso a información, referencien como no adecuada para publicar.

Proceso de solicitud: cuando se requiera obtener algún tipo de dato que no se encuentre publicado en los medios masivos de la empresa, se debe realizar una petición formal que contenga:

a) Datos de contacto del peticionario
b) La descripción clara y especifica de lo requerido.
c) Las opciones de entrega para dar respuesta a la petición.

Proceso de respuesta: al momento de ingreso de una solicitud de información al CSIRT:

a) El responsable de seguridad de la información, debe registra esta solicitud en un sistema que asegure su organización y seguridad, dando un numero de seguimiento al peticionario.

b) Se verificará que los datos solicitados no se encuentren de dominio público en los medios masivos de la entidad. En caso positivo de encontrar estos datos en alguno sitio de la empresa, se responderá el requerimiento indicando la ubicación.

c) Teniendo presente el tipo de información se remitirá solicitud a la dependencia responsable.

d) Al recibir la respuesta de la dependencia responsable de los datos, se realiza verificación de que los datos no estén dentro de las excepciones.

e) Con la firma de la dirección y visto bueno de la revisión se procede a realizar la entrega de los datos.

f) En caso de que los datos se encuentren dentro de las excepciones descritas en la presente política, se dará la respuesta argumentando los motivos.

- **Políticas de uso apropiado de los sistemas del CSIRT**.

Objetivo: Incluir controles de seguridad y verificación de datos, los cuales son gestionados por los sistemas de información del CSIRT, al igual que definir los procedimientos a seguir en el ciclo de vida de las aplicaciones y hardware de le empresa.

Alcance: Es obligatorio para todo el personal del CSIRT, que administre los sistemas de información e infraestructura que las gestione.

Responsable sistemas de información: el responsable de seguridad de los datos junto con el apoyo y aval de la dirección definirá los controles que se tendrán en cuenta en el momento de desarrollar o adquirir un sistema de información. Además de lo antes especificado también se hará cargo de:

a) Se deberá definir el nivel de criticidad y riesgo de los datos gestionados, lo cuales deberán ser protegidos con sistemas de cifrado.

b) Verificación de los controles implementados en los sistemas de información del CSIRT.

c) Desarrollar el proceso de administración de contraseñas.

d) Estructurar los procedimientos para el remplazo, verificación y auditorías internas sobre los sistemas de información.

Disposiciones: con el fin de salvaguardar la integridad, disponibilidad y confidencialidad de los datos, se deberá cumplir las siguientes consideraciones.

a) Los sistemas de información que se desarrollen o se adquieran a terceros, debe contar con módulos de gestión de usuarios y gestión de privilegios.

b) Dentro de cada sistema se deberá identificar el tipo de información que se gestionará teniendo como referencia los niveles de confidencialidad.

c) En el análisis de la información se debe tener en cuenta los requerimientos legales del lugar donde opere.

d) Todo sistema debe permitir el almacenamiento de registros de auditoria.

e) En el diseño de los sistemas, se deberá proveer la elaboración de mensajes de error de los sistemas con el fin de evitar mostrar datos técnicos a los usuarios.

f) Aplicar técnicas de evaluación de seguridad de sistemas de información en desarrollo.

g) Se debe realizar un análisis de riesgos en la codificación, a las aplicaciones desarrolladas y adquiridas por el CSIRT.
h) Se debe desarrollar un procedimiento que permita testear las vulnerabilidades de los sistemas de información.

i) Elaboración y ejecución de procedimiento de procesamiento de datos de entrada y salida de las aplicaciones, dejando documentado en un informe los resultados.

Protección de los archivos de los sistemas: dentro de los mayores riesgos que tienen los sistemas de información, se encuentran los archivos que componen la aplicación, por esta razón se debe:

a) Cada aplicación de la empresa se le debe asignar un único responsable técnico.

b) Se debe evitar el acceso a los ambientes de producción de software al personal no autorizado.

c) Cada modificación en los sistemas de información deberá contar con un sistema de control de cambios de versión.

d) Los datos usados para pruebas de sistema de información, deben ser ficticios y no pertenecer a los activos de la empresa.

e) Cualquier copia de las bases de datos del CSIRT, que se requiere por una persona ajena a los datos, debe tener una autorización formalmente elaborada.

f) Debe crearse un sistema de protección de códigos fuentes de los programas desarrollados por la empresa.

Control de Cambios: en el proceso de desarrollo y actualización de los sistemas de información, se debe implementar una herramienta de control de cambios, que permitan llevar registro de las modificaciones realizadas a los aplicativos dejando claro las revisiones realizadas y la persona que la ejecuto.

Se debe tener en cuenta que todo cambio de versión, requiere de una revisión de seguridad, la cual será asumida por el responsable de seguridad de la información, al igual que los cambios deberán ser verificados y aceptados por el propietario de los datos, los cuales tendrán en cuenta las posibles afectaciones al procesamiento de la información.

Desarrollo de software por terceros: al momento de requerir la implementación y desarrollo de aplicaciones que sean desarrolladas por personas o empresa ajenas al CSIRT, estos contratos se deberán asegurar de la siguiente manera:

a) Claridad sobre los acuerdos de licencia, propiedad del código fuente y derechos de propiedad intelectual.

b) Se debe verificar las condiciones de garantía de seguridad de los datos siguiendo los términos de las políticas establecidas en el CSIRT.

c) Si el desarrollador requiere de información confidencial de la empresa, con el fin de cumplir el objetivo de la herramienta, estos datos deben ser entregado a través de un compromiso de confidencialidad.

d) Se deberá tener la potestad de realizar auditoria de calidad y seguridad al código, por parte del CSIRT.

- **Definición de incidentes de seguridad y política de eventos**.

Objetivo: Identificar el concepto de incidente de seguridad y clasificar las categorías de los eventos a atender.

Alcance: Es obligatorio para todo el personal del CSIRT, conocer las categorías de eventos.

Definición: el incidente es un evento con consecuencias de afectación en la integridad, confidencialidad o disponibilidad de la información de una entidad.

Categorización de los incidentes de seguridad: teniendo en cuenta que se prestara el servicio a diferentes clientes, los cuales manejan diversos tipos de información y sistemas de información, se determina clasificar los incidentes de seguridad de la información según su nivel de criticidad y de urgencia, así:

Categoría de criticidad de incidentes

Figura 8. Criticidad del Incidente

Impacto / urgencia	Grave	Medio	Leve
Alto	1	2	3
Medio	2	3	4
Bajo	3	4	5

Fuente: “elaboración propia”, con base en datos de: OEA (2002) Buenas Prácticas para establecer un CSIRT nacional. Recuperado de: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Impacto.
Impacto Grave: afectan directamente al negocio, afectando sus objetivos principales y sus recursos principales para funcionar, ya que afectaran sistemas críticos para la empresa.

Impacto Medio: no afectan directamente al negocio en su funcionamiento, pero hace que algunos procesos de la entidad se ralenticen o no puedan ser prestados, afectando sistemas no críticos.

Impacto Leve: no presentan ninguna afectación a los servicios que presta la empresa, pero pueden presentar fallas en la ejecución de procesos internos o pueden repercutir en faltas disciplinarias de los empleados, afectando sistemas no críticos.

Urgencia.

Urgencia Alta: Requiera de atención inmediata, con el fin de garantizar la disponibilidad de la información a los clientes.

Urgencia Media: No se requiere disponibilidad inmediata para clientes, pero es de vital importancia para los procesos internos de la empresa.

Urgencia Baja: No requiere disponibilidad inmediata para los clientes o procesos internos del CSIRT.

- **Política de gestión de incidentes.**

Objetivo: definir los procedimientos de reporte y atención de incidentes, teniendo como criterio de atención las categorías de incidentes de seguridad.

Alcance: Es de obligatorio conocimiento y cumplimiento para todo el personal del CSIRT.

Programa general: con el fin de ofrecer una alta calidad a los clientes del CSIRT, todo el personal debe tener conocimiento básico del proceso de solicitud y respuesta a incidentes según los siguientes parámetros:

a) El gerente de comunicaciones debe enviar y mantener actualizados a los clientes de la entidad, los canales de atención de reportes de incidentes, al igual que mantendrá visible los datos de contacto de servicio al público en la página web y medios sociales de comunicación.

b) El gerente de comunicación realizara publicaciones sobre estadística y últimas amenazas en seguridad de la información, tanto conocidos por el CSIRT, como los más relevantes reportados por otros equipos y expertos en el tema.

c) El Gerente TRIAGE, realizara el cargue a los sistemas de información, de los incidentes reportados por los clientes que se identifiquen dentro de las categorías de incidente, los cuales no se encuentren sistematizados.

d) Se deben definir los procedimientos estandarizados para la atención de incidentes teniendo en cuenta las características diferenciadoras de cada caso.

e) Está totalmente prohibido el uso de técnicas o herramientas ilegales para atender incidentes.

f) En casos de incidentes donde se presuma la comisión de delitos informáticos, se solicitará el apoyo al representante legal del CSIRT.

g) La información recolectada en los incidentes de seguridad, será manejada según las políticas de protección de información del CSIRT.

h) Para la recolección y tratamiento de los datos se deben seguir estándares internacionales en el tema de recolección de evidencia digital, con el fin de asegurar que en el caso necesario pueda ser aportado a instancias legales.

Reporte de Incidentes de Seguridad: tanto los clientes como el personal del CSIRT, deben conocer el protocolo de reporte de incidentes de seguridad, por lo tanto, este deberá ser promulgado por el generante de comunicaciones. El procedimiento de atención será el siguiente.

a) Los reportes de incidente de seguridad, se realizará a través del Gerente TRIAGE, el cual, al momento de recibir la información, deberá remitir una respuesta de conocimiento de lo solicitado, notificándolo de que se iniciará el proceso de asignación del equipo para atender el requerimiento lo más rápidamente posible.
b) El gerente de TRIAGE, analiza el reporte llegado, clasificando su nivel de criticidad y verificando el tipo de equipo técnico que requiere, asignándolo para que ejecute el procedimiento respectivo.

c) El equipo técnico asignado, una vez atienda el incidente, deberá diligenciar un informe de diagnóstico de la situación encontrada y la solución del mismo, el cual será remitido al gerente de TRIAGE.

d) El gerente de TRIAGE, debe analizar el informe de respuesta enviado por el equipo técnico, registrando la información en el sistema de información de respuestas, verificando si requiere alguna aclaración desde el punto

de vista técnico y legal, de lo cual realizara un informe de respuesta al cliente, que solicito el servicio.

- **Política de cooperación.**

  Objetivo: se define el procedimiento de cooperación con otras entidades, especialmente con otros CSIRT y empresas de seguridad informática.

  Alcance: de conocimiento de todos los empleados del CSIRT, los Equipos de respuesta y entidades, con los que se tengan convenio de cooperación.

  Definición: la cooperación entre actores de la seguridad informática, fortalecen un frente común de defensa contra los riesgos que afectan la confidencialidad, disponibilidad e integridad de los datos, en los entornos donde se gestionen.

  Condiciones mínimas de cooperación. Para la realización de un acuerdo de cooperación con otros equipos de respuesta o entidad que trabaje por la ciberseguridad, deberán suscribir mínimo los siguientes requisitos:

  a) Aceptación y alineación de los objetivos que se quiere conseguir con el convenio.

  b) Sistemas que permitan evaluar el costo y beneficio del acuerdo.

  c) Claridad sobre los métodos de terminación o abandono del acuerdo.

  d) Definición de protocolo de flujo de información entre las entidades.

  e) Toda información compartida o llegada a través de cooperación, debe estar alineada con la política de protección de información.

6.4.2 Estructura orgánica para el CSIRT

Figura 9. Estructura Orgánica del CSIRT

Fuente: "elaboración propia", con base en datos de: OEA (2002) Buenas Prácticas para establecer un CSIRT nacional. Recuperado de: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

7 CONCLUSIONES

- Se diseñan e identifican los requerimientos administrativos, en la creación de un equipo de respuesta a incidentes, enfocado a PYMES.

- Se logró identificar el tipo de CSIRT que requiere la empresa, teniendo en cuenta la taxonomía de los ataques más importantes en Colombia y el contexto donde desarrollan sus funciones.

- Se logra definir el portafolio de servicios de CIBERSECURITY-CERT, teniendo en cuenta el análisis de la información recolectada.

- Se definen las políticas y procedimientos básicos desde donde el personal del CSIRT, se guiará para cumplir con los objetivos de calidad y legalidad dentro de sus actividades.

- Se estructuran los cargos y dependencias necesarias para ejecución eficiente de las labores del CSIRT, identificando las áreas a donde pertenecen cada empleado y directivo.

8 RECOMENDACIONES

- Desde la proyección que puede tener este estudio, se debería identificar a otros investigadores que decidieron realizar la temática técnica de este proyecto aplicado, y tratar de fusionar los dos documentos, con el fin de analizar la posibilidad de avanzar en volver una realidad este plan.

- Sería conveniente para el país, y las PYMES a nivel nacionales, la puesta en marcha de este tipo de proyectos, ya que a pesar de que Colombia cuenta con 14 CSIRT reconocidos, no existen muchos dirigidos a esta población, los cuales darían garantías de calidad a nivel internacional, para la entrada en el juego del comercio electrónico de sectores propios del País, como son el de la agricultura, la prestación de servicios, la economía naranja, entre otros.

BIBLIOGRAFÍA

CABALLERO, Daniel. “Matemáticos, ingenieros, informáticos: los criminales del futuro que amenazan a las empresas”. {En línea}. {24 noviembre de 2019} disponible en: https://www-abc-es.cdn.ampproject.org/c/s/www.abc.es/economia/abci-matematicos-ingenieros-informaticos-criminales-futuro-amenazan-empresas-201911240248_noticia_amp.html?fbclid=IwAR3NUZO-0WtaFEIF83F_GaOwA2gg5BeXU1bG1TEI3Ca0ZdrURUqfv6pVfBI

CEBALLOS, Adriana, BAUTISTA, Fredy, MESA, Lorena. “Tendencias Cibercrimen Colombia 2019-2020: Policía Colombia”. {En línea}. {24 noviembre de 2019} disponible en: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL [CONPES]. “Documento Conpes 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa”. {En línea}. {25 octubre de 2014} disponible en: http://www.mintic.gov.co/portal/604/articles3510_documento.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL [CONPES]. “Docu-mento Conpes 3854: Política Nacional De Seguridad Digital”. {En línea}. {11 abril de 2016} disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CORTES, Rodrigo. “Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia: Revista Derecho, Comunicación y Nueva Tecnologías”. {En línea}. {25 noviembre de 2019} disponible en: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics227.pdf

ENISA. “Cómo crear un CSIRT paso a paso: Enisa”. {En línea}. {02 diciembre de 2019} disponible en: https://www.enisa.europa.eu

FIRST. “Improving security together: First — Forum of Incident Response and Security Teams”. {En línea}. {21 julio de 2020} disponible en: https://www.first.org/

ISO. “ISO/IEC 27000:2018”. {En línea}. {16 noviembre de 2020} disponible en: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73906.html

KATS, Raúl. “El ecosistema y la economía digital en américa latina. Madrid, ESPAÑA”. {En línea}. {25 noviembre de 2019} disponible en: https://books.google.com.co/books?id=Axt5CgAAQBAJ&printsec=frontcover&dq=panorama+actual+de+CiberSeguridad+en+Colombia&hl=es-419&sa=X&ved=0ahUKEwjVzcCO7pXmAhXGq1kKHcYACI4Q6AEIYjAI#v=onepage&q=seguridad&f=false

OCDE. “Evaluar el impacto del gobierno digital en Colombia”. {En línea}. {16 noviembre de 2020} disponible en: https://www.oecd.org/countries/colombia/evaluar-el-impacto-del-gobierno-digital-en-colombia-9789264284272-es.htm

OEA. “Buenas Prácticas para establecer un CSIRT nacional”. {En línea}. {16 noviembre de 2020} disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

RIVAS, Javier. “INTECO-CERT, centro de respuesta antes incidentes en TI para pymes. Pymes y Autonomos”. {En línea}. {25 noviembre de 2019} disponible en: https://www.pymesyautonomos.com/tecnologia/inteco-cert-centro-de-respuesta-antes-incidentes-en-ti-para-pymes

ROBLES, Hernando. “Panorama Actual De La Seguridad Informática O De La Ciberseguridad, A Nivel Del País Y Las Tendencias Actuales Y Futura A Nivel Global: Universidad nacional abierta y A Distancia”. {En línea}. {25 octubre de 2019} disponible en: https://repository.unad.edu.co/bitstream/handle/10596/24018/haroblesp.pdf?sequence=1&isAllowed=y

SECRETARIA SENADO DE LA REPÚBLICA. Constitución Política. {En línea}. {20 noviembre de 2020} disponible en: http://www.secretariasenado.gov.co/index.php/constitucion-politica

SECRETARIA SENADO DE LA REPÚBLICA. Ley 581 (2012). {En línea}. {20 noviembre de 2020} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

SECRETARIA SENADO DE LA REPÚBLICA. Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_0599_2000]. {En línea}. {16 noviembre

de 2020} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

SECRETARIA SENADO DE LA REPÚBLICA. Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_1581_2012]. {En línea}. {16 noviembre de 2020} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

SECRETARIA SENADO DE LA REPÚBLICA. Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. {En línea}. {16 noviembre de 2020} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SECRETARIA SENADO DE LA REPÚBLICA. Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_1928_2018]. {En línea}. {16 noviembre de 2020} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

SECRETARIA SENADO DE LA REPÚBLICA. Leyes desde 1992—Vigencia expresa y control de constitucionalidad [LEY_0527_1999]. {En línea}. {16 noviembre de 2020} disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

VALOYES, Amancio. “Ciberseguridad en Colombia. Bogotá, COLOMBIA: Universidad Piloto de Colombia”. {En línea}. {25 noviembre de 2019} disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

VEGA, Fabio. “Métodos De Ataques Y Prevención De La Ingeniería social En Las alcaldías Del Huila En Colombia: Universidad nacional abierta y A Distancia”. {En línea}. {25 octubre de 2019} disponible en: https://repository.unad.edu.co/bitstream/handle/10596/18701/1075273452.pdf?sequence=1&isAllowed=y

ANEXO A. PORTAFOLIOS DE SERVICIOS CIBERSECURITY-CERT

Equipo De Respuesta A Incidente Informáticos

Bienvenido a CIBERSECURITY-CERT. Somos una empresa 100% colombiana, que se dedica al combate, prevención y educación contra los delitos informáticos. Nuestro compromiso es brindar un servicio de calidad que permita mitigar, prevenir e informar sobre las consecuencias de los delitos informáticos y la afectación que pueden sufrir los datos personales y empresariales, protegiendo de la mejor manera la información.

Nuestra visión es ser reconocidos a nivel nacional, como una empresa líder en el apoyo de compañías de gran tamaño y PYMES en la protección de la información.

Puede contar con nuestros servicios:

SERVICIOS REACTIVOS

- Gestión de incidentes. Con el cual se garantizara el manejo adecuado del lugar de los hechos en caso de un incidente informático.

- Respuesta a vulnerabilidades. Lograr brindar una mayor percepción de seguridad en sus sistemas.

- Respuesta a artefactos maliciosos. Buscar atender la necesidad de encontrar este tipo de archivos en un sistema de información y poder determinar su funcionamiento básico.

SERVICIOS PROACTIVOS

- Monitoreo y alertas (primer nivel). Permite verificar y alertar sobre posibles afectaciones que pueda estar sufriendo.

- Investigación y desarrollo (primer nivel). Disponer de información de investigaciones actuales sobre temas de últimas novedades en ataques y amenazas.

SERVICIOS COMPLEMENTARIOS

- Capacitación y educación. Se ofrecen cursos específicos a las labores que se desarrollan en cada departamento de la empresa y el manejo de las tecnologías que se emplean.

• Concientización. Se brindará charlas generales sobre el tema de ciberseguridad.

Para que esté siempre seguro, le ofrecemos en sus servicios reactivos servicio 24/7, 24 horas del día 7 días de la semana.

- Atención personalizada por vía telefónica en nuestros horarios, y Chat las 24 horas, los 365 días del año.

- Contamos con personal altamente calificado.

- Contamos con los equipos de última tecnología para prestar el mejor servicio.

Algunos de nuestros principales clientes son: Hospital Samaritano San Carlos, Almacén de prendas de dotación el Constructor.

Nuestro personal cuenta con la más alta idoneidad profesional y experiencia en el campo de la Ciberseguridad.

Contáctenos:

CIBERSECURITY-CERT.
“Protegemos sus Activos más importantes”
Calle 14 Sur No. 14 - 23.
Tel. PBX: (+57 1) 344 3700 Bogotá D.C., Colombia.
Mail: servicio_cliente @ cibersecurity-cert.com.
Visítenos: www.cibersecurity-cert.com