DISEÑO DOCUMENTAL PARA LA FORMACIÓN DE UN CSIRT

GUILLERMO BENITEZ RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

DISEÑO DOCUMENTAL PARA LA FORMACIÓN DE UN CSIRT

GUILLERMO BENITEZ RODRIGUEZ

Trabajo de grado para optar por el título:
Especialista En Seguridad Informática

Director de Proyecto:
MSc. **LUIS FERNANDO ZAMBRANO HERNANDEZ**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2020

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 01 de octubre de 2020

A mi querida madre que en la distancia y en la medida de su estado de salud, siempre me encomienda a la divina providencia.

AGRADECIMIENTOS

A los familiares que conocieron y me acompañaron en los momentos de dificultades durante el desarrollo de la especialización, un inmenso agradecimiento.

Sinceros agradecimientos a los docentes, tutores y director de proyecto, quienes, con sus aportes y diferencias, fortalecieron mis habilidades y conocimientos en el área de la seguridad.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO: Según la norma ISO 27000[1], es todo aquello que tiene valor para una organización. Comprende cualquier información o los elementos usados para su tratamiento como son los sistemas, redes, soportes, edificios, personas, entre otros.

AMENAZA: Según MINTIC[2], son las causas o factores potenciales que pueden provocar daños dentro de una organización.

ANS: un Acuerdo de Nivel de Servicio - ANS es un convenio entre un proveedor de servicios de TI y un cliente, donde se establecen las normas para la prestación de uno o múltiples servicios, en cuanto a las características, los niveles de cumplimiento, las sanciones y especifica las responsabilidades de las partes que lo suscriben.

APLICACION: Es un activo de información del tipo software que permite a los usuarios realizar una serie de tareas, utilizando dispositivos como computadores tabletas o celulares, entre otros.

AUTENTICACIÓN: es el proceso utilizado entre un emisor y un receptor, con el fin de dar garantía que una característica afirmada es correcta.

CIFRADO: método por el cual se esconde el contenido de archivo o mensaje, de manera que solo pueda ser leído por la persona autorizada.

CONTRASEÑA: es una palabra o frase secreta, utilizada para acceder a ciertas funciones informáticas.

COPIA DE RESPALDO: operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático.

CRIPTOGRAFÍA: la Real academia de la lengua española descompone etimológicamente la palabra, indicando ser derivada del griego kryptós que significa oculto y grafía que significa escritura[3], significando en conjunto el arte de escribir con clave secreta de forma enigmática; también representa escritura escondida. En este sentido se entiende la criptografía como la técnica que permite proteger los documentos e información, utilizando códigos que alteran la transmisión de un mensaje, de manera que no pueda ser leído por una persona diferente al

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Norma ISO/IEC 27000.
[2] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 10]. (15 de diciembre de 2010). Seguridad y Privacidad de la Información. Guía para la preparación de las TIC para la continuidad del negocio. Bogotá, Colombia: MINTIC.p.3

[3] Real Academia de la Lengua Española, Diccionario de la lengua española. Disponible en: http://dle.rae.es/?id=BHcfHjo

destinatario, y pueda ser transformado o descifrado solo por la persona autorizada con el conocimiento de las llaves correspondientes.

IMPACTO: Según ICONTEC[4], resultado adverso en el logro de los objetivos como consecuencia de la posible materialización de un riesgo.

INTERNET: herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP.

INTEGRIDAD: Según la norma ISO/IEC 27000[5]**,** es uno de los pilares de la seguridad de la información relativa a garantizar que la información sea autentica, exacta, completa y exenta de modificaciones no autorizadas**.**

LOG: Según el diccionario de informática y tecnología de ALEGSA[6], se refiere al registro automático de toda la actividad de una aplicación o servicio, en uno o más archivos creados y administrados por un servidor.

PLAN: enmarcado en el contexto de un SGSI, es un documento que define las estrategias y acciones para la implementación del Sistema de Gestión de Seguridad de la Información.

POLÍTICA: conjunto de reglas y procedimientos que definen la forma de actuar y comunicar de los actores de un sistema en relación con los recursos de una organización.

PORTAL WEB: es un sitio compuesto por varias páginas web, el cual, permite al usuario el fácil acceso a diferentes recursos y servicios que tienen relación con un mismo tema.

RIESGO: Según ICONTEC[7], se refiere a la posibilidad de que una amenaza explote las vulnerabilidades de los activos de información generando un impacto adverso en el logro de los objetivos.

SEGURIDAD: según ICONTEC[8], la Seguridad de información es una disciplina que tiene como propósito proteger la confidencialidad, integridad y disponibilidad de los activos de información de una organización.

---

[4] ICONTEC. NTC-ISO/IEC 27005. *Gestión del Riesgo en la Seguridad de la Información*. Bogotá.p.2

[5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Norma ISO/IEC 27000.

[6] ALEGSA. (2020). www.alegsa.com.ar, 1998-2020. Recuperado el 28 de abril de 2020, de Diccionario de Infornática y Tecnología: http://www.alegsa.com.ar/Dic/log_de_servidor.php

[7] Ibíd. ICONTEC.p.3

[8] ICONTEC. NTC-ISO/IEC 27001. *Sistemas de Gestión de la Seguridad de la Información (SGSI)*. Bogotá, Colombia: INCONTEC.p.11

SERVIDOR: Es un activo de información del tipo hardware, mediante el cual se prestan servicios a otros computadores y usuarios en un sistema de red.

SISTEMA INFORMÁTICO O DE INFORMACIÓN: “se entiende como todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos” [9]

TIC: Tecnologías de la Información y de las Comunicaciones

USUARIO: Según el diccionario de informática y tecnología de ALEGSA[10], es cualquier persona, dispositivo o mecanismo para acceder y hacer uso de los sistemas informáticos de una red.

VULNERABILIDAD: Según la norma ISO 27000[11], es una condición o característica de un control o activo de información que lo hace débil y explotable por una o varias amenazas.

[9] COLOMBIA. CONGRESO DE LA REPUBLICA. (21 de agosto de 1999). Ley 527 de 1999. Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Bogotá, Colombia: Diario Oficial. Artículo 2. Definiciones. Recuperado el 2019, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

[10] ALEGSA. (2020). www.alegsa.com.ar, 1998-2020. Recuperado el 28 de abril de 2020, de Diccionario de Informática Y Tecnología: http://www.alegsa.com.ar/Dic/usuario.php

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Norma ISO/IEC 27000.

RESUMEN

Por la descripción dada por LACNIC[12], un CSIRT, por su sigla en inglés *Computer Security Incident Response Team*, es un equipo que ejecuta, coordina y apoya la respuesta a incidentes de seguridad, mediante la prestación de servicios catalogados y con un nivel de servicio contratado, con el fin de proteger las infraestructuras críticas cibernéticas de una comunidad o clientes definidos. Para crear, conformar o implementar un CSIRT, se requiere adelantar un diseño documental y un diseño técnico.

Para este caso, el presente documento contiene una propuesta de diseño documental, con el cual se pretende dar unos lineamientos y acciones para la formación de un centro de respuesta a incidentes de seguridad informática, que comprende el estudio del panorama actual de la ciberseguridad en una región o sector determinado, definición de un catálogo de servicios a prestar, estructuración de la organización con sus funciones y perfiles del equipo de trabajo y definición de las políticas de seguridad que se deben implementar.

Palabras claves: CSIRT, incidentes, nivel de servicio, infraestructuras críticas

[12] LACNIC. (2010). *Proyecto Amparo. Manual: Gestión de Incidentes de Seguridad Informática.* Recuperado el 2019, de https://mafiadoc.com/queue/gestion-de-incidentes-de-seguridad-informatica-proyecto-amparo_59ef42a21723dd78f01e1b9a.html

INTRODUCCIÓN

La creación de un CSIRT se fundamenta en proporcionar una serie de servicios proactivos, reactivos y de calidad para la gestión de incidentes de seguridad informática, gestión de vulnerabilidades y recuperación del negocio ante eventos catastróficos.

Este proyecto tiene como objetivo la realización de un diseño documental para la conformación de un equipo de respuesta a incidentes de seguridad informática, mediante un modelo de organización incorporado en la empresa, Cyber Security de Colombia Limitada, con el fin de ofrecer a sus clientes servicios de notificaciones y gestión de incidentes, así como servicios proactivos de gestión de vulnerabilidades.

Este diseño documental tiene como alcance los siguientes componentes: descripción del panorama actual de la seguridad digital en Colombia, identificación de la taxonomía de tipos de incidentes, estructuración del catálogo de servicios de los tipos proactivos y reactivos, propuesta de un modelo organizativo con la definición de funciones de los perfiles del equipo de trabajo y la elaboración de políticas y procedimientos operacionales del CSIRT. Para el caso de los procedimientos, solamente se definirán los básicos necesarios de la operación, sin entrar en la filigrana de los procedimientos específicos.

Para lograr el objeto y el alcance planteado, se propone la utilización de la metodología para evaluación, diagnóstico y diseño de procesos, la cual persigue los objetivos de la reingeniería que consiste en crear un CSIRT dentro de una organización, sin desconocer los procesos existentes. Esta metodología se resume en cuatro etapas: conocimiento, interpretación, análisis y diseño[13].

Con la implementación de un CSIRT, se prende cerrar la brecha o eliminar las falencias de las empresas que no cuentan con el presupuesto y el recurso humano para atender los incidentes de seguridad o definitivamente necesitan centrarse en su función misional.

[13] **HERRERA M. Haroldo E.** Metodología para evaluación, diagnóstico y diseño de procesos [En línea]. - 22 de febrero de 2007. - 2020. - https://www.gestiopolis.com/metodologia-para-evaluacion-diagnostico-y-diseno-de-procesos.

1. DEFINICION DEL PROBLEMA

1.1 ANTECEDENTES

El Consejo Nacional de Política Económica y Social[14] expidió el documento 3854 donde se establece la política de seguridad digital, buscando que los ciudadanos, las Entidades del Gobierno y los empresarios realicen una gestión de riesgos de seguridad digital que les permita conocer e identificar los riesgos a los que están expuestos en el entorno digital y aprendan como protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos, lo que conlleva establecer un entorno digital confiable y seguro, que maximice los beneficios económicos y sociales en el país, impulsando la competitividad y productividad en todos los sectores de la economía. En este sentido, la política de seguridad digital busca la concientización y adaptabilidad de las Entidades del Gobierno, los Empresarios y los Ciudadanos a las circunstancias cambiantes del entorno digital.

En el caso de las Entidades del Gobierno, el Ministerio de Defensa[15] y demás sectores del país, elaboraron el Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia - PNPICCN V 1.0, en el cual se definieron los lineamientos generales que deben adoptar los diversos actores dueños y operadores de las infraestructuras críticas cibernéticas en Colombia - ICCN, así como cada uno de los actores del ecosistema de la infraestructura crítica cibernética del país, para ser utilizado como una herramienta que permite articular esfuerzos de manera coordinada, sistemática y eficiente, con el fin de prevenir y reaccionar ante la presencia de ataques cibernéticos que pongan en riesgo la continuidad y disponibilidad de los servicios críticos para el país. Adicionalmente se desarrolló el Catálogo de Infraestructuras Críticas Cibernética de Colombia – ICCN Versión 1.0, donde se definieron trece (13) sectores y su nivel de criticidad o de alto impacto cibernético de la siguiente manera: i) MUY ALTO (Electricidad; Hidrocarburos, Minas y Gas; Financiero; TIC), ii) ALTO (Gobierno; Seguridad y Defensa; Agua; Transporte), iii) MODERADO (Industria, Comercio y Turismo; Educación; Salud y Protección Social) y iv) BAJO (Ambiente; Agricultura - Alimentación). En consecuencia, con lo anterior, las

[14] CONPES 3854. (2016). Política de Seguridad Digital. Bogotá, Colombia.

[15] COLOMBIA. MINISTERIO DE DEFENSA. (2017). Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. PNPICCN V 1.0. Bogotá, Colombia. Recuperado el 2019, de https://www.ccoc.mil.co/recursos_user///PLAN_PUBLICO.pdf

entidades líderes de cada sector y las entidades que pertenecen a un mismo sector, en coordinación con MINDEFENSA y MINTIC, se encuentran estructurando el Plan de Protección y Defensa para la Infraestructura Crítica Cibernética de su sector.

Al final de esta cadena de cooperación conjunta, se encuentran las Entidades del Gobierno que cuenten con infraestructura de tecnologías de información y comunicaciones, quienes tienen la responsabilidad de la operación del plan nacional y sectorial, las cuales deben desarrollar e implementar un plan en donde se describan los servicios esenciales de la Entidad, con sus interdependencias con otras entidades del sector al cual pertenece, identificar los riesgos, amenazas y vulnerabilidades a los que están expuestos estos servicios y plantear las estrategias y controles para minimizar el impacto ante la eventual materialización de los riesgos, de tal manera que se fortalezcan las acciones de ciberseguridad que permitan incrementar la capacidad de la Entidad para afrontar posibles ciberataques a la infraestructura crítica de la Entidad.

En el caso de las Empresarios, estos son cada vez más conscientes de la necesidad de estructurar empresas más seguras. Esta situación se da por el Gobierno Nacional les exige el cumplimiento de ciertos requisitos de seguridad en calidad de proveedores del sector estatal, porque forman parte de la cadena de las infraestructuras críticas del país o porque han padecido o conocen casos de ataques a los sistemas, ya sean del sector privado o público.

En el caso de los Ciudadanos, tanto el Gobierno Nacional como el Sector Privado, buscan generar conciencia entre sus administrados o sus usuarios para que aprendan como actuar en el entorno digital y conozcan las herramientas con que cuentan para protegerse, prevenir y reaccionar ante un evento o incidente de seguridad. En ese sentido, la sociedad, el estado y los empresarios deben alinearse para conseguir el objetivo de establecer un entorno digital seguro, para obtener mejores beneficios económicos y sociales, impulsando la competitividad y productividad en los sectores de la economía colombiana.

Bajo este panorama, el Gobierno Nacional[16], con el fin de proteger las infraestructuras críticas y responder a los problemas asociados con la seguridad digital, creó tres instituciones para la seguridad digital en Colombia que son el Centro Cibernético Policial, el ColCERT[17] y el Comando Conjunto Cibernético. Estas instituciones prestan servicios limitados a las Entidades Estatales, ya sea que estas no cuentan un nivel de seguridad adecuado o simplemente porque los

[16] CONPES 3701. (2011). Lineamientos nacionales de política en Ciberseguridad. Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
[17] Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

recursos son insuficientes. Estos servicios no cubren las empresas del orden jurídico privado.

1.2 FORMULACION

Para las empresas privadas, los servicios de CSIRT pueden ser prestados de manera interna o externa por organizaciones privadas que proveen servicios a otras compañías ya sea por demanda o de forma regular. En este nicho, es donde se crea la necesidad de formar CSIRT comercial para cubrir las brechas de seguridad. En ese sentido, se desarrolla el presente proyecto de tipo académico, el cual busca resolver la siguiente pregunta:

¿Cómo crear y gestionar las funciones de un equipo 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?

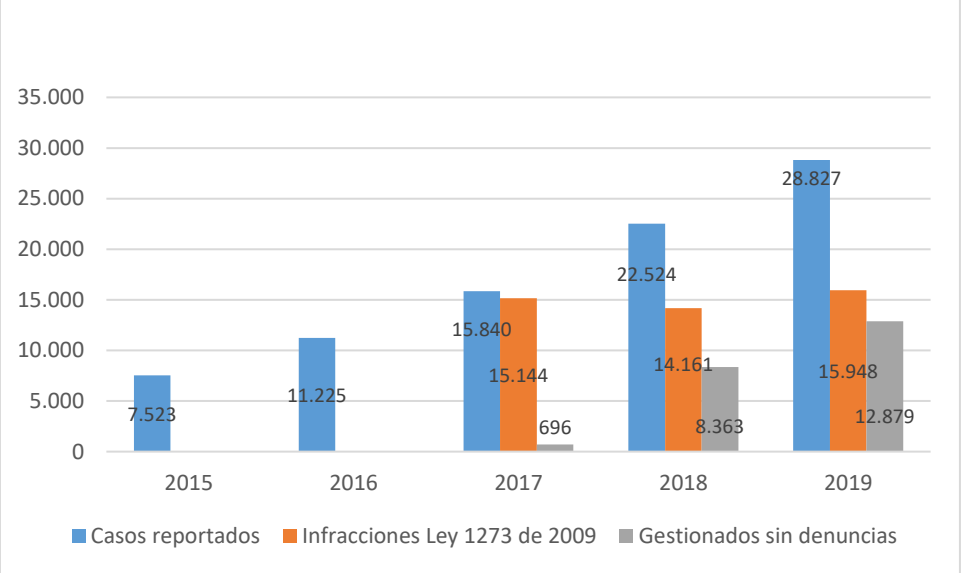
Este tipo de proyecto busca comprender y resolver alguna situación, necesidad o problema en un contexto determinado. El tipo de proyecto es de aplicación, con tipo de intervención de Investigación Acción. Se trabaja con un caso de estudio, interactuando con personas que tengan conocimiento en seguridad y consultando fuentes bibliográficas que apliquen a este caso.

En la cadena de formación de sistemas de la UNAD, se encuentran dos líneas de acción, de las cuales se seleccionó la línea de Gestión de sistemas (Área: Ciencias de la Computación), la cual involucra la seguridad informática; dentro de esa línea, se desarrolla el presente proyecto de aplicación.

2. JUSTIFICACIÓN

Según el informe denominado “Tendencias del Cibercrimen en Colombia 2019–2020”, publicado por la Policía Nacional de Colombia[18], entre el 2015 al 2019 se recibieron 85.939 incidentes de seguridad en las plataformas virtuales y medios físicos habilitadas por el Centro Cibernético Policial. En el mismo informe, se señala el reporte de los incidentes en orden descendente con mayor ocurrencia en Colombia: i) phishing 42%, ii) suplantación de Identidad 28%, iii) envío de programa maligno 14% y iv) fraudes en medios de pago en línea 16%.

Figura 1. Cifras de denuncias 2015-2019

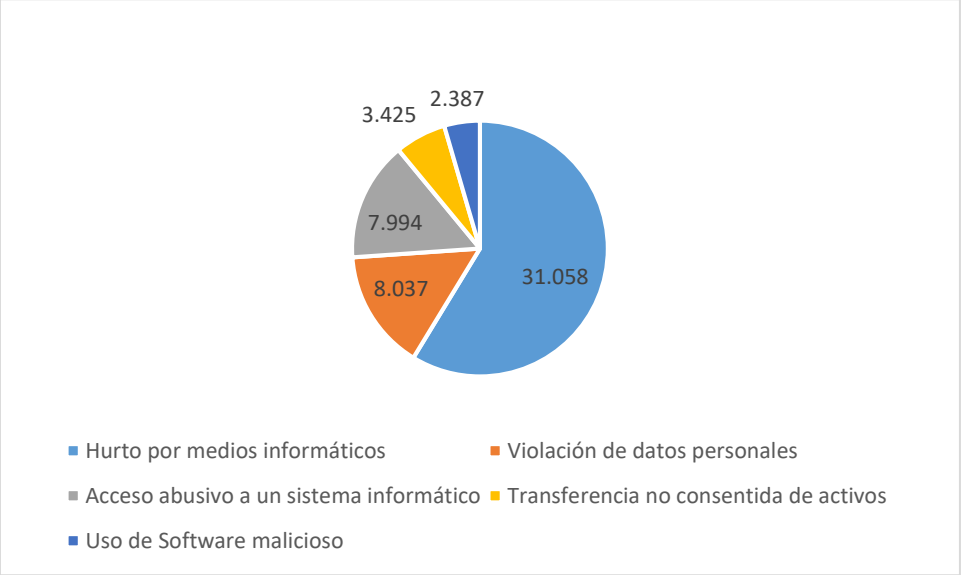


Fuente: POLICIA NACIONAL DE COLOMBIA. Informe “Tendencias del Cibercrimen en Colombia 2019 – 2020”

Adicionalmente, en el mencionado informe se relaciona el escalafón de los delitos informáticos más denunciados en Colombia:

[18] POLICIA NACIONAL DE COLOMBIA, CCIT. (29 de octubre de 2019). Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020. Bogotá, Colombia.

Figura 2. Escalafón de delitos informáticos en Colombia



Fuente: POLICIA NACIONAL DE COLOMBIA. Informe “Tendencias del Cibercrimen en Colombia 2019 – 2020”

Por otra parte, en la publicación más reciente denominada “Informe Tendencias del Cibercrimen primer trimestre 2020”[19], en el primer trimestre de 2020, se presentaron 7.082 denuncias por delitos informáticos lo que representa un incremento del 27%, comparado con en el mismo periodo de 2019.

Como se puede observar en las cifras publicada por la Policía Nacional, las actividades delictivas relacionadas con la seguridad digital visualizan una tendencia al aumento pasando de la selección de víctimas de personas a empresas. En ese sentido, para hacer frente a los incidentes de seguridad que se pueden presentar en las empresas, se deben establecer estrategias de fortalecimiento y formación de equipos de respuestas a incidentes de seguridad CSIRT, que permitan ofrecer diferentes tipos de servicios proactivos, reactivos y de valor agregado para contribuir con la defensa y continuad de los negocios en Colombia.

[19] POLICIA NACIONAL DE COLOMBIA, CCIT Informe Tendencias del Cibercrimen primer trimestre 2020. - Bogotá : CCIT, 2020. Recuperado de https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/

3. OBJETIVOS

3.1 OBJETIVO GENERAL.

Realizar el diseño documental para la conformación de un CSIRT para la empresa Cibersecurity de Colombia Limitada, con el fin de ofrecer a sus clientes servicios de respuesta a incidentes y de gestión de vulnerabilidades teniendo presente el nivel de servicio contratado.

3.2 OBJETIVOS ESPECÍFICOS

- Describir el panorama actual de la Seguridad Digital en Colombia en los últimos tres (3) años, que contribuya con la identificación del ámbito de actuación del CSIRT y la creación de la taxonomía de ataques de este.
- Estructurar el Catálogo de Servicios, el cual comprende los diferentes tipos de servicios proactivos y reactivos que presta el CSIRT.
- Elaborar el manual de funciones de los perfiles del equipo de trabajo, conforme a la estructura orgánica requerida para la creación del CSIRT.
- Estructurar el Manual de Políticas y Procedimientos Operacionales, que incluya la Gestión de Incidentes, gestión de notificaciones y la recolección y custodia de evidencias.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

Como afirma PARRA[20], la dinámica internacional y los avances tecnológicos colocan en un estado de vulnerabilidad a las personas consumidoras de servicios, a las empresas prestadoras de servicios y al mismo Estado, haciendo necesario que todos los sectores cuenten con mecanismos legales y tecnológicos para afrontar adecuadamente los ataques informáticos.

En este sentido, la OEA[21] concluye que los diferentes países deben adelantar más acciones para implementar mecanismos de control, tanto legislativos como técnicos, buscando minimizar el impacto adverso en la sociedad, disminuyendo las pérdidas económicas en un posible evento de ataque. En el siguiente cuadro se ilustran estas acciones adelantadas por países de Latinoamérica:

Tabla 1. Mecanismos de control por países

País	Organismos / Equipos	Normas
Perú	PECERT, Sistema de Coordinación de la Administración Pública, encargado de coordinar esfuerzos para resolver, prevenir, responder y proteger a la Nación ante los Ciber ataques.	Ley 30096 que incorpora los delitos cibernéticos al código penal Ley 29733 para la protección de datos personales
Argentina	El Centro de Ciberdefensa de Argentina es el encargado de la atención a los incidentes de seguridad. Mediante el Programa ICIC[22], se adopta el marco regulatorio que identifica y protege las infraestructuras estratégicas y críticas de Argentina.	Resolución 1380/2019 del Ministerio de Defensa, mediante la cual se oficializa la creación del centro.
Uruguay	CERTuy es el Centro Nacional de Respuesta a Incidentes de Seguridad	Ley No. 18.362 del 6 de octubre de 2008, Articulo 73 que crea el

[20] PARRA, R. (2016). *Proyecto Legal para un Esquema Nacional de Ciber Seguridad.* Lima, Perú: Universidad de San Martín de Porres. Recuperado el 2019, de http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/2051/1/parra_prg.pdf

[21] OEA, TREND MICRO. (2015). Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas.p.22. Recuperado el 2019, de https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

[22] Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad de Argentina - ICIC

	Informática de la República del Uruguay, creado por la Ley 18.362/2008 para dar respuesta y prevenir los incidentes de seguridad.	"Centro Nacional de Respuesta a Incidentes de Seguridad Informática" CERTuy Decreto No. 451 del 28 de septiembre de 2009, mediante el cual se regula el funcionamiento y organización del CERTuy
Colombia	Centro Cibernético Policial. Responsable de la ciberseguridad de Colombia, ofreciendo información, apoyo y protección ante los delitos cibernéticos. ColCERT. Responsable de la protección de la infraestructura crítica de Colombia frente a emergencias de ciberseguridad. CCOC - Comando Conjunto Cibernético.	CONPES 3701 de 2011. Política de seguridad digital y se asegura la creación de estos organismos.

Fuente: OEA, TREND MICRO. Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas

4.2 MARCO CONCEPTUAL

Las acciones adelantadas por los países con el objetivo de conformar equipos para atención de incidentes de seguridad no solamente deben ser gubernamentales, sino que se pueden presentar para diferentes ámbitos y pueden ser implementadas tanto por empresas públicas como privadas. Según la OEA[23], los CSIRT varían en misión y alcance, los cuales se clasifican o agrupan dependiendo de la comunidad o el sector objeto de la prestación de sus servicios:

4.2.1 CSIRT del sector académico. Prestan servicios a organizaciones educativas y comunidades académicas, como centros o corporaciones universitarias, escuelas o institutos de investigación. El tamaño e instalaciones puede variar en función de la comunidad que atiende, las cuales pueden estar orientados a una facultad, a una sede, a una institución o grupos de instituciones

[23] OEA. (2016). *Buenas Prácticas para establecer un CSIRT nacional.p.5-8.* Recuperado el 2020, de https://seguridadenlanube.blogspot.com/2016/04/buenas-practicas-para-establecer-un.html

o centros. Por lo general este tipo de equipo de respuesta aúnan esfuerzos con otros CSIRT y algunos se especializan en investigaciones.

4.2.2 CSIRT comercial. Por limitaciones de recursos humanos o por la necesidad de centrarse en el negocio, algunas empresas tercerizan las funciones de respuesta a incidentes mediante la contratación y pago de servicios prestados por CSIRT comerciales. Por lo general, la relación entre el proveedor de servicios y sus clientes se establece mediante un convenio o documento suscrito entre las partes denominado Acuerdo de Niveles de Servicio – ANS, donde se establecen las normas para la prestación de uno o múltiples servicios, en cuanto a las características, los niveles de cumplimiento, las sanciones y responsabilidades de cada uno.

4.2.3 CSIRT gubernamentales. Prestan sus servicios a los ciudadanos, agencias públicas o instituciones del Estado de cualquier nivel territorial: local, regional o nacional. En el caso de las entidades gubernamentales buscan garantizar que la infraestructura de TI que soporta sus procesos misionales críticos y los servicios que les ofrecen a los ciudadanos tengan niveles de seguridad adecuados. Los CSIRT gubernamentales se pueden crear para atender un sector especifico de manera independiente o pueden interactuar entre sectores para combinar y compartir estrategias, esfuerzos, recursos y conocimientos.

4.2.4 CSIRT del sector militar. Proporcionan servicios a las instituciones u organizaciones militares de un país, para la protección de infraestructuras de TI destinas a la defensa de un país, por ejemplo, armamento y sistemas de radares. Este podría ser el caso de un CSIRT gubernamental que atiende a un sector del gobierno, pero que debe interactuar con los demás sectores. Los servicios que presta se limitan generalmente a la defensa o a las capacidades cibernéticas ofensivas de una nación.

4.2.5 CSIRT de infraestructuras críticas. Prestan sus servicios para la protección de los activos de información y la infraestructura críticos de la nación, sin importar si es operado por el sector público o privado o si es para una entidad del orden local, regional o nacional.

4.2.6 CSIRT nacionales. Es considerado como un punto de coordinación y de contacto para la seguridad interna de país donde opera y un punto de contacto para incidentes internacionales. Por su rol de intermediario de un país, por lo general no tiene un grupo de clientes directo, pero ante la ausencia de centro de

respuestas puede asumir las funciones o roles de otro CSIRT, como, por ejemplo, asumir las responsabilidades normalmente asignadas a un equipo de respuesta de infraestructura crítica.

4.2.7 CSIRT del sector de las PYMES. Presta sus servicios a pequeñas y medianas empresas, en razón a su tamaño y su naturaleza no se les posibilita la implementación de equipos de respuesta a incidentes de manera individual. Por lo tanto, hay una necesidad de crear CSIRT que entiendan y respondan a las necesidades de esta comunidad de empresas o de grupos de interés especial como la Federación de Departamentos de Colombia.

4.2.8 CSIRT de proveedores. Prestan servicios relacionados con productos específicos de un fabricante, desarrollador o proveedor de servicios. Tienen por objetivo desarrollar soluciones para eliminar vulnerabilidades y mitigar los efectos negativos relacionados con sus productos. Están orientados a los propietarios de productos como Hewlett Packard (HP CSIRT), Banelco Bank (Banelco CSIRT), Adobe (Adobe PSIRT), entre otros.

4.3 MARCO HISTORICO

4.3.1 Ataques. En esta sección se presenta una aproximación histórica de los principales ataques a la seguridad, según investigación realizada por PARRA[24].

4.3.1.1 Morris WORM - 1998. Primer gran ataque realizado por Robert Tappan Morris, un estudiante de la Universidad de Harvard. El gusano informático afectó 6000 computadores, correspondiente al 10% de los sistemas conectados a la ARPANET[25], conocida como la infraestructura de red antecesora de la Internet. Entre los sistemas infectados se encontraba el Centro de Investigación de la NASA[26].

4.3.1.2 NASA - 2006. El ataque filtró información sobre el lanzamiento de vehículos al espacio. La entidad bloqueó sus sistemas de correo electrónico con archivos adjuntos.

4.3.1.3 Estonia - 2007. Ataque a través de BOTNETS atribuido a Rusia. Mediante el envío de solicitudes masivas se presentó negación de servicio de las páginas web del presidente de Estonia, del Parlamento de Ministros Gubernamentales, Organizaciones de noticias y algunos bancos.

[24] PARRA R.G. Proyecto Legal para un Esquema Nacional de Ciber Seguridad
[25] Advanced Research Projects Agency Network
[26] Agencia Nacional de la Aeronáutica y del Espacio de los Estados Unidos - NASA.

4.3.1.4 Estados Unidos - 2007. Obtención de información clasificada del Pentágono, mediante el ingreso indebido a las cuentas de correo del secretario de defensa de los Estados Unidos.

4.3.1.5 China - 2007. Ataque de Spyware a la infraestructura critica de China en el cual se robó información de la entidad Aerospace Science & Industry Corporation (CASIC).

4.3.1.6 ISRAEL - 2009. Ataque a la infraestructura de internet ejecutado durante durante la ofensiva militar de enero de 2009 en la Franja de Gaza. El ataque afectó principalmente los sitios web del gobierno

4.3.1.7 Siemens - 2010. Ataque mediante el uso de malware Stuxnet diseñado para interferir con los sistemas de control industrial Siemens.

4.3.1.8 Canadá - 2011. Ataque dirigido a la Defensa de Investigación y Desarrollo de Canadá, Departamento de Defensa Nacional de Canadá y al Departamento de Finanzas y del Consejo del Tesoro, quienes se vieron obligados a desconectarse de Internet.

4.3.1.9 octubre Rojo - 2012. La empresa rusa Kaspersky descubrió un ataque cibernético en todo el mundo llamado “Octubre Rojo”, mediante se obtuvo información a través de vulnerabilidades en los programas Microsoft Word y Excel. Los objetivos principales de los ataques fueron los países de Europa del Este, la ex Unión Soviética y Asia Central, aunque Europa occidental y América del Norte reportaron víctimas también.

4.3.1.10 Corea de Sur - 2013. Ataque realizado a instituciones financieras de Corea del Sur.

4.3.2 Respuestas. Como medida de respuesta a los incidentes de seguridad, según ENISA se destacan las siguientes iniciativas:

4.3.2.1 CERT-CC - 1988. Con el auspicio de DARPA[27], nace en Pensilvania, Estados Unidos el centro de coordinación CERT-CC como respuesta a los ataques por el gusano informático Morris WORM.

4.3.2.2 FIRST - 1990. Se crea el FIRST[28], ante la necesidad de una mejor comunicación y coordinación entre los equipos de respuesta a incidentes de seguridad.

[27] Defense Advanced Research Projects Agency - Agencia de Investigación de Proyectos Avanzados de Defensa)

[28] FIRST Foro sobre los Equipos de Respuesta a Incidentes y Seguridad

4.3.2.2 SURFnet - 1992. El modelo CERT-CC se adopta en Europa por el proveedor académico holandés SURFnet.

4.3.2.3 ENISA - 2004. Se crea la Agencia Europea de Seguridad de las Redes y de la Información - ENISA, con el objetivo de "garantizar un nivel elevado y efectivo de seguridad de las redes y de la información en la Comunidad Europea y desarrollar una cultura de la seguridad de las redes y la información en beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público de la Unión Europea, contribuyendo así al funcionamiento armonioso del mercado interior"[29].

4.3.2.4 Índice mundial de ciberseguridad – GCI. "La primera encuesta de GCI se llevó a cabo en 2013/2014 en asociación con ABI Research, donde un total de 105 países respondieron de 193 Estados Miembros de la UIT. La encuesta busca fomentar una cultura global de ciberseguridad y su integración en el núcleo de las tecnologías de la información y la comunicación"[30].

4.4 MARCO TECNOLOGICO

En el medio se conocen diversos modelos organizacionales para el funcionamiento un CSIRT. Según ROLDAN[31] estos modelos se clasifican de la siguiente forma:

4.4.1 Modelo de organización independiente. Se constituye como una empresa aparte con personería jurídica, autonomía administrativa y financiada por una organización externa o por los integrantes de una comunidad. En este modelo existe un equipo de respuesta definido, con sus propios directivos y empleados.

4.4.2 Modelo integrado en una organización preexistente. También conocido como modelo incrustado, funciona como una dependencia de la organización, que reporta a la presidencia o dirección general, sin personería jurídica, sin autonomía administrativa y financiera. Cuenta con un alto grado de autonomía técnica, sin detrimento a solicitar asistencia técnica especializada a al resto de las dependencias de la organización.

4.4.3 Modelo CAMPUS. También conocido como modelo universitario,

[29] HENK Bronk y Hakkaja Marco Thorbruegge y Mehis Como Crear un CSIRT Paso a paso
[30] INTERNATIONAL TELECOMMUNICATION UNION Global Cibersecurity Index – GCI 2018
[31] ROLDAN, F. S. (2011). Guía de creación de un CERT/CSIRT. Capítulo 5. Modelo Organizativo, Centro criptológico nacional, recuperado de https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf

adoptado principalmente por universidades o redes de investigación, conformado por una sede central que coordina otras sedes distribuidas geográficamente, ya sea en un ámbito regional, nacional o transnacional. Estos equipos de respuesta tienden a especializarse y a intercambiar servicios básicos entre sí. Presentan un alto sentido de la colaboración y trabajo en equipo. Son ideales para redes de investigación y para organizaciones con un elevado grado de descentralización, como por ejemplo en empresas multinacionales. Cada centro puede tener personería jurídica y autonomía administrativa y financiera.

4.4.4 Modelo basado en el voluntariado. En este modelo un grupo de especialista se unen voluntariamente para prestarse servicios entre ellos, con la posibilidad de extender sus servicios a una comunidad. Actúan de forma espontánea y depende de la motivación de los integrantes.

4.5 MARCO ESPACIAL

En MAGERIT[32] se consigna que en toda empresa la información y los servicios deben ser considerados como los activos fundamentales o esenciales para el desarrollo de su misión y la apropiada toma de decisiones; razón por la cual, debe existir un compromiso expreso de protección de sus propiedades más significativas y críticas como parte de una estrategia orientada a la Continuidad del negocio.

Consciente de estas necesidades, el Ministerio de las Tecnologías de la Información y las Comunicaciones[33] invita a las empresas a adaptar, implementar, revisar y mejorar el modelo de seguridad de la Información definido para cada organización, el cual debe hablar de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que permitan exigir niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

En ese sentido y con el fin de proteger la información y los servicios críticos, MIRANDA[34] recomienda que las organizaciones desarrollen un modelo de seguridad de información, que apalancado en la seguridad informática se encargue de las implementaciones técnicas de la protección de la información,

[32] MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

[33] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC. (2016). Modelo de Seguridad y Privacidad de la Información.p.8. Modelo. Obtenido de https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

[34] MIRANDA, J. M. (2016). *Estableciendo controles y perímetro de seguridad para una página web de un CSIRT.* (C. d. CIMAT, Ed.) RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação. Recuperado el 2019, de https://dx.doi.org/10.17013/risti.17.1-15

el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales.

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 los CSIRT comerciales.

Para dar respuesta a este requerimiento tecnológico, se busca 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.

Consciente de las necesidades actuales, la empresa decide adelantar una iniciativa para la conformación de un CSIRT comercial, para lo cual se organizaron en dos grupos de trabajo; uno desarrolla el enfoque administrativo y el segundo el enfoque técnico. En este proyecto se desarrolla el enfoque administrativo, bajo el cumplimiento de los siguientes requisitos:

Tabla 2. Entregables del proyecto

Actividad	Entregable
Definir el ámbito de actuación del CSIRT	Documento que contenga panorama actual de la seguridad digital en Colombia en los últimos tres (3) años.
Creación de la Taxonomía de ataques	Taxonomía de ataques relevantes a partir del documento de panorama actual
Definir los tipos de servicios “proactivos y reactivos” del CSIRT además de los posibles servicios complementarios que se podrían ofertar.	Catálogo de servicios del CSIRT
Definir requisitos y perfiles del equipo de trabajo para la conformación del CSIRT	Manual de funciones de los perfiles del equipo de trabajo del CSIRT
Políticas y Procedimientos Operacionales	Manual de Políticas y Procedimientos Operacionales: • Gestión de Incidentes • Cooperación. Notificaciones e Intercambio de información • Recolección y custodia de evidencias
Definir la estructura orgánica del CSIRT	Estructura Orgánica del CSIRT

Fuente: El autor

4.6 MARCO LEGAL

4.6.1 Política de seguridad digital. El Consejo Nacional de Política Económica y Social – CONPES, fue creado mediante la ley 19 de 1958 para asesorar a la Presidencia de la República en el desarrollo económico y social del estado colombiano. En relación con la seguridad digital, este organismo ha expedido los siguientes documentos:

4.6.1.1 CONPES 3701 de 2011[35]. Con este documento el gobierno colombiano busca desarrollar una estrategia nacional para defenderse y atacar el incremento de las amenazas que afectan al país en materia cibernética, mediante la generación de capacidades de ciberseguridad para minimizar el nivel de riesgo o exposición de los ciudadanos, ante amenazas o incidentes de seguridad

4.6.1.2 CONPES 3854 de 2016[36]. Documento donde se establece la política de seguridad digital, buscando que los ciudadanos, las entidades del Gobierno y los empresarios realicen una gestión de riesgos de seguridad digital que les permita conocer e identificar los riesgos a los que están expuestos en el entorno digital y aprendan como protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.

4.6.2 Convenios internacionales. Mediante la ley 1928 de 2018[37], el Congreso de la República ratifica el convenio sobre la ciberdelincuencia firmado por el gobierno colombiano el 23 de noviembre de 2001 en la ciudad de Budapest. El convenio compromete a los estados firmantes a adoptar una política y normatividad penal y de colaboración, orientada a proteger a la sociedad de la ciberdelincuencia.

4.6.3 Leyes relacionadas. El Congreso de la República ha emitido las siguientes normas:

4.6.3.1 Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC– se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

[35] CONPES 3701. (2011). Lineamientos nacionales de política en Ciberseguridad. Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
[36] CONPES 3854. (2016). Política de Seguridad Digital. Bogotá, Colombia.

[37] COLOMBIA. CONGRESO DE LA REPUBLICA Ley 1928. - Bogotá : Diario Oficial, 24 de julio de 2018. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

4.6.3.2 Ley 1266 de 2008. Conocida como la ley de hábeas data y del manejo de la información contenida en bases de datos personales.

4.6.3.3 Ley 1273 de 2009. Esta ley modifica el Código Penal y crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos. A través de esta ley, se tipifican los delitos informáticos, con sus respectivas penalizaciones.

4.6.3.4 Ley 1581 de 2012. En esta norma se dictan disposiciones generales para la protección de datos personales.

4.6.3.5 Ley 1712 de 2008. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

4.6.4 Reglamentaciones. El Congreso de la República ha emitido las siguientes normas:

4.6.4.1 Decreto 2693 de 2012. El Ministerio de las Tecnologías de la Información y las Comunicaciones establece los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

4.6.4.2 Decreto 1377 de 2013. Mediante este decreto, el gobierno nacional reglamenta y ordena algunas disposiciones respecto a la ley 1581 de 2012, para la protección de datos personales, que, concede el derecho a todas las personas, de conocer, actualizar o modificar la información recolectada y almacenada en bases de datos o archivos[38].El Ministerio de Industria, Comercio y Turismo determinó que el tratamiento de datos personales debe estar legalizado por medio de un contrato suscrito entre el dueño de la información y responsable de tal actividad. La entidad responsable del tratamiento de la información debe responder por los daños ocasionados al titular de los datos personales por el manejo inadecuado de los mismos.

4.6.4.3 Decreto 2573 de 2014. El Ministerio de las Tecnologías de Información y las Comunicaciones establece los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

[38] COLOMBIA. MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO. Decreto1377 de 2013. Obtenido de https://mintic.gov.co/portal/604/articles-4274_documento.pdf

4.6.4.4 Circular 007 de 2018. La Superintendencia Financiera señala a las entidades objeto de su vigilancia a informar a los usuarios sobre los incidentes de seguridad y a tomar medidas de seguridad para proteger las actividades en pasarelas de pago.

4.6.5 Guías. El Ministerio de las Tecnologías de la Información y Comunicaciones, en el marco del modelo de Seguridad y Privacidad de la Información desarrollo una serie de guías destinadas a las entidades estatales y cualquier tercero que decida implementar la seguridad informática de acuerdo con estos lineamientos:

- Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información.
- Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.
- Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.
- Guía No 5 - Gestión De Activos.
- Guía No 6 - Gestión Documental.
- Guía No 7 - Gestión de Riesgos.
- Guía No 8 - Controles de Seguridad.
- Guía No. 12. Seguridad en la Nube
- Guía No 14 - Plan de comunicación, sensibilización y capacitación.
- Guía para la Implementación de Seguridad de la Información en una MIPYME. Versión 1.2. (6/11/2016)

5. DISEÑO METODOLOGICO

Para el desarrollo del presente proyecto se realizan las siguientes etapas de la metodología para evaluación, diagnóstico y diseño de procesos[39]:

Tabla 3. Metodología para evaluación, diagnóstico y diseño de procesos

Etapa	Actividad
I. Conocimiento	Mediante la identificación y consulta de fuentes documentales se recolecta información en los aspectos de evolución de los CSIRT, situación actual y estadísticas de la seguridad digital en Colombia, tipos de servicios, tipos de CSIRT, taxonomía de ataques, metodologías para definir funciones y perfiles del equipo de trabajo, estructuras de organización utilizadas, políticas y procedimientos operacionales.
II. Interpretación	En esta etapa se identifica y clasifica la información consultada para facilitar el análisis y transformación de esta. La información o fuentes documentales con poca utilidad son desechadas y se complementa con nuevas fuentes documentales, en los casos que sea necesario. Adicionalmente se representa en un diagrama de alto nivel el flujograma de las actividades de los procesos con que se atiende el CSIRT.
III. Análisis	En esta etapa se verifican, cuestionan y se revisa la aplicabilidad de la información recolectada y de los diseños implementados en otros CSIRT, con el fin de implementarlos, mejorarlos o darles un valor agregado en este proyecto. Adicionalmente se selecciona la metodología para definir las funciones y perfiles del equipo de trabajo. En esta etapa se realiza el análisis de factibilidad, indicando el ámbito de actuación del CSIRT en Colombia y se crea la Taxonomía de ataques para la actuación del CSIRT.
IV. Diseño	Es esta etapa se realizaron los siguientes pasos: • Diseñar la visión del CSIRT. En este paso se define la misión, funciones, ámbito y ubicación del CSIRT dentro de la organización. • Definir las Políticas y Procedimientos Operacionales

[39] HERRERA M. Haroldo E. Metodología para evaluación, diagnóstico y diseño de procesos [En línea]. - 22 de febrero de 2007. - 2020. - https://www.gestiopolis.com/metodologia-para-evaluacion-diagnostico-y-diseno-de-procesos/.

	• Definir a la estructura orgánica requerida para la creación del CSIRT

Fuente: HERRERA M. Haroldo E. https://www.gestiopolis.com/metodologia-para-evaluacion-diagnostico-y-diseno-de-procesos/

6. DESARROLLO DE LOS OBJETIVOS

6.1 PANORAMA ACTUAL DE LA SEGURIDAD DIGITAL EN COLOMBIA

6.1.1 Inversión en ciencia tecnología e innovación. Colombia ha logrado un importante crecimiento económico y social gracias al mantenimiento y fortalecimiento del marco de políticas macroeconómicas, acciones que se constituyen en la clave para aumentar la productividad e inclusión de los sectores marginados de la sociedad. La OCDE señala en este documento:

"… Para que Colombia se embarque en la senda de un crecimiento más sólido e inclusivo y reduzca su dependencia de los recursos naturales, es necesario impulsar la productividad mediante la adopción de reformas estructurales en materia de competencia, regulación, política comercial, infraestructuras, innovación y habilidades. …"[40]

Específicamente en materia de innovación, con el propósito de incrementar la inversión en ciencia, tecnología e innovación, en el año 2011, se creó en Colombia el Fondo de Ciencia, Tecnología e Innovación - FCTeI en el marco del Sistema General de Regalías con una asignación del 10% de los recursos del sistema. Según el Congreso de la República de Colombia el objeto del fondo corresponde a:

"… incrementar la capacidad científica, tecnológica, de innovación y de competitividad de las regiones, mediante proyectos que contribuyan a la producción, uso, integración y apropiación del conocimiento en el aparato productivo y en la sociedad en general, incluidos proyectos relacionados con biotecnología y tecnologías de la información y las comunicaciones, contribuyendo al progreso social, al dinamismo económico, al crecimiento sostenible y una mayor prosperidad para toda la población …"[41]

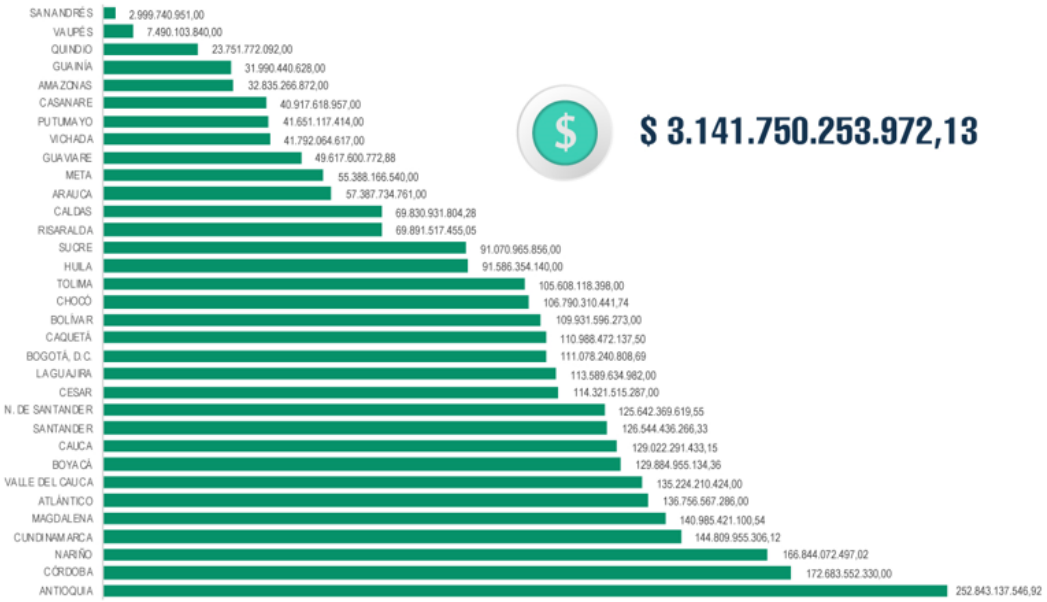
El presupuesto aprobado para el FCTeI en el periodo 2012 – 2019 fue superior a los tres (3) billones de pesos (Figura 3. Presupuesto 2012-2019 Fondo Ciencia, Tecnología e Innovación). Para la línea de I + D empresarial la cifra ascendió al 0.2% del PIB 2019 (Figura 4), indicador muy por debajo del promedio de la OCDE de 2%. Los anteriores datos fueron obtenidos del OBSERVATORIO COLOMBIANO DE CIENCIA Y TECNOLOGIA[42].

[40] (OECD, 2019) Estudios Económicos de la OCDE: Colombia 2019. Obtenido de https://doi.org/10.1787/805f2a79-es

[41] (COLOMBIA. CONGRESO DE LA REPUBLICA, 2011). Acto legislativo 5 de 2011. Artículo 2, mediante el cual se modifica el Artículo 361 de la Constitución Política de Colombia. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/acto_legislativo_05_2011.html

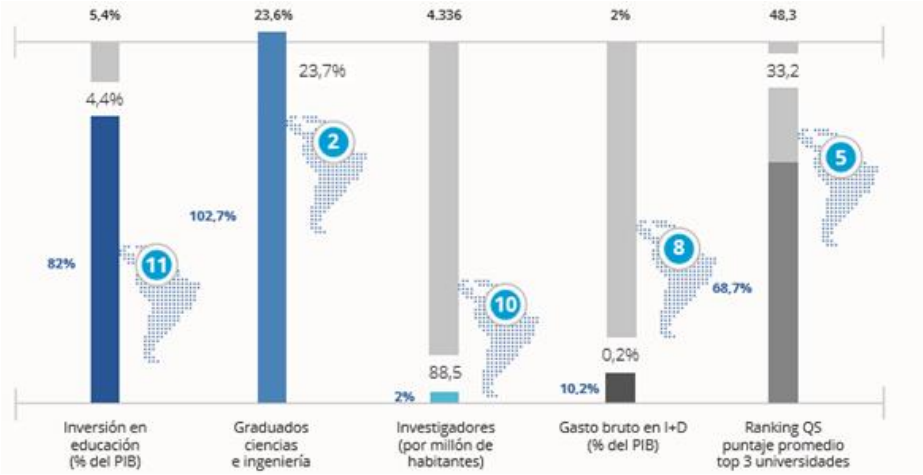
[42] OBSERVATORIO COLOMBIANO DE CIENCIA Y TECNOLOGIA. (Septiembre de 2019). Boletín de análisis de indicadores de ciencia, tecnología e innovación No. 1. *La Eficiencia de la Innovación en Colombia frente al mundo: Un*

Figura 3. Presupuesto 2012-2019 Fondo Ciencia, Tecnología e Innovación



Fuente: Seguimiento Presupuesto de inversión – Secretaría Técnica OCAD del Fondo Ciencia, Tecnología e Innovación del Sistema General de Regalías – SGR a corte del 4 de octubre de 2019. Obtenido de https://www.colciencias.gov.co/portafolio/gestion-territorial/fondo-fctei-sgr/recursos

Figura 4. Comparación indicadores de capacidades versus promedio OECD



Fuente: Global Innovation Index 2019. Cálculos OCyT. Puesto de Colombia en América Latina y el Caribe.

análisis desde el Global Innovation Index, 2016 – 2019. Bogotá, Colombia: OCyT. Recuperado el 2019, de http://www.ocyt.org.co

6.1.2 Tipos de innovación. La innovación se define como:

"146. Una innovación es la introducción de un nuevo, o significativamente mejorado, producto (bien o servicio), de un proceso, de un nuevo método de comercialización o de un nuevo método organizativo, en las prácticas internas de la empresa, la organización del lugar de trabajo o las relaciones exteriores."[43]

Según el Manual de Oslo, a la hora de desarrollar una estrategia, las empresas tienen a su disposición cuatro tipos de innovación (OECD, EUROSTAT, 2005):

> "156. Una **innovación de producto** se corresponde con la introducción de un bien o de un servicio nuevo, o significativamente mejorado, en cuanto a sus características o en cuanto al uso que se destina. Esta definición incluye la mejora significativa de las características técnicas, de los componentes y los materiales, de la información integrada, de la facilidad de uso u otras características funcionales.
> ….
>
> 163. Una **innovación de proceso** es la introducción de un nuevo, o significativamente mejorado, proceso de producción o de distribución. Ello implica cambios significativos en las técnicas, los materiales y/o los programas informáticos.
> ….
>
> 169. Una **innovación de mercadotecnia** es la aplicación de un nuevo método de comercialización que implique cambios significativos del diseño o el envasado de un producto, su posicionamiento, su promoción o su tarificación.
> ….
>
> 177. Una **innovación de organización** es la introducción de un nuevo método organizativo en las prácticas, la organización del lugar de trabajo o las relaciones exteriores de la empresa."[44]

La innovación de producto, por lo general la aplican las grandes empresas, como por ejemplo Apple con el lanzamiento del iPhone, junto con sus actualizaciones y ediciones del producto o dispositivo. Para el tipo de innovación de mercadotecnia, se encuentran los casos de franquicias o las páginas web para ventas en línea. Para el tipo de innovación de organización, se encuentra el caso de la empresa Avon con sus ventas directas. Estas cambiaron la forma del lugar de trabajo. Para la innovación de proceso, están los casos de los sistemas informáticos que permite a los agricultores conocer la evolución y necesidades de los cultivos.

---

[43] OECD, EUROSTAT (2005), Manual de Oslo. Guía para la Recogida e Interpretación de Datos Sobre la Innovación, Tercera Edición, Grupo TRAGSA – Empresa de Transformación Agraria S.A., Pág. 56.

[44] OECD, EUROSTAT (2005), Manual de Oslo. Guía para la Recogida e Interpretación de Datos Sobre la Innovación, Tercera Edición, Grupo TRAGSA – Empresa de Transformación Agraria S.A., Capítulo 3, Pág. 60 – 63.

6.1.3 Las TIC y los procesos de innovación. Las Tecnologías de la Información y las Comunicaciones son herramientas que facilitan el acceso al conocimiento, habilitan el aprendizaje de destrezas, sirven para la potenciación de talentos y estimulan la creatividad y los procesos de innovación.

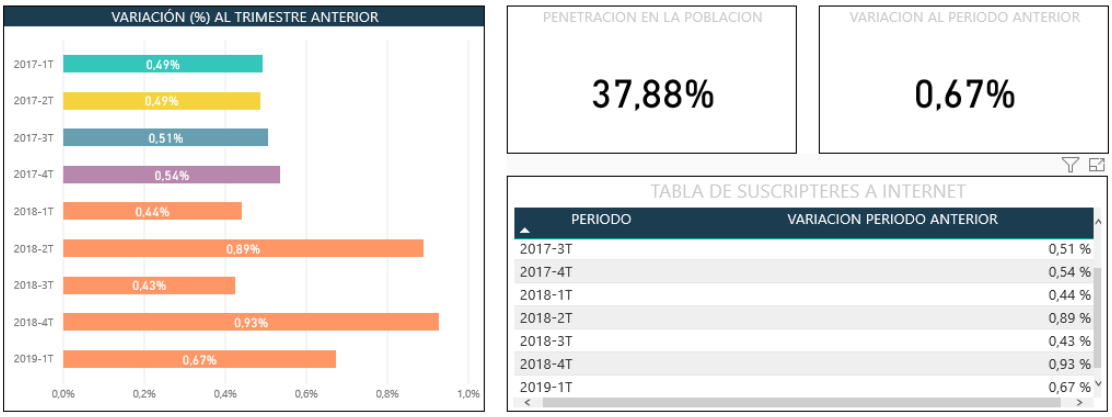
La adopción y uso de las TIC es una forma de innovación empresarial (OECD, 2018), las cuales generan ganancias, reducen las limitaciones geográficas, reducen costos de transacción, mejoran los procesos productivos, misionales y de apoyo de las empresas, permiten el trabajo colaborativo e interoperabilidad entre proveedores y aumentan la diversificación.[45] La introducción de una nueva tecnología de la información y la comunicación es una innovación de proceso si está destinada a mejorar la eficiencia y la calidad de las actividades de los procesos misionales y de apoyo en general.

En ese sentido, el gobierno colombiano ha identificado a la transformación digital, mediante el impulso de una mayor adopción y uso de las tecnologías de información y comunicaciones, como un pilar fundamental para impulsar el crecimiento económico y social del país.

Con corte al segundo trimestre de 2019, Colombia presenta un avance de penetración de internet por suscripción del 37.88% en la población a nivel nacional (
Figura 5. Número de suscriptores de internet a nivel nacionalcon aproximadamente de 18.670.033 suscripciones. Así mismo, según el módulo TIC de la Encuesta Anual Manufacturera (EAM) realizada en la vigencia 2017, el 99.5% de las empresas de los sectores comercio e industria manufacturera contaban con acceso a internet (Figura 6. Porcentaje de empresas que utilizaron computador, internet y sitio web*Figura 6*). En el sector de servicios el porcentaje oscilaba entre 34.1 al 97.1% dependiendo del tipo de empresa. Las empresas encuestadas utilizaron el internet para los siguientes temas: enviar o recibir correo electrónico, búsqueda de información, banca electrónica, servicio al cliente, transacciones con organismos del gobierno, uso de aplicaciones, ya sean compradas, por suscripción o desarrolladas, hacer o recibir pedidos por internet, capacitación de personal, telefonía VoIP, contratación, entrega de productos en forma digitalizada, venta o compra de productos y servicios a través de comercio electrónico.

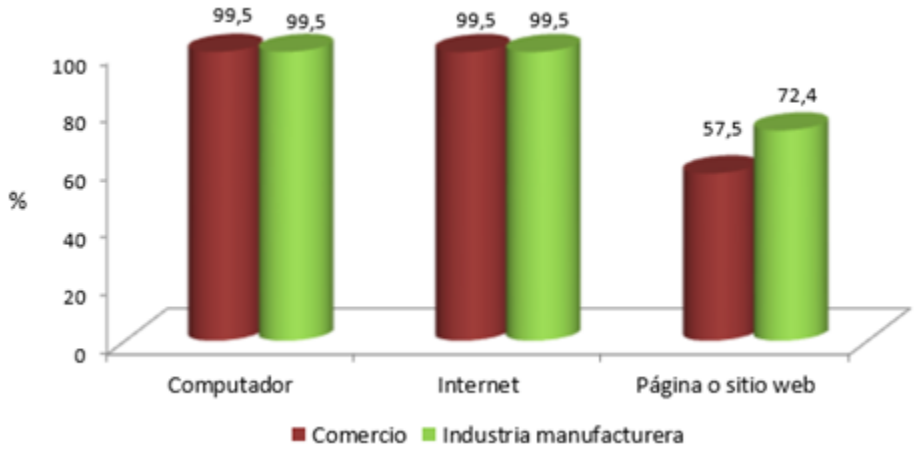
[45] Are ICT Users More Innovative? An Analysis of ICT-Enabled Innovation in OECD Firms. http://www.oecd.org/eco/growth/are ict users more innovative.pdf

Figura 5. Número de suscriptores de internet a nivel nacional



Fuente: Colombia TIC. Portal de Estadísticas del Sector. Obtenido de https://colombiatic.mintic.gov.co/679/w3-propertyvalue-47275.html

Figura 6. Porcentaje de empresas que utilizaron computador, internet y sitio web



Fuente: Colombia TIC. Portal de Estadísticas del Sector. Obtenido de https://colombiatic.mintic.gov.co/679/w3-propertyvalue-47275.html

6.1.4 Nodo de innovación de ciberseguridad. La iniciativa del Ministerio tecnologías de Información y Comunicaciones - MINTIC[46] denominada Investigación, Desarrollo e Innovación – I+D+I, busca fortalecer y dinamizar la sinergia entre la Academia, la Industria y el Estado, para que en conjunto con

[46] MINTIC. https://mintic.gov.co/portal/inicio/Sector-TIC/I+D+I/

actores internacionales se trabaje en el fortalecimiento de la Ciencia, Tecnología y la Innovación en el sector TIC y para las TIC.

A través de la iniciativa (I+D+i), MINTIC[47] promueve la implementación de los Nodos de Innovación con la participación de los actores anteriormente enunciados. Los nodos son espacios de concertación y diseño de soluciones innovadoras a las necesidades y oportunidades TIC identificadas, así como canales de propuesta de proyectos TIC innovadores en temáticas estratégicas, que son consignados en documentos denominados Agendas Estratégicas de Innovación – AEI (Figura 7. Nodos de Innovación de la iniciativa I+D+I*Figura 7*).

Figura 7. Nodos de Innovación de la iniciativa I+D+I

Fuente: MINTIC. Estructura de los nodos de innovación

A continuación, se relacionan y describen los nodos de innovación:

[47] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC. (Junio de 2012). Estructura de los nodos de innovación. Bogotá, Colombia: MINTIC. Obtenido de https://www.mintic.gov.co/portal/604/articles-6116_recurso_4.pdf

Tabla 4. Nodos de Innovación

Nodos de Innovación	Descripción
Salud	Espacio para fomentar la creación de productos, servicios y soluciones para el sector, con el fin de minimizar y contribuir al cierre de la brecha de las iniquidades en salud, a partir de uso y apropiación de las TIC
Justicia	Punto de encuentro y de desarrollo de proyectos para la implementación de soluciones innovadoras de TIC y de alto impacto en el ámbito del sector de justicia
Arquitectura TI	Punto de encuentro donde se definen los temas prioritarios de innovación para el desarrollo de proyectos de TI, con base en la Arquitectura de Referencia de Gobierno en línea.
Servicio al Ciudadano	Es el punto de encuentro de la Academia, la Industria y el Gobierno para generar y discutir prioridades y soluciones TIC para la ciudadanía.
Ciberseguridad	Según el documento CONPES 3701[48], se busca desarrollar una estrategia nacional para defenderse y atacar el incremento de las amenazas que afectan al país en materia cibernética, mediante la generación de capacidades de ciberseguridad para minimizar el nivel de riesgo o exposición de los ciudadanos, ante amenazas o incidentes de seguridad

Fuente: MINTIC. Estructura de los nodos de innovación

El nodo de innovación de ciberseguridad persigue los siguientes objetivos:

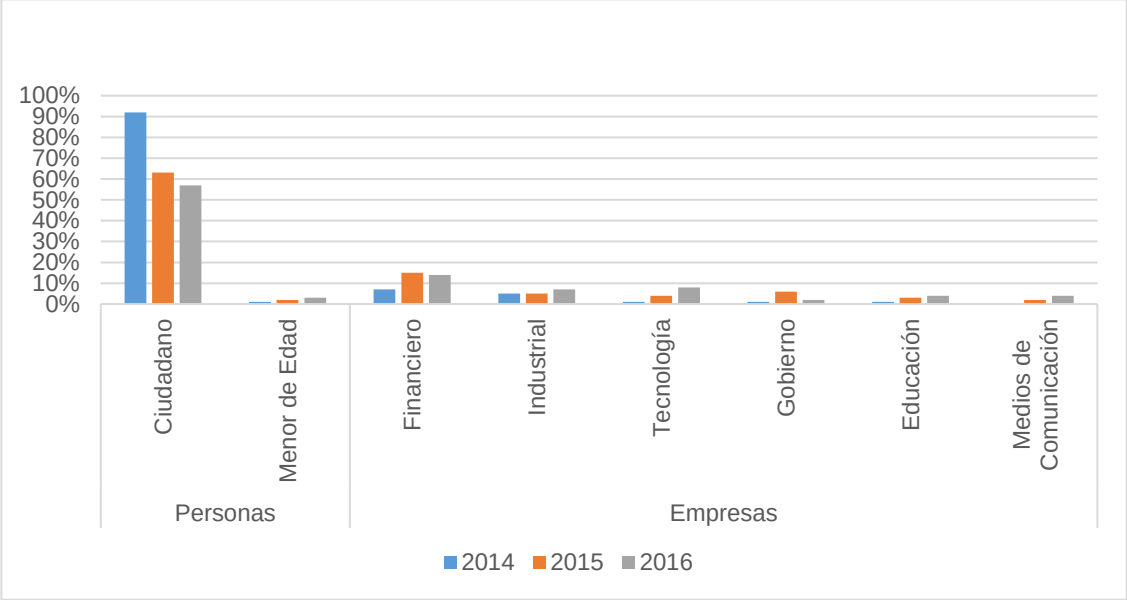
- Fortalecer la posición estratégica en el ciberespacio
- Asegurar la infraestructura del Estado y la protección de los servicios que provee a los ciudadanos
- Enfrentar de forma adecuada los riesgos cibernéticos
- Adaptar las tecnologías existentes
- Generar nuevas tecnologías
- Minimizar y contrarrestar los riesgos e incidentes de naturaleza cibernética en el Estado
- Permitir la apropiación y uso de las tecnologías

6.1.5 Cifras del cibercrimen. Según el informe denominado Amenazas del Ciber crimen en Colombia 2016-2017, publicado por la Policía Nacional de

[48] CONPES 3701. (2011). Lineamientos nacionales de política en Ciberseguridad. Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Colombia[49], entre el 2014 al 2016 se recibieron 15.565 incidentes informáticos a través de las plataformas dispuestas por Centro Cibernético Policial. En la Figura 8. Tendencia de incidentes por grupos de Interés, se ilustra el cambio en la selección de las víctimas, pasando de las personas a las empresas, las cuales generan una mayor rentabilidad a la actividad criminal. Para ese mismo periodo, el informe señala que, del total de incidentes atendidos, el 66% afectaban a la ciudadanía en general, el 12% al sector financiero, el 5% al sector industrial, el 6% al sector de tecnología, el 3% a entidades gubernamentales, el 3% al sector educación y el 3 % a los medios de comunicación.

Figura 8. Tendencia de incidentes por grupos de Interés



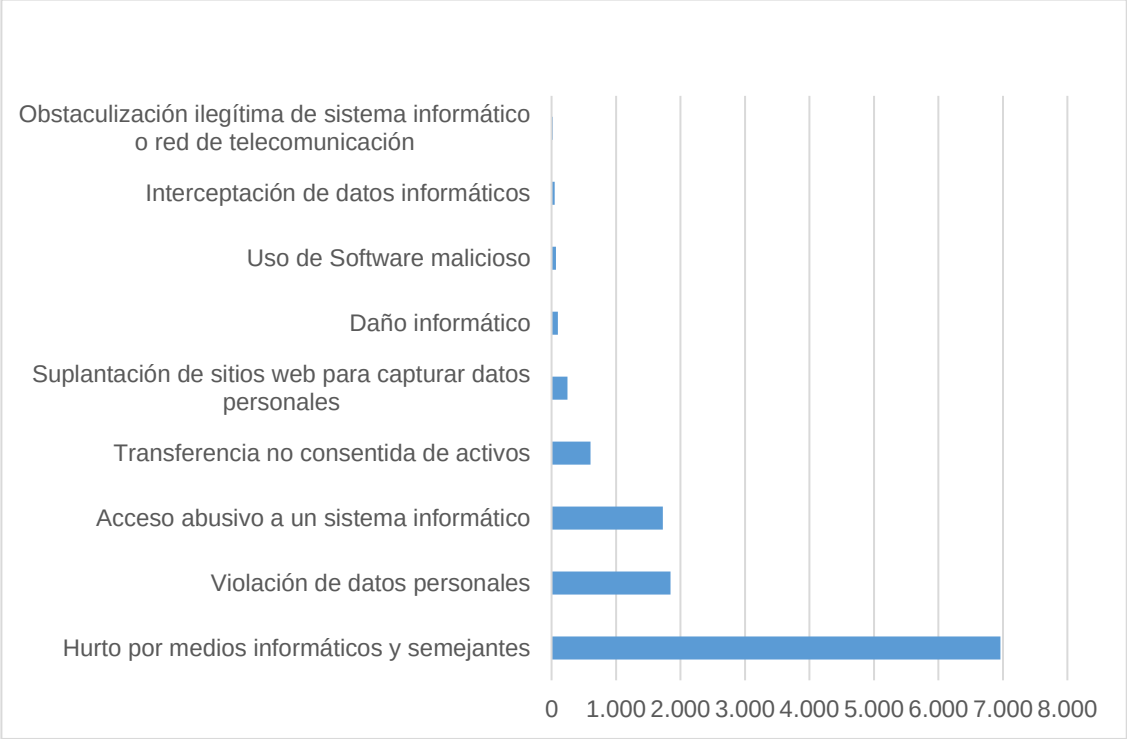
Fuente: POLICIA NACIONAL DE COLOMBIA. Amenazas del Cibercrimen en Colombia 2016-2017

Según el informe Balance Ciber Crimen Colombia 2017 del Centro Cibernético Policial de la Policía Nacional de Colombia[50], se recibieron 11.618 denuncias por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país:

[49] POLICIA NACIONAL DE COLOMBIA. (2018). Amenazas del Cibercrimen en Colombia 2016-2017. Bogotá. Recuperado el 2019, de https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017_1.pdf

[50] POLICIA NACIONAL DE COLOMBIA. (2017). Balance del cibercrimen en Colombia 2017. Bogotá. Recuperado el 2019, de https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

Figura 9. Casos por tipo de delitos



Fuente: POLICIA NACIONAL DE COLOMBIA. (2017). Balance del cibercrimen en Colombia 2017

Según el Centro Cibernético Policial, las modalidades más usadas se relacionan a continuación, indicando que para el año 2017 se presentó un incremento del 29.30% con respecto al año anterior:

- Estafa por suplantación de SIM Card
- Vishing – Tráfico de datos financieros personales
- Fraude por falso WhatsApp
- Ciber pirámides con criptomonedas
- Ataque a entes gubernamentales por infección de programa maligno y la utilización de RAT (Remote Access Tool)
- BEC - Suplantación de correo corporativo
- Carding
- Estafas por internet
- Ventas ilícitas en internet

La Cámara Colombiana de Informática y Telecomunicaciones – CCIT es una entidad gremial privada sin ánimo de lucro, que busca fortalecer el crecimiento y desarrollo del sector TIC en Colombia, con el fin de generar confianza y un entorno favorable para el desarrollo del sector de las TIC.

En el 2016, la CCIT estableció el primer "tanque de análisis y creatividad del sector TIC en Colombia" [51] denominado TicTac, con el fin de proponer iniciativas de política pública orientadas a la transformación digital del país, con base en la sostenibilidad y competitividad económica, la inclusión social, y la eficiencia gubernamental. Actualmente Tictac adelanta los siguientes programas

> "Alianza 80/180. Programa cuyo propósito es crear una red de empresas que genere un espacio de análisis y discusión alrededor de temas relacionados con el Internet de las Cosas (IoT). El programa cuenta con empresas que ofrecen soluciones basadas en el IoT como aquellas que las necesitan para, de esta manera, crear un espacio donde se una la oferta con la demanda.
>
> …
>
> Ciudades VIC: Ciudades Verdes, Inteligentes y Creativas. Programa de política pública, desde las perspectivas de movilidad, seguridad ciudadana, gestión ambiental, despliegue de infraestructura y las Áreas de Desarrollo Naranja (ADNs), creada en miras de orientar el debate electoral gubernamental de 2019 en Colombia, para que sea adoptada y adaptada por los candidatos a las alcaldías y gobernaciones en Colombia como una guía que redunde en la transformación digital de los territorios urbanos en cada rincón del país.
>
> ….
>
> Fintechgración: Destruyendo barreras, construyendo oportunidades. El programa plantea el concepto de Fintechgración como una oportunidad para integrar de manera acelerada, mas no afanada, al sistema financiero tradicional con el uso extendido de nuevas tecnologías a lo largo y ancho de la cadena de valor de los distintos productos y servicios financieros requeridos por la economía y la sociedad.
>
> ….
>
> SAFE: Seguridad Aplicada al Fortalecimiento de las Empresas. Programa que busca sensibilizar a la industria en general frente a los ciberataques, a través de un mapeo de tendencias y modalidades en Colombia y basado en datos, identificando de qué manera incide en su operación."[52]

Conociendo que el cibercrimen se ha convertido en uno de los principales delitos del país, durante el 2019 TicTac fortalece la alianza estratégica con la Policía Nacional para adelantar iniciativas vinculadas con la ciberseguridad. En ese sentido el programa SAFE en asocio con el Centro Cibernético Policial[53],

---

[51] CAMARA COLOMBIANA DE INFORMATICA Y TELECOMUNICACIONES. CCIT. (2019). Tanque de Análisis y Creatividad de las TIC. *tictac*. Bogotá, Colombia. Obtenido de http://www.ccit.org.co/tictac/

[52] http://www.ccit.org.co/tictac/

[53] POLICIA NACIONAL DE COLOMBIA, CCIT. (29 de octubre de 2019). Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020. Bogotá, Colombia.

presentaron las cifras y modalidades de los delitos informáticos en la vigencia 2019 y las tendencias que seguramente enfrentan las empresas y los ciudadanos en el 2020. Estas cifras fueron presentadas en el marco del Estudio de la Tendencias del Cibercrimen en Colombia 2019 – 2020, las cuales se citan de manera resumida:

- Vigencia 2017: Desde julio se recibieron 24.711 denuncias por ciberdelitos en la aplicación denominada “A Denunciar”.

- Vigencia 2018; Se recibieron 983 denuncias menos con respecto a la vigencia 2017, lo que representa una disminución del 5.8%.

- Vigencia 2019: Fueron reportados 28.827 casos por intermedio de los canales de atención. Del total de casos, 15.948 fueron denunciados por sus víctimas como posibles delitos o infracciones a la Ley 1273 de 2009[54]. Los 12.879 incidentes restantes (43%), fueron gestionados sin presentar una denuncia ante la Fiscalía General de la Nacional. La anterior cifra corresponde un incremento del 54% respecto del 2018.

El principal interés de los delincuentes se centra en la motivación económica y el posterior recibo de las ganancias generadas por los ataques. En la Figura 2, se relacionan los delitos informáticos más denunciados en Colombia.

Según la Dirección de Investigación Criminal e INTERPOL[55], dependencias de la Policía Nacional de Colombia, se presentaron los siguientes delitos informáticos (Tabla 5).

[54] COLOMBIA. CONGRESO DE LA REPUBLICA. (5 de Enero de 2009). Ley 1273. *Modificación del Código Penal*. Bogotá, Colombia: Diario oficial. Recuperado el 2019, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[55] DIJIN, INTERPOL. (septiembre de 2019). Frente de Seguridad Empresarial. *Informe*. Bogotá, Colombia. Obtenido de http://edubasc.org/cursos/Vision%20Holistica%20de%20la%20Criminalidad/AYUDAS_VISION_HOLISTICA_2019revisado.pdf

Tabla 5. Delitos informáticos tipificados según Ley 1273 del 2009

Tipo de Delito	Suma del 01/01/2018 al 22/08/2018	Suma del 01/01/2019 al 22/08/2019
Artículo 269I. Hurto por medios informáticos y semejantes	8.233	6.656
Artículo 269A. Acceso abusivo a un sistema informático	1.984	2.187
Artículo 269F. Violación de datos personales	2.141	1.988
Artículo 269J. Transferencia no consentida de activos	805	995
Artículo 269 G. Suplantación de sitios web para capturar datos personales	481	590
Artículo 269 E. Uso de software malicioso	235	292
Artículo 269C. Interceptación de datos informáticos	147	260
Artículo 269D. Daño informático	147	167
Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación	43	66
TOTAL	14.216	13.201

Fuente: DIJIN, INTERPOL. (septiembre de 2019). Frente de Seguridad Empresarial. Informe.

6.1.6 Tendencias del cibercrimen. Según el programa Alianza 80/180 de la CCIT[56], el Internet de las cosas IoT se mantiene el dinamismo de crecimiento y consolidación en todos los sectores, especialmente, en servicios públicos, transporte y la industria, debido al aumento de dispositivos conectados y por la evolución de la infraestructura de conectividad, en donde las redes de quinta generación (5G) se perfilan como uno de sus principales aliados para el corto plazo. Esta dinámica supone un fuerte aumento de brechas y ataques, por lo cual la seguridad digital relacionada con el IoT debe transformarse en una prioridad hasta convertirse en una verdadera tendencia en las empresas.

Conforme a lo consignado en el "Estudio sobre las Tendencias del Cibercrimen en Colombia 2019 – 2020 de la Policía Nacional de Colombia"[57], en el 2020 el cibercrimen continúa sofisticándose con ataques combinados y con la utilización de nuevas capacidades tecnológicas como la inteligencia artificial y técnicas antiforense. Las tendencias se citan según el mencionado informe:

> "Inteligencia artificial y programa maligno. El escaneo automatizado de vulnerabilidades por parte de los Cibercriminales facilita la detección de víctimas

[56] http://alianza80180.com/el-iot-se-convierte-en-megatendencia-para-la-seguridad/

[57] POLICIA NACIONAL DE COLOMBIA, CCIT. (29 de octubre de 2019). Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020. Bogotá, Colombia.

potenciales. El Malware puede detectar si un sistema de seguridad se está analizando (sandbox) y se auto elimina.

Uso de perfiles falsos en redes sociales para difusión de programa maligno. Cuentas falsas en redes sociales como Twitter y Facebook son usadas para generar contenidos de manera automatizada masificando las cifras de infección de programa maligno.

BEC basado en Deepfake. Las empresas en Colombia podrán recibir audios e incluso videos, en los cuales los cibercriminales suplanten a ejecutivos, clientes y proveedores para conseguir transferencias de dinero o despacho de productos. La tecnología Deepfake es una técnica basada en Inteligencia Artificial, que coloca imágenes o videos sobre otro video, así como imitación de voces.

Uso de Botnet para difusión de correos extorsivos. Se prevé el incremento de casos de Sextorsión, basados en el envío masivo de mensajes por parte de los cibercriminales utilizando equipos controlados remotamente (Botnet). La tasa puede alcanzar hasta 30 mil correos por hora.

Uso de mercados ilegales en DarkNet. El cibercrimen seguirá utilizando los foros de la Dark-Net para la venta de datos bancarios en la internet Profunda. Aprovecharán el creciente uso de Criptomonedas en Colombia para facilitar la dispersión de las ganancias de los Ciberataques."[58]

6.1.7 Respuestas al cibercrimen

6.1.7.1 Global Cybersecurity Index. Es una referencia creada por la agencia de las naciones unidad denominada Unión Internacional de Telecomunicaciones[59], ITU por su sigla en inglés, que busca medir el nivel de compromiso de los países con la ciberseguridad a nivel mundial. Este nivel de desarrollo o participación de cada país se evalúa en relación con cinco pilares estratégicos:

i) Jurídico. Mide la existencia de instituciones legales, legislación sobre ciberdelincuencia y regulación de ciberseguridad.
ii) Técnico. Mide la existencia de CSIRT, CERT o CIRT, marco técnico estandarizado de implementación de ciberseguridad, mecanismos de protección, uso de la nube para propósitos de seguridad.

[58] POLICIA NACIONAL DE COLOMBIA, CCIT. (29 de octubre de 2019). Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020. Bogotá, Colombia.

[59] INTERNATIONAL TELECOMMUNICATION UNION – ITU. Global Cibersecurity Index – GCI 2018. ISBN 978-92-61-28201-1. Consultado en https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

iii) Organización. Mide la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad a nivel nacional y métricas de ciberseguridad.
iv) Fortalecimiento de capacidad. Mide la existencia de programas de investigación y desarrollo, educación y formación, profesionales certificados y organismos del sector público que fomenten la creación de capacidad.
v) Cooperación. Mide la existencia de participación en foros y asociaciones, convenios bilaterales y multilaterales de cooperación y redes de intercambio de información público privadas.

De acuerdo con documento Global Cibersecurity Index de 2018, Colombia ocupa a nivel mundial el puesto 73 de 175 países y a nivel del América el puesto 7, con un indicador de 0.565, donde el mayor obtenido fue de 0.931 por el Reino Unido.

Tabla 6. Posiciones Índice Global de Ciberseguridad 2018 Región América

País Miembro	**Puntuación**	**Posición Regional**	**Posición Global**
USA	0.926	1	2
Canadá	0.892	2	9
Uruguay	0.681	3	51
México	0.629	4	63
Paraguay	0.603	5	66
Brasil	0.577	6	70
Colombia	0.565	7	73
Cuba	0.481	8	81
Chile	0.470	9	83
República Dominicana	0.430	10	92
Jamaica	0.407	11	94
Argentina	0.407	11	94

Fuente: INTERNATIONAL TELECOMMUNICATION UNION. Global Cibersecurity Index 2018

6.1.7.2 FIRST. El FIRST[60] es un foro que reúne aproximadamente 529 equipos de seguridad y respuesta a incidentes de los sectores gubernamental, comercial y académico ubicado en 96 países del mundo. Entre los objetivos del foro se encuentra el intercambio de información y la cooperación en cuestiones como nuevas vulnerabilidades o los ataques de amplio alcance en sistemas básicos como los servidores DNS, servidores web e infraestructura crítica. En Colombia se encuentran 12 equipos de respuesta asociados a esta organización:

BS-CSIRT. Centro de operaciones de seguridad de B-Secure para el sector comercial con sede en Colombia. Enlace https://www.b-secure.co/.

C-DOC. Cyber Defense Operation Center para el sector público y privado. Cuenta con un centro de operaciones en Colombia y uno alterno en Estados Unidos. Enlace https://www.c-doc.us/.

CSIRT OLYMPIA. Computer Security Incident Response Team of OLIMPIA DIGITAL para el sector industrial con cubrimiento en varios países de Latinoamérica. Enlace http://www.olimpiait.com/.

CSIRT-ETB. CSIRT de producto de la Empresa de teléfonos de Bogotá – ETB, la cual ofrece servicios a nivel nacional de telefonía, centro de datos, seguridad en la nube para pequeñas y medianas empresas, servicios de conectividad para viviendas y empresas. Enlace http://www.etb.com.co/.

CSIRT-CCIT. CSIRT de la Cámara Colombiana de Informática y Telecomunicaciones – CCIT para el sector de la Informática y las Telecomunicaciones. Enlace www.ccit.org.co.

CSIRT-PONAL. CSIRT de la Policía Nacional de Colombia para sector gobierno y militar. Adicionalmente presenta servicios a los ciudadanos en general. Enlace http://www.ccp.gov.co/

DigiCSIRT. DigiSOC CSIRT para los clientes de DigiSOC S.A.S., divididos en todos los segmentos económicos. Enlace http://www.digiware.net/

ETEK-CSIRT. CSIRT para los usuarios internos de la firma comercial ETEK Internacional y los clientes externos que requieran de servicios de seguridad. Enlace www.etek.com.co

[60] FIRST Foro sobre los Equipos de Respuesta a Incidentes y Seguridad [En línea]. - 10 de mayo de 2020. - https://www.first.org/

ITSSOC-CSIRT. IT SECURITY SERVICES S.A.S SOC CSIRT para el sector gobierno y privado, con clientes principalmente del sector financiero y de seguros. Enlace https://www.itsecurityservices.com.co/

ShieldNow. Para el sector comercial de los elementos del Sistema de Información de la firma 4IT (Usuarios, Sistemas y Redes). Enlace https://shieldnow.co/ o en el sitio https://www.o4it.com/

SOC Team Claro Colombia. Equipo SOC de la marca Claro y sus filiales de Argentina, Brasil, Chile, Estados Unidos, México, Perú y Colombia, la cual ofrece servicios de telecomunicaciones, incluyendo voz, datos y vídeo, acceso a Internet y soluciones integradas para clientes en las pequeñas y medianas empresas, así como grandes corporaciones internacionales. Enlace https://www.claro.com.co

SOC-CCOC. Equipo de respuesta para la gestión de incidentes en seguridad de la información para las Fuerzas Armadas, propietarios y operadores de infraestructura crítica en Colombia. El CCOC es un comando militar conformado por Ejército, Armada y Fuerza Aérea. Enlace ccoc.mil.co

6.1.7.2 CSIRT Financiero. Los sectores financieros y de servicios[61] son los que han realizado más inversiones en acciones para la protección de los datos y de los sistemas de información. Adicionalmente han incorporado prácticas internas de seguridad de la información, en concordancia con el Sistema de Atención al Riesgo Operacional - SARO. En este sentido Asobancaria cuenta con UN CSIRT Financiero el cual tiene entre sus funciones las siguientes:

> "1. Desarrollar y establecer una comunidad de intercambio de inteligencia cibernética,
> 2. Establecer un enfoque organizado y estructural de la gestión de incidentes,
> 3. Sensibilizar a las entidades sobre la importancia de la ciberseguridad y fortalecer las capacidades proactivas con el fin de proteger la infraestructura tecnológica, los activos de información y,
> 4. Mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones."[62]

6.1.7.3 COLCERT. Es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, que se encarga de la gestión de incidentes, prestar colaboración en la resolución de incidentes informáticos y brindar servicios de asistencia técnica

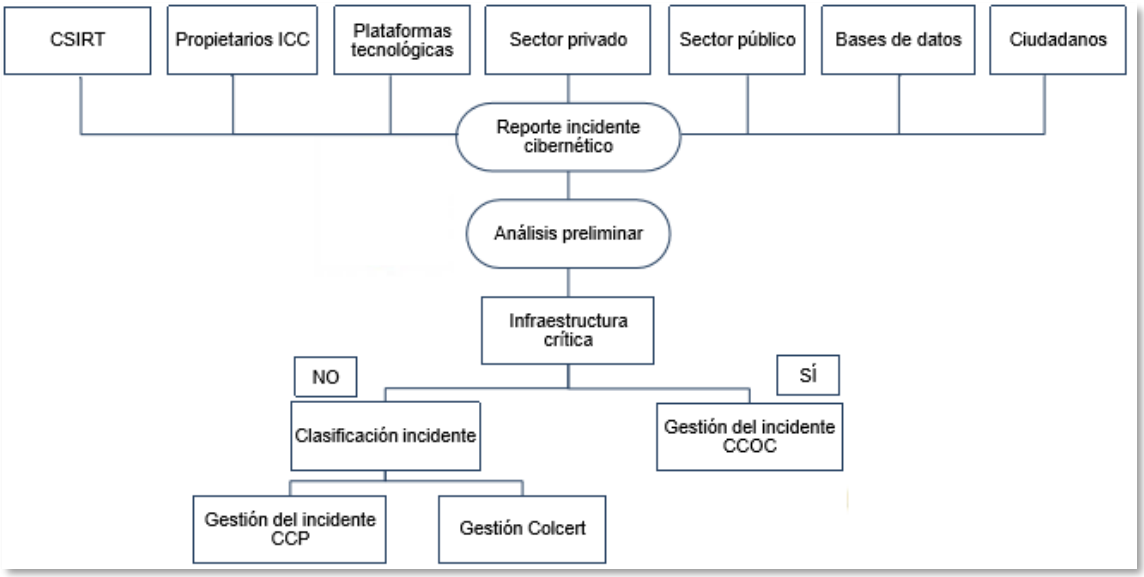
[61] BID, OEA, MINTIC. Estudio Impacto de los incidentes de seguridad digital en Colombia 2017. Consultado en https://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

[62] CSIRT Financiero. Un enfoque proactivo en la gestión de la seguridad. Consultado en https://www.asobancaria.com/csirt/

al sector público y privado. El Colcert hace parte del Ministerio de Defensa y es un punto de coordinación para el reporte de incidentes. Enlace http://www.colcert.gov.co

Con el fin de evitar que este CSIRT de desborden por concentrar el reporte de incidentes de seguridad de las entidades públicas o privadas, el Ministerio de las Tecnologías de Información y las Comunicaciones está liderando la implementación de CSIRT sectoriales, que sirva como gestor de los incidentes de las entidades de un sector respectivo, según el modelo expuesto en la Figura 10. Modelo Nacional de Gestión de Incidentes.

Figura 10. Modelo Nacional de Gestión de Incidentes



Fuente: MINISTERIO DE DEFENSA. Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. Anexo A: Procedimiento Modelo Nacional de Gestión de Incidentes Cibernéticos

6.2 TAXONOMIA DE ATAQUES

Para la definición de la categorización de incidentes, se incorporaron lineamientos del Gobierno de España[63], en lo referente a los niveles de gravedad o peligrosidad del vector de ataque y en los tipos de incidentes aplicables y de

[63] ESPAÑA. CONSEJO NACIONAL DE CIBERSEGURIDAD Guía Nacional de Notificación y Gestión de Ciber incidentes. - Madrid: [s.n.], 2019.p.13-20

mayor ocurrencia en Colombia. La taxonomía de los ataques de describe en los numerales siguientes:

6.2.1 Contenido abusivo. Agrupan los eventos por ataques dirigidos a dañar la imagen del Cliente o a utilizar los recursos tecnológicos infringiendo la normatividad y las leyes.

6.2.1.1 Spam. Es la distribución de correo electrónico de manera masiva, sin que el destinatario del contenido haya otorgado autorización explicita. Estos correos pueden contener material que provoca pánico.

6.2.1.2 Incitación al odio. "Contenido difamatorio o discriminatorio, como acoso, racismo, amenazas a una persona o colectivo de personas." [64]

6.2.1.3 Pornografía infantil. Transmisión de material relacionado con pornografía infantil o pederastia.

6.2.1.4 Contenido sexual o violento inadecuado. Transmisión de material relacionado con pornografía diferente a la infantil, apología de la violencia, racismo o extorsión.

6.2.2 Obtención de información. Agrupan los eventos por ataques dirigidos a obtener información confidencial para generar ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.

6.2.2.1 Escaneo de redes (scanning). Corresponde al envío de solicitudes peticiones a un sistema con el objetivo de realizar la identificación de activos y descubrir posibles vulnerabilidades o debilidades. Mediante esta técnica se ejecutan procesos para recopilar información de los servicios y cuentas, como peticiones DNS, ICMP o escaneo de puertos.

6.2.2.2 Análisis de paquetes (sniffing). Corresponde al análisis y almacenamiento del flujo de datos o tráfico de redes.

6.2.2.3 Ingeniería social. Recopilación de información personal, mediante engaños, sobornos o amenazas.

[64] DISCURSO DE ODIO Y LA INCITACIÓN A LA VIOLENCIA CONTRA LAS PERSONAS LESBIANAS, GAYS, BISEXUALES, TRANS E INTERSEX EN AMÉRICA. Recuperado de http://www.oas.org/es/cidh/expresion/docs/informes/odio/Discurso_de_odio_incitacion_violencia_LGTBI.pdf

6.2.3 Intrusiones. Agrupa los eventos por ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas del Cliente.

6.2.3.1 Explotación de vulnerabilidades conocidas. Intento de interrupción o compromiso de un servicio o sistema mediante el uso de técnicas conocidas como las descritas a continuación.

Desbordamiento de búfer. Consiste en introducir entradas en la memoria de acceso aleatorio denominado búfer, mucho más grandes de las esperadas generando problemas en la ejecución de las aplicaciones. En un programa bien diseñado se debe configurar un tamaño máximo para los datos de entrada garantizando que no supere el valor asignado. Cuando el tamaño de los datos es mayor que el tamaño del búfer, los datos y las instrucciones de ejecución almacenadas en la pila de la aplicación atacada, se sobrescriben generando una violación de segmento en la aplicación. El atacante puede incluir instrucciones en la memoria sobrescrita del búfer para ejecutar alguna aplicación previamente determinada.

Puertas traseras. Son componentes de código de un software que se encuentran ubicados sin realizar ninguna función, los cuales se implementan dando la instrucción causando dificultades en los sistemas informáticos.

Cross site scripting (XSS). Este ataque consiste en introducir un código en una aplicación web, para ejecutar una serie de acciones maliciosas en el servidor. Una página es vulnerable a un ataque XSS, cuando lo que se envía al servidor, aparece posteriormente en la respuesta de la página. Los ataques pueden producir efectos como:

- la toma de control del navegador del usuario,
- modificación del comportamiento y apariencia de la página (pishing),
- visualización de mensajes, imágenes o videos comprometedoras (defacement),
- denegación del servicio (DDos),
- introducción de un gusano para propagarse en el sitio.

Cross Site Request Forgery (CSRF). Consiste en hacer que un usuario haga acciones en un dominio, desde otro. Normalmente este tipo de ataque utiliza a

un usuario validado, para que a través de este introducir solicitudes aparentemente válidas que cambien el comportamiento de la aplicación a favor del atacante. Se produce aprovechando la persistencia de las sesiones entre las pestañas del navegador, usando las credenciales guardadas en la cookie de sesión de un usuario.

Intento de acceso con vulneración de credenciales. Múltiples intentos para obtener o vulnerar credenciales.

6.2.3.2 Ataque desconocido. Explotación de vulnerabilidades mediante el uso de programas o técnicas desconocidas.

6.2.3.3 Compromiso de cuentas empresariales. Según el CCIT de la Policía Nacional de Colombia, "los Ataques BEC, por sus siglas en inglés Business Email Compromise, son una de las principales amenazas a la cadena de suministros, componente fundamental en la actividad diaria de una empresa. Las comunicaciones con proveedores externos y socios de confianza requieren de entornos seguros, que garanticen la integridad de correos electrónicos y servicios de mensajería instantánea utilizados".

Los principales vectores de ataques se relacionan a continuación:

Phishing. Es uno de los ataques más utilizados por los hackers para obtener información mediante correo electrónico o páginas web falsas, con el objetivo obtener nombres de usuarios contraseñas, cuentas bancarias, números de tarjetas crédito, entre otros. Las características del phishing normalmente el texto tiene errores ortográficos, contienen imágenes o logotipos de las páginas.

Correos Fraudulentos Personalizados (Spear Phishing). Es una variante del Phishing, técnica que consiste en el envío de mensajes de correo electrónico con apariencia de legítimos a los empleados de una determinada empresa puede incluir peticiones de nombres de usuario o contraseñas. El objetivo de este ataque consiste en obtener ingreso al sistema informático de una empresa, cuando se responde con un nombre de usuario, clave, clic en vínculos o abre datos adjuntos de un mensaje de correo electrónico, que los direcciona hacia una ventana emergente o un sitio web desarrollado para una estafa.

Enmascaramiento de correos (Spoofing). Es la creación de mensajes de correo electrónico con una dirección de remitente falso. Es fácil de hacer porque los protocolos básicos no tienen ningún mecanismo de autenticación. Se puede llevar a cabo desde dentro de una LAN o desde un entorno externo utilizando troyanos. Emails de spam y phishing suelen utilizar este engaño para inducir a

error al destinatario sobre el origen del mensaje. En la actualidad son muchas las empresas que no implementan el registro SPF en sus servidores de correo o no lo validan y tampoco se comprueba que la dirección IP inversa de quien envía el mensaje sea realmente del servidor de correo legítimo que dice ser SANCHEZ[65].

Infección de sitios frecuentemente visitados por empleados (Watering Hole). Vector de ataque en la que la víctima es un empleado de una empresa en particular. El atacante observa o infiere los sitios web utilizados con frecuencia por la empresa e infecta con programa maligno a uno o varios de los sitios identificados. Eventualmente, algún empleado de la empresa objetivo se infecta. Los atacantes que buscan información sólo pueden atacar a los empleados procedentes de una dirección IP específica.

Ataque por archivo host. También conocido como Pharming. Este tipo de ataque presenta las siguientes características: Los archivos hosts son utilizados en los sistemas operativos Windows, Linux y Mac. En este archivo se almacenan las direcciones realizando una correspondencia entre dominio de Internet y la dirección IP. El sistema verifica esta resolución de nombres, antes que lo haga el servicio DNS. Este es un archivo de texto puede ser editado por el administrador del sistema. El ataque consiste en la modificación del archivo de hosts, con el fin de que las solicitudes de acceso a un sitio por parte de los usuarios del servidor son redirigidas a otra dirección, bajo control de los atacantes. Se usan virus, gusanos y spyware que modifican este archivo para bloquear el acceso a las páginas web de los fabricantes de software antivirus.

6.2.3.4 Compromiso de aplicaciones. Explotación de vulnerabilidades de una aplicación o sistema utilizando técnicas como Defacement, inyección SQL, inyección de ficheros remota.

Defacement. Consiste en vulnerar los servidores o páginas web, dejando modificar la página web o su configuración. La forma de realizar este ataque es utilizar inyección SQL, en el cual logran ingresar a la base de datos de la página web y de esta manera logran ingresar como administrador y modificar las configuraciones de las páginas web.

Inyección SQL. El ataque no se realiza directamente hacia el motor de bases de datos. Este ataque se realiza por intermedio de las aplicaciones, mediante la alteración de una cadena de consulta o instrucción SQL. Si la aplicación se accede desde internet, generalmente el ataque se realiza en el formulario de autenticación a una aplicación, o en el formulario de recuperación de una clave

[65] SANCHEZ Rubén Seguridad en Redes. - [s.l.] : Universidad Autónoma del Estado de Hidalgo.

o en consultas de información donde no se requiere autenticación. Estos ataques se presentan por errores en programación. Si el usuario esta autenticado, podría inyectar código desde cualquier formulario, siempre y cuando la aplicación es vulnerable. Cuando en una aplicación se pretende realizar una consulta de un producto. La aplicación usa código construido dinámicamente y sin validaciones.

Inyección de archivos remota. Consiste en ejecutar código en una aplicación vulnerada. Por lo general afecta a los lenguajes interpretados como PHP, donde es posible adicionar un archivo con código, para su procesamiento del lado del servidor dentro de la ejecución de la aplicación. Los archivos se pueden cargar de manera local como remota.

6.2.4 Compromiso de la información. Agrupan los eventos relacionados con la confidencialidad de la información como el acceso y fuga o relacionados con la integridad de la información como modificación o borrado de información no pública.

6.2.4.1 Acceso no autorizado a información. Comprende la obtención de credenciales de acceso mediante el monitoreo de tráfico o revisión de documentos físicos, accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos y medios de almacenamiento.

6.2.4.2 Modificación no autorizada de información. Un atacante una vez obtenga de manera fraudulenta las credenciales de un sistema o aplicación, puede modificar la información de su interés.

6.2.4.3 Pérdida de información. Robo, fuga o pérdida por fallo físico de un dispositivo de almacenamiento, filtración de líneas telefónicas para uso indebido, espionaje y divulgación de información.

6.2.4.4 Exfiltración de información. Este tipo de ataque se puede realizar mediante la compresión de datos. Los datos, entre ellos los confidenciales, son recopilados y comprimidos con el fin de hacerlos manejables y minimizar la cantidad de datos enviados a través de la red. La compresión se realiza por separado del canal de exfiltración y se realiza mediante un programa, dll o utilidad de compresión común, como 7zip, RAR, ZIP o zlib. Los ataques pueden ocurrir a través de canales cifrados y no cifrados.

6.2.5 Códigos maliciosos. Agrupan los eventos relacionados con software o script dañino que puede auto ejecutarse cuyo objetivo es acceder de manera remota un computador, IoT, sistema u otro dispositivo de red, sin el conocimiento

de su responsable o usuario, con el fin de obtener, eliminar o secuestrar algún activo de información[66].

El principal medio de propagación del programa maligno son los archivos adjuntos enviados por correo electrónico, los cuales esconden el programa a instalar por el atacante. Entre los principales vectores en un ataque de programas maliciosos, se encuentra la suplantación de entidades gubernamentales, mediante el envío masivo de mensajes sobre algún tema de interés de la víctima.

6.2.5.1 Sistema infectado. Sistema, computador o teléfono móvil infectado con software y script maliciosos como rootkit, gusanos, troyanos, virus, Spyware, Ransomware, herramienta para acceso remoto Remote Access Tools (RAT), página Web con script malicioso incrustado.

Troyanos. Tareas escondidas en un software de tal manera que este parezca realizar las actividades comunes pero que se realiza ejecutan tareas ocultas.

Virus. Líneas seguidas de código de una aplicación que ingresan en un archivo que se ejecuta llamado huésped de manera que cuando el archivo se inicia el virus también se activa, infectando a otros programas el modo habitual que se encuentran en el sistema.

Ransomware. Es un programa malicioso con la capacidad de bloquear un dispositivo desde una ubicación remota y cifrar la información y datos almacenados. Mediante esta técnica, un atacante secuestra la información y pide una remuneración, por lo general económica en moneda virtual, por el rescate de esta. El principal medio de propagación del Ransomware es el correo electrónico. Una vez el usuario es engañado o atrapado, es direccionado a un servidor para la descarga de un programa maligno.

Entre los principales vectores en un ataque de ransonware, se encuentran los mensajes sobre embargos o citaciones diligencias judiciales, reportes de centrales de riesgo, alarmas de transferencias no consentidas, foto comparendos, designación como jurado de votación, afiliaciones al sistema de seguridad social en salud.

En Colombia[67] se han detectado los siguientes tipos de Ransomware, donde se destacan variaciones de Wannacry, Crysis, Darma, y Ryuk:

[66] ¿Qué es el código malicioso? (2018). Accedido desde https://latam.kaspersky.com/resource-center/definitions/malicious-code

[67] POLICIA NACIONAL DE COLOMBIA, CCIT. (29 de octubre de 2019). Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020. Bogotá, Colombia.p.12

- Ransomware de cifrado de documentos como hojas de cálculo, imágenes y videos.

- Ransomware de cifrado de los archivos alojados en los servidores web.

- Lock Screen Ransomware WinLocker o bloqueo de la pantalla, impidiendo el acceso y el uso del computador o servidor.

- Master Boot Record (MBR) Ransomware. Infección del registro de arranque maestro y evitar que el sistema operativo se cargue. El Master Boot Record (MBR) es un pequeño programa que se ejecuta cada vez que se inicia el equipo. Se utiliza para el proceso de puesta en marcha del sistema operativo.

- Ransomware de dispositivos móviles. Los dispositivos móviles son infectados por descargas no oficiales. El sistema Android es el más afectado.

6.2.5.2 Servidor de Mando y Control (C&C). Ataque donde un equipo es comprometido por programas maliciosos y Botnet.

Botnet. Es un grupo de sistemas que al ser infectados empiezan a ser parte de una red y ejecutan órdenes recibidas desde un servidos de comando y control. Un sistema entra en un estado de infección en el cual empieza a hacer parte de una red de máquinas controladas por el atacante.

Commonly Used Port. Esta es una de las técnicas para obtener información de una red antes de efectuar un ataque, esta envía uno o varios paquetes de red y luego aguarda los resultados. Existen muchas técnicas para descubrir los puertos que tiene abierto un equipo y determinar qué servicios están corriendo, incluso con que privilegios. Los atacantes utilizan los puertos de uso común, como los puertos TCP 25 (SMTP), 53 (DNS), 80 (http), 443 (https), para evadir los firewalls e IDS y combinan los ataques con la actividad normal.

6.2.5.3 Distribución de Software malicioso. Los recursos tecnológicos son usados para la distribución de software malicioso, identificado mediante comunicaciones maliciosas y Botnet.

Configuración de Software malicioso. Recurso que aloje archivos de configuración de software malicioso como por ejemplo ataque de webinjects para troyano.

Su objetivo es inyectar un código de algún lenguaje como java, javascript, VBScript o html, para engañar al usuario o suplantarlo. Con la inyección de código se quiere modificar el mismo introduciendo parámetros no deseados en los campos, donde los usuarios pueden o están autorizados a ingresar.

Se produce mediante algunas técnicas como:

- spoofing de correo, DNS o IP,
- elevación de privilegios para acceder a información o sistemas restringidos,
- negación de privilegios para interrumpir los procesos o servicios de una organización,
- divulgación de información por un usuario no autorizado
- manipulación (tampering) de algún mecanismo de seguridad mediante la falsificación o la alteración de la información y
- repudio para evitar la certificación o garantía de un hecho.

Minería de Criptomonedas. El CRYPTOJACKING, el inglés Cryptography y Hijack, se refiere a la actividad maliciosa a través de la cual un atacante usa el computador o teléfono de otra persona, con el fin de obtener criptomonedas a través de la ejecución de comandos. Los principales vectores en un ataque de minería de datos son los sitios web infectados y los correos electrónicos. Este método sobrecarga los equipos, disminuyendo su rendimiento dado que recarga el consumo de procesamiento y de red.

6.2.6 Compromiso de la disponibilidad de información. Agrupa los eventos por ataques dirigidos a dejar fuera de servicio los sistemas[68], con el objeto de causar daños en la productividad o en la imagen de los clientes atacados.

6.2.6.1 Denegación de servicio DDOS. Un ataque de denegación de servicios, también llamado ataque DDoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

[68] ¿Qué es Ataque de denegación de servicio (DDoS)? - Definición en WhatIs.com. (2018). Accedido desde https://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

Normalmente provoca la pérdida de la conectividad de la red por el consumo de la transferencia de información (ancho de banda) de la red de la víctima.

Entre las principales causas que origina este tipo de ataque, se encuentran la competencia desleal, empleados inconformes o atacantes que buscan una remuneración económica o un grado de satisfacción.

Entre los principales vectores de un ataque generalizado de denegación de servicio se encuentran la inundación de paquetes SYN, amplificación NTP, saturación utilizando servicios basados en UDP, ping http y ataques de día cero.

6.2.6.2 Denegación de Servicio DoS. Ataque focalizado de denegación de servicio como el envío de solicitudes a sistemas, provocando una afectación al servicio hasta lograr su interrupción.

6.2.6.3 Interrupciones. Interrupciones por causas como desastre natural, operaciones incorrectas, error humano, actualizaciones de software y hardware.

6.2.7 Fraude. Agrupa eventos relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.

6.2.7.1 Uso no autorizado de recursos. Uso de recursos para propósitos ilícitos como beneficio económico por ejemplo el uso de correo electrónico para participar en estafas piramidales.

6.2.7.2 Derechos de autor. Evento de instalación de software sin una licencia de uso autorizada por el fabricante, utilización o distribución de material protegido por derechos de autor como imágenes, documentos, entre otros.

6.2.7.3 Suplantación de Identidad. Una entidad suplanta a otra para convencer a usuarios revelen las cuentas de acceso para obtener beneficios ilegítimos. Mediante técnicas de ingeniería social, los atacantes engañan a los empleados identificados como claves con el fin de suplantar a ejecutivos, clientes y proveedores, con el objeto de que realicen acciones que conllevan a defraudar a las empresas. La forma de hacerlo se presenta en varios tópicos, partiendo desde una llamada telefónica donde se puede presentar la suplantación de personas o al tener un cargo superior al usuario se le presenta amedrentándolo sobre las consecuencias de su negación a colaborar.

6.2.7.4 Secuestro o Cambio de SIM Card. También conocido como SIM SWAPPING, consiste en obtener información de la víctima, ya sea en las redes sociales como en bases de datos atacadas. Los atacantes obtienen un duplicado

de la tarjeta SIM CARD, mediante el reporte de teléfono robado o extraviado al operador que presta el servicio de telefonía de la víctima. Una vez realizado el engaño, los atacantes pueden obtener el acceso a cuentas financieras que tienen habilitado el segundo factor de autenticación a través de mensajes de texto enviados al teléfono.

SIM SWAPPING también es usado en los ataques BEC, mediante la creación chats falsos para la suplantación de gerentes ante las áreas financieras, logrando la transferencia de dineros a cuentas bancarias bajo el dominio del atacante.

6.3 CATALOGO DE SERVICIOS

Según lo consignado en el numeral 4.5 MARCO ESPACIAL, los servicios propuestos se prestarán en el ámbito de un CSIRT comercial. Estos servicios del se agrupan en tres categorías: reactivos, proactivos y de gestión de la calidad de la seguridad. Por definición todo servicio debe agregar valor, por lo cual los servicios de valor añadido no son considerados.

6.3.1 Servicios reactivos. Bajo esta categoría, se consideran los siguientes servicios:

- Gestión de incidentes: Incluye tratamiento, análisis y respuesta virtual o en sitio de incidentes.

6.3.2 Servicios proactivos. Bajo esta categoría, se consideran los siguientes servicios:

- Gestión de disponibilidad y capacidad de la infraestructura: Incluye Monitoreo de redes, aplicaciones y servicios tecnológicos,
- Gestión de comunicaciones: Incluye Comunicados, anuncios, difusión de información relacionada con la seguridad, Boletines diarios y estadísticas
- Gestión de la configuración y mantenimiento de la seguridad: Incluye Servicios de detección de intrusos, seguridad en la nube, identificación y mitigación temprana de riesgos, Análisis periódicos de seguridad digital
- Gestión de alertas y advertencias de seguridad
- Gestión de vulnerabilidades: Incluye tratamiento, análisis, remediación, respuesta y asistencia remota de vulnerabilidades.

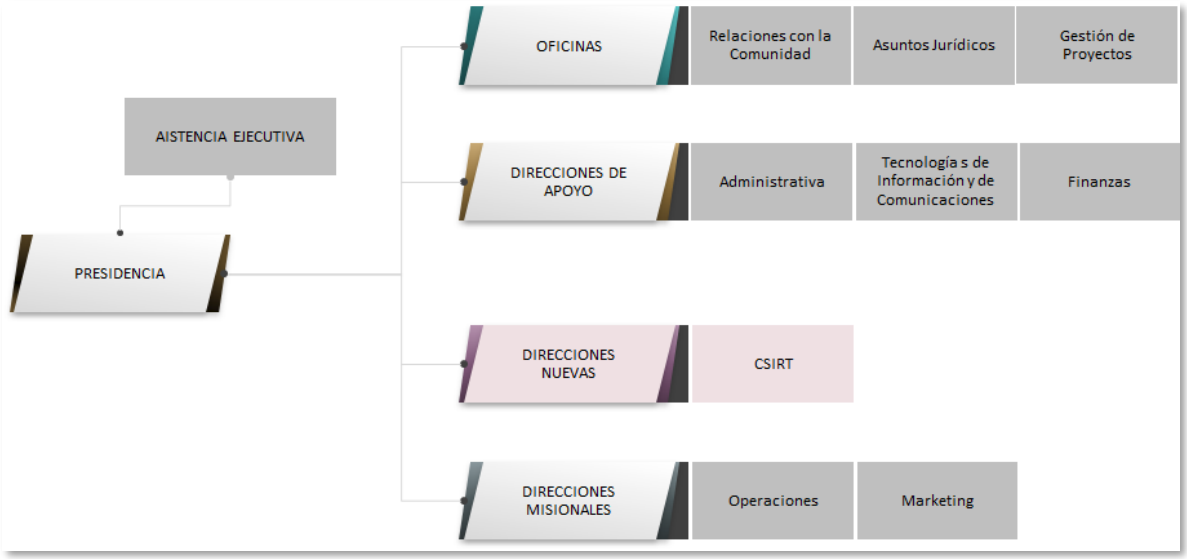
6.3.3 Servicios de gestión de calidad. Bajo esta categoría, se consideran los siguientes servicios:

- Gestión de riesgos de seguridad
- Sensibilización y educación en la gestión de calidad de la seguridad

6.4 MODELO ORGANIZACIONAL

Teniendo en cuenta la clasificación de los modelos organizacionales presentados en el numeral 4.4 MARCO TECNOLOGICO y dado que el objetivo principal es el de realizar el diseño documental para la conformación de un CSIRT para la empresa Cibersecurity de Colombia Limitada, se opta por un modelo organizacional integrado a una organización prexistente. Por lo anterior no se consideran aspectos relativos a la creación de una empresa, entendiéndose que las demás áreas administrativas de la empresa apoyan la creación y el funcionamiento del CSIRT. Permitiendo así, que el desarrollo se centre en el objetivo propuesto, mediante la identificación de procesos, procedimientos y definición de los perfiles. En la Figura 11. Organigrama Propuesto se ilustra el modelo integrado a una organización existente.

Figura 11. Organigrama Propuesto



Fuente: El autor

Para el establecimiento del CSIRT, se define un marco de referencia compuesto por varios elementos con el fin de determinar los objetivos y la visión estratégica del equipo de respuestas ante incidentes. Estos elementos se describen en los siguientes numerales:

6.4.1 Misión. EL CSIRT de Cibersecurity de Colombia Limitada tiene como propósito ofrecer información y asistencia a empresas privadas en la aplicación de medidas proactivas para minimizar la materialización de los riesgos de seguridad informática, así como para responder a los incidentes de seguridad cuando se produzcan.

6.4.2 Visión. Cibersecurity de Colombia LTDA, es una empresa colombiana que presta servicios de seguridad para la protección de la Información, cuyo propósito es el de consolidarse como un Centro de Respuesta a Incidentes Cibernéticos confiable, constituyéndose en un referente a nivel de las empresas privadas en el ámbito de los CSIRT.

6.4.3 Organización. La creación de este CSIRT está promovida por CiberSecurity Colombia Limitada, entidad que ha identificado la necesidad de proveer a las empresas privadas de la capacidad de respuesta ante la ocurrencia de incidentes de seguridad informática. Para lograrlo se han identificado las siguientes necesidades fundamentales de cambio en el relacionamiento con las dependencias y la comunidad y en la misma estructura organizacional:

- La Oficina de Relaciones Públicas se encarga de mantener las actividades de comunicación con la comunidad con el fin de promocionar y divulgar los servicios y el conocimiento relacionados con la seguridad. Esta dependencia debe velar por la confianza y reconocimiento de las empresas, mediante el énfasis en la promoción de sus actividades y servicios, mediante la identificación de los medios disponibles de comunicación, definición de los mecanismos oficiales de divulgación de información de la sala de prensa, participación en eventos y foros especializados, así como adelantar la afiliación a organismos internacionales.

- La Oficina de Asuntos Jurídicos se encarga de mantener actualizada la información de las normas constitucionales, legales, reglamentarias y la jurisprudencia relacionada con las operaciones del CSIRT. Esta oficina debe representar judicialmente a la organización en los procesos judiciales en calidad de accionante o demandado que resulten de las relaciones con la comunidad del CSIRT, así como proteger las pruebas legales en caso de controversias y juicios.

- La Oficina de Gestión de Proyectos, en coordinación con el CSIRT, se encarga de dirigir el análisis de viabilidad, la planeación, ejecución, seguimiento y evaluación de los planes, programas y proyectos orientados al cumplimiento de los objetivos del CSIRT.

- La Dirección Administrativa se encarga de estructurar y hacer el seguimiento a la ejecución de los planes de contratación y de adquisición de bienes y servicios, que incluyan los correspondientes al CSIRT. Se debe realizar el registro y seguimiento, de las peticiones, quejas, reclamos, sugerencias y denuncias - PQRSD que le sean formulados a la entidad, con énfasis en las relaciones con la comunidad objeto del CSIRT y realizar los estudios técnicos para modificar la estructura organizacional y de la planta del talento humano.

- La Dirección de Tecnologías de la Información y de las Comunicaciones, en coordinación con el CSIRT, se encarga de definir e implementar las políticas y mecanismos que permitan la interoperabilidad de los procesos y procedimientos de la gestión de TIC con la gestión de eventos e incidentes de seguridad, mediante la estructuración de metodologías para la implementación de los procesos y técnicas, para la gestión del ciclo de vida de los servicios de la organización. Esta dirección apoya técnicamente y con recursos humanos de ser necesario la gestión del CSIRT y debe trasladar al CSIRT los eventos e incidentes de seguridad de ocurran en la organización.

- La Dirección de Finanzas se encarga de elaborar, ejecutar, modificar, controlar y hacer seguimiento a las políticas, planes y programas relacionados con la gestión y las operaciones presupuestales, contables y de tesorería de los recursos financieros de inversión inicial y de explotación del CSIRT. También debe efectuar el recaudo y el control de las fuentes de los recursos del CSIRT

- La Dirección de Operaciones apoya técnicamente y con recursos humanos de ser necesario la gestión y la implementación de proyectos y servicios del CSIRT.

- La Dirección de Marketing se encarga de identificar los agentes externos principales con los que se interactúa y ofrece los diferentes servicios a las empresas objeto del CSIRT

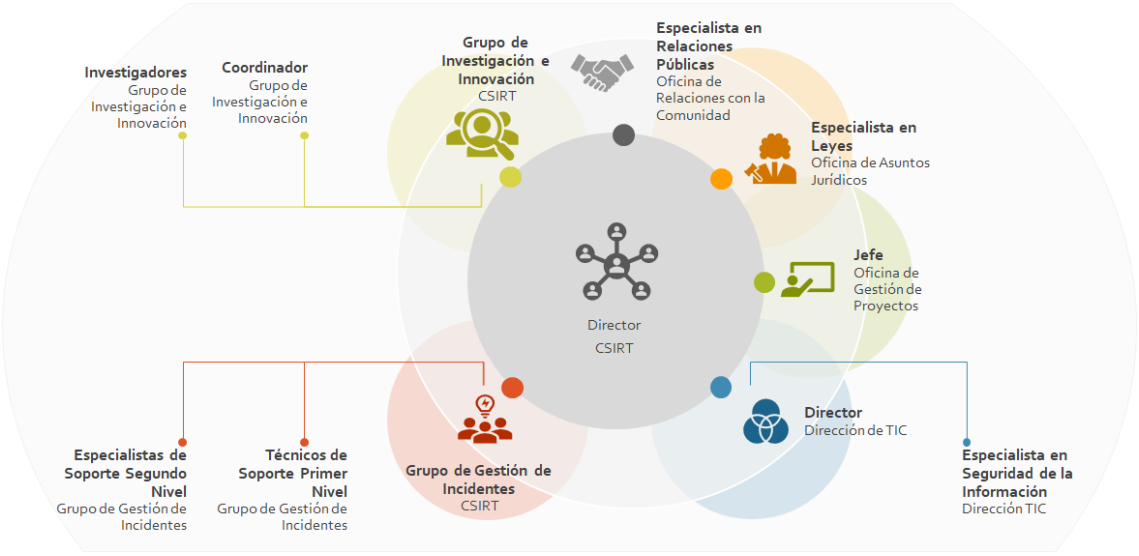
6.4.4 Estructuración del CSIRT. Para el inicio de operaciones se debe contar con el siguiente equipo de trabajo, ver Figura 12. Estructura del CSIRT, el cual depende de la magnitud de la demanda de los servicios ofertados en un momento determinado:

- Director quién gestiona el equipo del CSIRT, con formación en seguridad y experiencia en procesos de gestión de crisis y continuidad del negocio. Es el punto de contacto técnico entre las dependencias, comunidad y los colaboradores externos.

- Grupo de Investigación e Innovación, conformado por un (1) Coordinador y tres (3) investigadores, encargados del desarrollo y entrega de los servicios. Los investigadores deben contar con conocimientos en seguridad y experiencia en implementación de proyectos de seguridad.

- Grupo de Gestión de Incidentes. El grupo está conformado por los siguientes técnicos y especialistas, con capacidades de trabajo en equipo, bajo presión y disposición para trabajar en diferentes horarios, con el fin de brindar un nivel de servicio 7x24: i) tres (3) técnicos para el soporte de primer nivel de servicio, con conocimientos básicos en tecnologías de la información y comunicaciones para entender y atender los incidentes de seguridad que se presenten y ii) tres (3) especialistas para el soporte de segundo nivel de servicio, con conocimientos técnicos en distintas áreas de la seguridad y habilidades de intercomunicación con otros miembros de la comunidad y proveedores de servicios de Internet. Son los responsables de gestionar las situaciones de emergencia originadas por la ocurrencia de los incidentes. Adicionalmente tiene a su cargo las funciones de formación, divulgación y análisis forenses.

Figura 12. Estructura del CSIRT



Fuente: El autor

- Especialista en seguridad de la Información. Ubicado en la Dirección de TIC, responsable de la operación y administración de los sistemas que aportan el CSIRT en su operación.

- Especialista en Relaciones Públicas. Ubicado en la Oficina de Relaciones con la Comunidad, encargado de mantener las actividades de comunicación

con la Comunidad para promocionar y divulgar el conocimiento y los servicios que presta.

- Especialista en Leyes. Ubicado en la Oficina de Asuntos Jurídicos en leyes, experto para tratar los asuntos jurídicos relacionados con el CSIRT y en caso de juicio, proteja las pruebas legales correspondientes.

6.4.5 Manual de Funciones. Establecer el gobierno del CSIRT es una actividad estratégica mediante la cual se definen las funciones, roles y responsabilidades del personal en los diferentes niveles de la estructura de CiberSecurity de modo que se logren los objetivos propuestos. El alcance de este manual está dado por la definición de funciones y actividades a realizar acerca de la gestión del CSIRT, por medio de la asignación de responsabilidades por cada rol definido como se especifica en la siguiente tabla:

Tabla 7. Roles y responsabilidades del CSIRT

ROL	RESPONSABILIDADES
Director CSIRT	• Realizar las actividades de planeación, ejecución y control de las políticas, planes, programas y proyectos relacionados con la gestión y las operaciones del CSIRT • Liderar y dirigir la gestión del equipo de trabajo del CSIRT, en lo referente a la gestión de incidentes de seguridad, análisis forense y de las investigaciones tecnológicas relacionadas con los objetivos, funciones y actividades del CSIRT. • Promover la interacción entre los diferentes CSIRT y colaboradores externos nacionales, a partir de la suscripción de acuerdos de cooperación y el establecimiento de relaciones de confianza, para facilitar el intercambio de información y de servicios entre las organizaciones y actores del sector. • Adelantar las gestiones necesarias para realizar los procesos de contratación de bienes y servicios de acuerdo con las necesidades de su dependencia, así como realizar el seguimiento de los contratos que se deriven. • Asegurar la aplicación de los estándares, buenas prácticas y principios para la gestión de claves y autorización de los permisos para el acceso y suministro de la información a cargo de la dependencia. • Coordinar con la Oficina de Gestión de Proyectos el análisis de viabilidad, la planeación, ejecución, seguimiento y evaluación de los planes, programas y proyectos orientados al cumplimiento de los objetivos del CSIRT.

	• Coordinar con la Dirección de Tecnologías de la Información y de las Comunicaciones, la definición e implementación de las políticas y mecanismos que permitan la interoperabilidad de los procesos y procedimientos de la gestión de TIC con la gestión de eventos e incidentes de seguridad. • Comunicar tanto a las partes internas como externas el impacto de la materialización de incidentes, así como las acciones de respuesta. • Realiza seguimiento sobre las acciones correctivas y preventivas en torno a los riesgos, incidentes y problemas de la seguridad de la información.
Coordinador del Grupo de Investigación e Innovación	• Coordinar las actividades de planeación, formación, desarrollo de soluciones e investigación de nuevas tendencias y amenazas de la seguridad cibernética • Realizar labores de investigación sobre medidas para atender riesgos y demás factores de seguridad. • Liderar los proyectos de seguridad de la información que le sean asignados • Mantener actualizado el catálogo de servicios del CSIRT • Estructurar y dirigir el observatorio de tecnología, mediante el análisis estadístico de incidentes y tendencias. • Apoyar técnicamente al grupo de gestión de incidentes en la resolución de vulnerabilidades y análisis de código malicioso.
Investigadores	• Realizar investigaciones de nuevas tendencias y amenazas de seguridad informática. • Realizar investigaciones sobre redes e ingeniería sociales • Desarrollar material técnico para el uso interno o de formación. • Desarrollar herramientas de seguridad, monitoreo y seguimiento. • Realizar cursos de formación en seguridad informática • Definir la metodología y establece el plan para capacitaciones y fomento de la sensibilización en seguridad de la información
Coordinador del Grupo de Gestión de Incidentes	• Coordinar las actividades de análisis, asesoramiento, seguimiento sobre los incidentes de seguridad y en general gestionar las situaciones de emergencia originadas por la ocurrencia de incidentes. • Coordinar las respuestas a incidentes y vulnerabilidades. • Tomar las decisiones sobre los asuntos relacionados a los activos de información en la identificación de riesgos o cuando ocurre un evento de seguridad. • Ofrecer un entendimiento claro sobre el impacto del negocio en los procesos por medio del análisis de impacto al negocio BIA o en el plan de respuesta a incidente.

	• Mantener la comunicación con organizaciones y colaboradores externos que gestionen incidentes de seguridad en otros CSIRT
Técnicos de Soporte de Primer Nivel	• Prestar asistencia inicial en la atención de los eventos e incidentes de seguridad de bajo nivel. • Registrar, analizar, clasificar y priorizar la información recibida de los casos de incidentes y eventos de seguridad • Apoyar la recolección de información y documentación sobre afectaciones a la seguridad de la información. • Monitorear la infraestructura crítica de los clientes • Prestar asistencia técnica remota en vulnerabilidades e incidentes
Especialistas de Soporte de Segundo Nivel	• Solucionar, documentar e informar sobre la solución de eventos o incidentes que atenten contra la seguridad de la información. • Contribuir con la toma de evidencias digitales y con su cadena de custodia. • Implementa medidas para la gestión de seguridad de la información y de respuesta a incidentes. • Realizar monitoreo sobre el funcionamiento y la capacidad de los recursos tecnológicos de los clientes. • Adelantar acciones formativas para la transferencia de conocimiento a la Comunidad y a los colaboradores técnicos y funcionales de la organización y de los clientes • Realizar el análisis, tratamiento y respuesta a las vulnerabilidades. • Prestar asistencia técnica remota o presencial en vulnerabilidades e incidentes
Especialista en Seguridad de la Información	• Administrar, configurar y mantener los sistemas y herramientas de seguridad del CSIRT • Gestionar y mantener la infraestructura de red del CSIRT. • Asistir y colaborar en la respuesta a incidentes cuando se necesita conocimiento en sistemas y herramientas de seguridad. • Gestionar el acceso a repositorios seguros de información. • Establecer los niveles y tipos de acceso de los usuarios sobre los diferentes activos de información. • Eliminar o solicitar la eliminación de usuarios que tienen acceso a los diferentes sistemas de información
Especialistas en Relaciones Públicas	• Mantener las actividades de comunicación con la comunidad para promocionar y divulgar el conocimiento y los servicios que presta. • Velar por la confianza y reconocimiento de las empresas, mediante el énfasis en la promoción de sus actividades y servicios.

	• Identificar, definir y mantener los medios sociales de comunicación y de los mecanismos oficiales de divulgación de información del CSIRT • Participar en eventos y foros especializados, así como adelantar la afiliación a organismos internacionales. • Elaborar y publicar documentos CSIRT. • Mantener actualizado el portal web del CSIRT
Especialista en Leyes	• Representar judicialmente a la organización en los procesos judiciales en calidad de accionante o demandado que resulten de las relaciones con la comunidad del CSIRT • Proteger las pruebas legales en caso de controversias y juicios.

Fuente: El autor

6.5 MANUAL DE POLÍTICAS Y PROCEDIMIENTOS OPERACIONALES

En este capítulo se desarrollarán las políticas y procedimientos operacionales con el fin de generar un marco de referencia de cómo proceder en la gestión de incidentes, recolección y custodia de evidencias, intercambio de información y comunicación de incidentes a organismos competentes según la legislación vigente.

6.5.1 Gestión de incidentes

6.5.1.1 Política. Dependiendo de los servicios del CSIRT contratados por un Cliente, se debe gestionar que sus sistemas de información, dispositivos de red y demás servicios tecnológicos deben contar con mecanismos de registros de auditoría debidamente protegidos y respaldados en donde las finalidades de estos buscan lo siguiente:

- Identificación de usuarios.
- Datos consultados, modificados o eliminados.
- Intentos fallidos de conexión.
- Tipos de transacción realizada.
- Fechas, horas y detalles de los eventos clave, (entrada y salida).
- Intentos de acceso al sistema exitosos y rechazados.
- Establecer los cambios a la configuración del sistema
- Uso de privilegios.
- Acceso a archivos y tipo de acceso
- Identificación del dispositivo o ubicación, si es posible, e identificador del sistema.

Los empleados y contratistas de CyberSecurity Ltda que por su relación con el CSIRT tenga acceso a la información del Cliente, deben reportar oportunamente sobre cualquier incidente de seguridad del cual tengan conocimiento, por medio de los canales dispuestos por el CSIRT.

Para la exactitud de los registros de auditoría, la fecha y hora de las herramientas de gestión de incidentes, deben estar sincronizados con la hora legal colombiana.

Con el fin de realizar un adecuado análisis, contención y erradicación de los eventos de seguridad, se debe aplicar la siguiente clasificación de incidentes.

Tabla 8. Clasificación de incidentes

Categoría	Tipo incidente	Ejemplos
Contenido abusivo	Spam	• Distribución de correo electrónico de manera masiva, sin que el destinatario del contenido haya otorgado autorización explicita. • Abuso y mal uso de los servicios informáticos • Transmisión de material que provoca pánico
	Incitación al odio	• "Contenido difamatorio o discriminatorio, como acoso, racismo, amenazas a una persona o colectivo de personas." [69]
	Pornografía infantil	Transmisión de material relacionado con: • Pornográfico infantil • Pederastia
	Contenido sexual o violento inadecuado	Transmisión de material relacionado con: • Pornografía diferente a la infantil • Apología de la violencia • Racismo • Extorsión
Obtención de información.	Escaneo de redes (scanning)	• Envío de solicitudes peticiones a un sistema con el objetivo de realizar la identificación de activos y descubrir posibles vulnerabilidades o debilidades. Mediante esta técnica se ejecutan procesos para recopilar información de los

69 http://www.oas.org/es/cidh/expresion/docs/informes/odio/Discurso_de_odio_incitacion_violencia_LGTBI.pdf

Categoría	Tipo incidente	Ejemplos
		servicios y cuentas, como peticiones DNS, ICMP o escaneo de puertos.
	Análisis de paquetes (sniffing)	• Análisis y almacenamiento del flujo de datos o del tráfico de redes
	Ingeniería social	• Recopilación de información personal, mediante engaños, sobornos o amenazas.
Intrusiones	Explotación de vulnerabilidades conocidas	• Intento de interrupción o compromiso de un servicio o sistema mediante el uso de técnicas conocidas como Desbordamiento de buffer, puertas traseras, cross site scripting (XSS), Cross-Site Request Forgery (CSRF)
	Intento de acceso con vulneración de credenciales	Múltiples intentos para obtener o vulnerar credenciales.
	Ataque desconocido	• Explotación de vulnerabilidades mediante el uso de programas o técnicas desconocidas.

	Compromiso de cuenta con privilegios	• La cuenta de un usuario administrador o con privilegios es obtenida mediante el uso de técnicas como:
		  • Phishing
		  • Spear phising
		  • Pharming
		  • Préstamo de usuario y contraseña

	Compromiso de cuenta sin privilegios	• La cuenta de un usuario sin privilegios es obtenida mediante el uso de técnicas como:
		  • Phishing
		  • Spear phising
		  • Pharming
		  • Préstamo de usuario y contraseña

	Compromiso de aplicaciones	• Explotación de vulnerabilidades de una aplicación o sistema utilizando técnicas como:
		  • Defacement
		  • inyección SQL.
		  • Inyección de Ficheros Remota

Compromiso de la información	Acceso no autorizado a información	• Obtención de credenciales de acceso mediante el monitoreo de tráfico o revisión de documentos físicos.

Categoría	Tipo incidente	Ejemplos
		• Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos. • Ingreso de medios de almacenamiento no autorizado.
	Modificación no autorizada de información	• Modificación de información obtención de manera fraudulenta de las credenciales de acceso a un sistema o aplicación
	Pérdida de información	• Pérdida por fallo físico de un dispositivo de almacenamiento como discos duros. • Fuga, robo o pérdida de Información. • Filtración de líneas telefónicas para uso indebido • Espionaje y divulgación de información
Códigos maliciosos	Sistema infectado	Sistema computador o teléfono móvil infectado con software y script maliciosos como: • rootkit • Gusanos • Troyanos • Virus • Spyware • Ransomware • Herramienta para Acceso Remoto Remote Access Tools (RAT) • Página Web con script malicioso incrustado
	Servidor de Mando y Control (C&C)	Ataque donde un equipo es comprometido por programas maliciosos y Botnet
	Distribución de Software malicioso	• Recurso usado para distribución de software malicioso, identificado mediante comunicaciones maliciosas y Botnet
	Configuración de Software malicioso	• Recurso que aloje archivos de configuración de software malicioso como por ejemplo ataque de webinjects para troyano.
Compromiso de la disponibilidad de información	Denegación de Servicio - DoS	• Ataque focalizado de denegación de servicio como el envío de solicitudes a sistemas, provocando una afectación al servicio hasta lograr su interrupción.
	Denegación distribuida de Servicio - DDoS	• Ataque generalizado de denegación de servicio como: • Inundación de paquetes SYN,

Categoría	Tipo incidente	Ejemplos
		• Amplificación NTP • Saturación utilizando servicios basados en UDP, ping http. • Ataques de día cero
	Interrupciones	Interrupciones por causas como: • Desastre natural • Operaciones incorrectas • Error humano • Actualizaciones de software y hardware
Fraude	Uso no autorizado de recursos	• Uso de recursos para propósitos ilícitos como beneficio económico por ejemplo el uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	• Evento de instalación de software sin una licencia de uso autorizada por el fabricante, • Utilización o distribución de material protegido por derechos de autor como imágenes, documentos, entre otro
	Suplantación de Identidad	• Una entidad suplanta a otra para convencer a usuarios revelen las cuentas de acceso para obtener beneficios ilegítimos.
Otros	Otros incidentes	Todo incidente que no se pueda categorizar ni tipificar.

Fuente: CONSEJO NACIONAL DE CIBERSEGURIDAD. Guía Nacional de Notificación y Gestión de Ciber incidentes

Se deben aplicar los siguientes niveles de criticidad de los incidentes, dependiendo del valor o importancia de los sistemas afectados que soportan los procesos del cliente, tomando como insumo lo señalado en la Tabla 9. Para la definición de estos niveles, se incorporaron lineamientos del Modelo de Seguridad y Privacidad de la Información de MINTIC[70].

[70] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 21] Seguridad y Privacidad de la Información // Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. - Bogotá : MINTIC, 2016.p.17

Tabla 9. Niveles de criticidad del activo de información

Nivel de criticidad	Valor	Definición
Inferior	0.1	Activos de información no críticos, como estaciones de trabajo de usuarios con funciones no críticas
Bajo	0.25	Activos de información que apoyan a un solo proceso de la entidad.
Medio	0.5	Activos de información que apoyan más de un proceso de la entidad.
Alto	0.75	Activos de información pertenecientes a la Dirección de Gestión de Tecnologías de Información y Comunicaciones o estaciones de trabajo de usuarios con funciones críticas.
Superior	1	Activos de información críticos

Fuente: MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información

Se deben aplicar los siguientes niveles de impacto actual[71] y futuro[72] de los incidentes, conforme a la escala señala en la Tabla 10. Para la definición de estos niveles, se incorporaron lineamientos del Modelo de Seguridad y Privacidad de la Información de MINTIC[73].

Tabla 10. Niveles de impacto actual y futuro

Nivel de impacto	Valor	Definición
Inferior	0.1	Impacto leve en un activo de información.
Bajo	0.25	Impacto moderado en un activo de información.
Medio	0.5	Impacto alto en un activo de información.
Alto	0.75	Impacto moderado en más de un activo de información.
Superior	1	Impacto alto en más de un activo de información.

Fuente: MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información

[71] Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

[72] Impacto Futuro: Depende de la cantidad de daño que puede causar el incidente si no es contenido y erradicado.

[73] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 21] Seguridad y Privacidad de la Información // Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. - Bogotá : MINTIC, 2016.p.17-18

La priorización de los eventos e incidentes de seguridad se define por la siguiente formula:

$$\text{Prioridad} = [\text{Impacto Actual} * 2.5] + [\text{Impacto Futuro} * 2.5] + [\text{Criticidad del activo} * 5]$$

Con la información definida sobre criticidad e impacto se calcula el valor de la prioridad del incidente y se valida frente a la escala de la columna Valor. Adicionalmente se estima el tiempo de respuesta para ser atendido un incidente.

Tabla 11. Niveles de prioridad del incidente

Prioridad	Valor	Tiempo de Respuesta
Inferior	00,00 – 02,49	3 horas
Bajo	02,50 – 03,74	1 hora
Medio	03,75 – 04,99	30 min
Alto	05,00 – 07,49	15 min
Superior	07,50 – 10,00	5 min

Fuente: MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información

6.5.1.2 Procedimiento. Inicia con el reporte del evento por parte de Cliente, Comunidad o proveedores de servicios a través de los canales definidos en el sistema de gestión de incidentes, continúa con el análisis, priorización y definición de planes de acción para contención, erradicación, recuperación de los activos de información afectados y reporte ante las instancias respectivas. Finaliza con el seguimiento periódico de incidentes de seguridad con el fin de establecer planes de mejora.

Tabla 12. Procedimiento de gestión de incidentes de seguridad

No	Actividad	Descripción de la Actividad	Responsable	Registro
1	Reportar un evento de seguridad	El Cliente, Comunidad, herramienta de monitoreo o el Técnico de Soporte de Primer Nivel reportan el evento de seguridad como resultado de: • Investigación inicial por monitoreo de redes • Reporte de eventos directamente por herramienta de monitoreo.	Cliente, Comunidad, Proveedor, herramienta de monitoreo o el Técnico de Soporte de Primer Nivel	Interacciones en el sistema de gestión de incidentes

No	Actividad	Descripción de la Actividad	Responsable	Registro
		• Notificaciones recibidas por el Cliente • Notificaciones recibidas por la Comunidad en General		
2	Registrar caso de un evento o incidente de seguridad	El Cliente, herramienta de monitoreo o el Técnico de Soporte de Primer Nivel registra el caso en el sistema de gestión de incidentes con la siguiente información mínima: • Identidad del usuario • Fecha y hora del reporte • Miembro de la Comunidad o Cliente • Descripción de la situación notificada	Cliente, herramienta de monitoreo o el Técnico de Soporte de Primer Nivel	Casos en el sistema de gestión de incidentes
3 **PC**	Validar pertinencia de clasificación	El técnico determina si es un Incidente de Seguridad tomando como insumo las categorías de incidentes definidas en las políticas de operación del presente proceso. ¿Es considerado como evento o incidente de Seguridad? **SI**: Se continuará con la siguiente actividad. **NO:** Se cierra y se notifica el caso Toda acción realizada deberá quedar registrada dentro del sistema de gestión de incidentes	Técnico de soporte primer nivel	Caso cerrado en el sistema de gestión de incidentes
4	Identificar y asignar el evento de seguridad	El técnico de soporte de primer nivel, una vez que un caso ha sido catalogado como Incidente de Seguridad, asigna el caso al Técnico o especialista de soporte para el respectivo análisis.	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel	Caso asignado en el sistema de gestión de incidentes
5	Recolectar y manejar evidencia del evento de seguridad	El investigador o quién haga las veces de analista forense junto con las personas que este crea pertinente, una vez ha confirmado el evento o incidente de Seguridad de la Información	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel	Pruebas recolectadas

No	Actividad	Descripción de la Actividad	Responsable	Registro
		inicia la recolección de pruebas realizando la debida cadena de custodia de las evidencias. Para esto debe tomar las consideraciones definidas en las políticas del procedimiento de recolección y cadena de custodia. Adicionalmente, si se requiere se puede solicitar apoyo de las entidades especializadas en recolección de información y evidencia forense.	Investigador / Analista Forense	
6	Valorar criticidad y nivel de impacto del incidente de seguridad	El técnico o especialista, una vez cuente con la evidencia necesaria del incidente de seguridad, con el propósito de definir la priorización para la resolución de este; establece tanto el impacto como la criticidad conforme con las políticas de operación definidas en el actual procedimiento. En este paso se debe • Hay que confirmar que no es un falso positivo • Correlacionar la información recibida con el resto de información del sistema de gestión • Enlazar el tiquete en otro ya existente • Reclasificar el incidente • Priorizar el incidente	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel	Caso valorado en el sistema de gestión de incidentes
7	Definir estrategia de contención	Los responsables que se hayan determinado después de la valoración del incidente de Seguridad de la Información, con el propósito de realizar las recuperaciones necesarias, definen la estrategia de contención del incidente. Para lo cual, se debe tener en cuenta: i. Daño potencial de activos de información por causa del evento o incidente	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel	Acta de reunión

No	Actividad	Descripción de la Actividad	Responsable	Registro
		teniendo en cuenta la criticidad del activo. ii. Preservación de la evidencia. iii. Tiempo y recursos internos y externos necesarios para la estrategia. iv. Duración estimada de las medidas a tomar. v. Características de las posibles fuentes de ataque. vi. Recurso humano necesario para implementar la solución. Este recurso está tanto a nivel técnico como operativo. vii. Implicaciones reputacionales, económicas y legales. viii. Definir y notificar a responsables para llevar a cabo la estrategia de solución Adicionalmente, se deben definir si se requiere o no ejecutar alguna acción desde el componente legal, para lo cual se comunicará al jefe de la oficina de Asuntos Jurídicos, para que se definan la actuación a seguir. Como soporte a esta actividad quedará la definición de la estrategia dentro del formato de acta que se defina.		
8	Implementar solución frente al evento o incidente de seguridad	El especialista responsable que se definió como necesario para la implementación de la estrategia de solución, ejecuta la estrategia definida en la actividad anterior. La evidencia de las acciones ejecutadas debe ser registrada en el sistema de gestión de incidentes En caso de presentarse alguna incidencia relevante en el	Tercero o Especialista de soporte segundo nivel	Caso documentado en el sistema de gestión de incidentes

No	Actividad	Descripción de la Actividad	Responsable	Registro
		momento de estar desarrollándose las actividades definidas, se debe comunicar inmediatamente al grupo que definió la solución para replantear las acciones a seguir.		
9	Reportar a las instancias respectivas	El director de la CSIRT, una vez se inicie la estrategia de solución frente al incidente de seguridad y con el fin de dar cumplimiento al reporte ante instancias respectivas, cuando aplique, realizará la novedad respectiva, conforme con lo definido en la política de notificaciones.	Director CSIRT	Soporte de registros en los canales de reporte instancias respectivas
10	Realizar seguimiento posterior a los incidentes de seguridad	Periódicamente el grupo de trabajo que el director del CSIRT designe analizan los eventos e incidentes que se hayan presentado para: i. Definir esquemas y controles más efectivos con el fin de prevenir y responder ante situaciones que afecten la seguridad de la información dentro de la entidad. ii. Mantener la documentación de los eventos e incidentes de seguridad y privacidad de la Información. iii. Mantener actualizada las bases de datos de conocimientos. iv. Evaluar avances frente a los planes de mejora producto de la materialización de riesgos de Seguridad de la Información. v. Incluir dentro de las capacitaciones que se definan, la sensibilización y lecciones aprendidas relacionas a eventos e incidentes de Seguridad de la Información.	Líder de Seguridad de la Información / director del CSIRT / Coordinadores del CSIRT	Acta de reunión

No	Actividad	Descripción de la Actividad	Responsable	Registro
		Los avances y tareas que se definan dentro de dichas reuniones deberán quedar registradas en un acta de la reunión. FIN DEL PROCEDIMIENTO		

Fuente: El autor

6.5.2 Intercambio de información y comunicación de incidentes

6.5.2.1 Política. EL CSIRT debe dar cumplimiento a las obligaciones de reporte de incidentes de seguridad a las autoridades competentes y a los CSIRT de referencia, en los términos de modo y tiempo que exige la normatividad vigente.

Tabla 13. Autoridades competentes y CSIRT de referencia

Entidad	Contacto	
CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	Correos	ponal.csirt@policia.gov.co
	Página Web	https://cc-csirt.policia.gov.co
	Teléfonos	(+571) 5159090/ 5159586
Equipo de Respuesta a Emergencias Cibernéticas del Gobierno Nacional - CSIRT de gobierno	Correos	csirtgob@mintic.gov.co
	Teléfonos	018000910742 - opción 4
CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	Correos	contacto@colcert.gov.co
	Página Web	http://www.colcert.gov.co/
	Teléfonos	(+571) 295 98 97
Policía Nacional de Colombia	Correos	caivirtual@delitosinformaticos.gov.co
	Página Web	https://caivirtual.policia.gov.co/

Fuente: El autor

La notificación de incidentes es obligatoria para aquellos casos que se encuentren asociados a uno de los niveles de criticidad e impacto establecidos o categorizados como Superior o Alto. También queda incluido en estas notificaciones, cualquier incidente que no tenga este nivel de criticidad, pero que

se identifique un nivel de impacto que haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia.

En ejecución de las actividades de resolución de incidentes, los casos se pueden escalar a los CSIRT de referencia o a los organismos nacionales o internacionales con los cuales se cuente con una relación de afiliación, contractual o de cooperación. En el caso contrario, estas entidades pueden reportar casos conforme al procedimiento de gestión de incidentes.

El director del CSIRT es el responsable de reportar incidentes de seguridad ante las autoridades competentes, CSIRT de referencia y organismos nacionales e internacionales. Dicho director, de acuerdo con la relevancia del evento o incidente de seguridad generado, debe informar a la Dirección General para que, de acuerdo con los protocolos de comunicación definidos se realice una comunicación formal a las instancias que se definan pertinentes.

6.5.2.2 Procedimiento. Este procedimiento inicia con la revisión de los casos que se encuentran registrados en el sistema de gestión de incidentes, continúa con el reporte y entregas de los informes del incidente a las instancias respectivas, reporta los casos al Cliente de los casos que pueden constituir un delito. Finaliza con el seguimiento de las notificaciones hasta que el incidente es cerrado.

Tabla 14. Procedimiento de intercambio de información de incidentes

No	Actividad	Descripción de la Actividad	Responsable	Registro
1	Revisar casos candidatos para notificación	Una vez valorados los niveles de criticidad e impacto de los incidentes, el técnico o especialista revisa los casos abiertos con el fin de determinar si es procedente: • la notificación a las instancias respectivas • sí está presente un posible delito Si es procedente, prepara la información y notifica al director del CSIRT para su notificación o entrega de información.	Técnico de soporte de primer nivel / Especialista de soporte de segundo nivel	Caso documentado en el sistema de gestión de incidentes
2 PC	Reportar a las	El director de la CSIRT, una vez revisado y confirmado el caso	Director CSIRT	Soporte de registros en

No	Actividad	Descripción de la Actividad	Responsable	Registro
	instancias respectivas	para notificación y con el fin de dar cumplimiento al reporte ante instancias respectivas, cuando aplique, realizará la novedad respectiva, conforme con lo definido en la política de notificaciones. ¿El caso es de notificación obligatoria o de prudente notificación? **SI**: Se realiza la novedad respectiva conforme a la política de notificaciones y normatividad vigente y se continua con la siguiente actividad. **NO:** Se marca el caso como no obligatorio para notificación y se continua con la actividad 4.		los canales de reporte instancias respectivas
3	Entregar informes a las instancias respectivas	El director de la CSIRT, una vez se avance en la resolución o cierre del incidente y con el fin de dar cumplimiento al reporte ante instancias respectivas, realizará la entrega de los informes parciales o finales respectivos.	Director CSIRT	Soporte de registros en los canales de reporte instancias respectivas
4 PC	Reportar posible delito	El director de la CSIRT, una vez revisado y confirmado el caso para posible ocurrencia de un delito, notifica la novedad respectiva ¿El caso constituye un delito? **SI**: Se notifica la novedad al Cliente adjuntando las evidencias y se continua con la siguiente actividad. **NO:** Se marca el caso como no constitutivo de delito y se da por finalizado el procedimiento para el caso.	Director CSIRT	Soporte de registros en los canales de reporte con el Cliente
5	Realizar seguimiento a las	El director del CSIRT realiza seguimiento de las notificaciones	Director CSIRT	Caso documenta do en el

No	Actividad	Descripción de la Actividad	Responsable	Registro
	notificaciones del caso	hasta el cierre y elaboración final del caso. FIN DEL PROCEDIMIENTO		sistema de gestión de incidentes

Fuente: El autor

6.5.3 Recolección y custodia de evidencias

6.5.3.1 Política. La gestión de eventos e incidentes debe tener en cuenta las siguientes consideraciones para la recolección de evidencia en el momento en que se detecta un evento o Incidente de Seguridad o Privacidad:

i. Reconstruir la sucesión de los acontecimientos a partir de los hechos sobre los cuales se encuentre evidencia obtenida de mecanismos de auditoría propios de los recursos tecnológicos involucrados.
ii. Los hallazgos deben ser documentados mediante la utilización de imágenes y la copia de archivos que sirvan como evidencia.
iii. Los registros de auditoría de los sistemas de información, sistemas operativos, soluciones por hardware, entre otros deben ser utilizados como insumo para detectar y obtener evidencia de los eventos e incidentes de seguridad, para lo cual es indispensable que se cuente con la fecha y hora de la creación y modificación de los registros.
iv. El registro fotográfico y de vídeo puede llegar a ser útil para obtener evidencia frente a los eventos e incidentes de seguridad relacionados con acceso físico a las instalaciones.
v. Se deben evitar los siguientes errores, que son muy comunes dentro de la recolección de la evidencia a nivel de estaciones de trabajo:
    a. Añadir datos al sistema.
    b. Finalizar o detener la ejecución procesos y servicios del sistema.
    c. Usar herramientas no confiables.
    d. Actualizar el sistema operativo antes de recolectar la evidencia.
    e. Continuar trabajando con el equipo luego de presentarse el incidente.
    f. Apagar el equipo cuando se observa actividad sospechosa, porque esto elimina cualquier rastro del incidente y proporciona pérdida de evidencia digital que puede ser muy relevante y que está almacenada en medios volátiles como la Memoria RAM del componente.

6.5.3.2 Procedimiento. Este procedimiento inicia con la asignación de recursos, para luego identificar, recolectar y examinar las fuentes de información, continua con el análisis de información, para finalizar con la elaboración y socialización

del informe final del incidente. Durante todo el procedimiento se debe garantizar la cadena de custodia.

Tabla 15. Recolección y custodia de evidencias

No	Actividad	Descripción de la Actividad	Responsable	Registro
1	Iniciar la recolección de evidencias	Una vez verificado y confirmado el incidente según el procedimiento de incidentes de Seguridad, el técnico o especialista asignado al caso, inicia la actividad de recolección de evidencias con el motivo principal de ayudar en la resolución del caso.	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel /	Caso documentado en el sistema de gestión de incidentes
2 PC	Determinar la necesidad de realizar un análisis forense	El técnico o especialista de soporte, una vez realizado el análisis preliminar del incidente, determina la necesidad si se requiere de un análisis forense. ¿Se requiere análisis forense? **SI**: Se informa al coordinador del grupo de gestión de incidentes para que proceda con la solicitud de un investigador y se continua con la siguiente actividad. **NO:** Se continua con la actividad 4.	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel	Soporte de registros en los canales de reporte instancias respectivas
3	Solicitar y asignar un analista forense	Mediante correo electrónico, el coordinador del grupo de gestión de incidentes, solicita al coordinador del grupo de investigación la asignación de un analista para realizar labores de recolección de evidencias y/o para realizar un análisis forense. Por este mismo medio, el coordinador del grupo de investigación asigna el respectivo analista o investigador.	Coordinador del grupo de gestión de incidentes / Coordinador del grupo de investigación	Correos electrónicos
4	Alistar la escena del incidente	Los responsables de la recolección de la información deben asegurar el lugar o zona	Técnico de Soporte primer nivel/	Informe inicial del incidente

No	Actividad	Descripción de la Actividad	Responsable	Registro
		de los hechos del incidente, con el fin de evitar alteraciones en las posibles evidencias a recolectar. Dentro de las acciones que se deben realizar antes de la intervención, se encuentran las siguientes: • Toma de fotografías de los equipos o sitio del incidente. • Sin importar el estado del equipo, no prender ni apagar. Si se requiere apagar un equipo, se debe desconectar desde la fuente de energía. • Tomar fotografías de lo visible en el monitor o pantalla del equipo • Sellar los puertos y unidades de los equipos • Capturar información volátil del equipo mediante el uso de herramientas forenses • Asegurar dispositivos y medios físicos de almacenamiento de información • Relacionar los posibles dispositivos de red que tienen interacción con el equipo afectado como firewall, directorio activo, proxy, entre otros.	Especialista de soporte segundo nivel / Investigador	
5	Identificar las fuentes de información	Los responsables de la recolección de información identifican y evalúan de donde se obtendrá la información relevante, para luego proceder con la recolección y examinación de esta. Si la información va a ser usada para fines legales, desde el inicio se debe garantizar la cadena de custodia, llevando un registro de las acciones de recolección, almacenamiento con fecha y	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel / Investigador	Informe actualizado del incidente

No	Actividad	Descripción de la Actividad	Responsable	Registro
		hora y las herramientas que se han utilizado. En el evento de requerirse apoyo externo, se debe solicitar a los organismos competente conforme al procedimiento de notificaciones de incidentes. Las fuentes visibles de información son entre otras servidoras, computadores de escritorio, dispositivos y medios de almacenamiento, celulares, cámaras fotográficas, tabletas. Las fuentes no visibles de información son entre otras los registros de auditoría de cualquier dispositivo en red.		
6	Recolectar y examinar la información	Una vez identificadas las fuentes de información, los responsables de la recolección de información, mediante el uso de técnicas y herramientas forenses extraen la información relevante, sin alterar la integridad de los datos, realizando el registro de las actividades realizadas y de hallazgos encontrados	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel / Investigador	Informe actualizado del incidente
7	Realizar el análisis de la información recolectada	Una vez recolectada y examinada la información, los responsables de la actividad realizan el análisis de la información relevante con el fin de determinar las causas y dar las respuestas para la solución del caso. El análisis comprende la realización de correlación de los eventos mediante el uso de herramientas diseñadas para tal fin.	Técnico de Soporte primer nivel/ Especialista de soporte segundo nivel / Investigador	Informe actualizado del incidente
8	Informar los resultados	Como último paso de este procedimiento se elabora el informe final con los resultados del análisis que debe incluir como mínimo:	Técnico de Soporte primer nivel/ Especialista de soporte	Informe final del incidente

No	Actividad	Descripción de la Actividad	Responsable	Registro
		• Procedimientos que se llevaron a cabo para recolectar y analizar la información • Identificación del ataque realizado • Herramientas utilizadas • Verificaciones pendientes • Cambios realizados • Recomendaciones y acciones de mejoras	segundo nivel / Investigador	

Fuente: El autor

7. CONCLUSIONES

Se observa un aumento en el reporte de los incidentes de seguridad con lo cual se evidencia la materialización del estado de vulnerabilidad en la que se encuentra la población por las acciones delictivas de los ciberdelincuentes. Este aumento se da en primera instancia por el incremento de los ataques informáticos, pasando de una focalización orientada a las empresas hacia una focalización orientada hacia las personas. En segunda instancia, el resultado se presenta por las iniciativas del estado mediante la implementación de centros de respuesta que permitan a las víctimas contar con mecanismos de apoyo y de atención y, por otra parte, los ciudadanos y las empresas son más conscientes sobre la necesidad de informar y denunciar los eventos de seguridad y delitos informáticos. La ocurrencia de muchos de los incidentes puede ser evitada mediante un trabajo coordinado entre entes gubernamentales y privados, adoptando y adecuando la tecnología como medida de prevención y protección ante las nuevas tendencias de la delincuencia.

Como consecuencia se genera la necesidad para que la tecnología forme parte integral de la vida cotidiana de todos, en especial de las personas, quienes son el eslabón más débil en la cadena de seguridad. Sin embargo, como en todo sistema la tecnología no es todo, por lo cual es necesario tomar medidas con el fin de compartir las experiencias relacionadas a los ataques informáticos con las comunidades que tiene la responsabilidad de la defensa de las infraestructuras tecnológicas que se encuentran dentro del territorio nacional e internacional, sin afectar la soberanía de los estados.

La defensa de las infraestructuras tecnológicas se refiere a la función de detectar, recuperar y responder a los ataques y a las medidas de seguridad para garantizar que los sistemas informáticos se encuentran protegidos. La defensa y la seguridad solo es posible mediante el desarrollo e implementación de unas soluciones y herramientas administrativas, técnicas y jurídicas. Una de esas soluciones es la implementación de equipos o centros de respuesta y defensa como son los CSIRT.

8. RECOMENDACIONES

Las siguientes son las recomendaciones que debe tener en cuenta el CSIRT para su mejoramiento a futuro:

Alineación: El proceso de gestión de incidentes se debe alinear con el Modelo de Arquitectura Empresarial que por normativa defina el Gobierno Nacional para la implementación o mejoramiento de un CSIRT.

Integración: La organización debe diseñar los mecanismos de integración para garantizar que el flujo de información relacionada con el reporte, respuesta y notificaciones de incidentes con sus clientes y las autoridades competentes se realice de manera oportuna y sistematizada. Debe prevalecer la integración mediante el uso de sistemas de gestión de incidentes; no obstante, en ausencia de estas herramientas, se considera válido el uso de correo electrónico.

Taxonomía: Para mejorar el intercambio de información y de las comunicaciones, se debe adoptar y mantener actualizada una taxonomía homogénea, o al menos homologable, en cuanto a clasificación y tipificación de los incidentes de seguridad que defina el Gobierno Nacional o el organismo privado delegado por el Estado Colombiano.

Proceso de maduración. La implantación y consolidación del CSIRT es un proyecto a largo plazo, que debe ir madurando y ampliando su estructura en la medida que ofrezca más servicios con un mayor valor agregado para las empresas. Un CSIRT alcanza su nivel máximo de implantación, después de dos años de haber iniciado la operación.

Planeación Estratégica. Dentro del Plan Estratégico de Tecnologías de Información y las Comunicaciones de la organización, se deben planear las acciones, proyectos y la entrada de nuevos servicios que permitan la evolución del CSIRT, sin descuidar los aspectos de financiación y sostenibilidad a largo plazo.

BIBLIOGRAFÍA

ALEGSA www.alegsa.com.ar [En línea] = Diccionario de Infornática Y Tecnología // Diccionario de Infornática Y Tecnología. - 28 de Abril de 2020. - http://www.alegsa.com.ar/Diccionario/diccionario.php.

ALEJO Luis Méndez webempresa [En línea] // Que es el Mail Spoofing y como evitarlo usando SPF. - 25 de 08 de 2014. - 06 de 04 de 2019. - https://www.webempresa.com/blog/que-es-el-mail-spoofing-y-como-evitarlo-usando-spf.html.

ASOBANCARIA La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones = Semana Económica 2018. - Bogotá : [s.n.].

BID, OEA y MINTIC Estudio Impacto de los incidentes de seguridad digital en Colombia 2017.

CAMARA COLOMBIANA DE INFORMATICA Y TELECOMUNICACIONES. CCIT Tanque de Análisis y Creatividad de las TIC // tictac. - Bogotá : [s.n.], 2019.

CARGILL Andrés www.linkedin.com [En línea] = Entendiendo los CSIRT: responsabilidades, roles y diferencias respecto a un SOC y CERT.. - 2019. - 2019. - https://www.linkedin.com/pulse/entendiendo-los-csirt-responsabilidades-roles-y-respecto-cargill-1f/.

COLOMBIA. CONGRESO DE LA REPUBLICA Acto Legislativo 5 // Por el cual se constituye el Sistema General de Regalías, se modifican los artículos 360 y 361 de la Constitución Política y se dictan otras disposiciones sobre el Régimen de Regalías y Compensaciones. - Bogotá : Diario Oficial, 18 de Julio de 2011.

COLOMBIA. CONGRESO DE LA REPUBLICA Ley 1273 de 2009 // deModificación del Código Penal. - Bogotá : Diario oficial, 5 de Enero de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA Ley 1530 [Ley] // Por la cual se regula la organización y el funcionamiento del Sistema General de Regalías. - Bogotá : Diario Oficial, 17 de Mayo de 2012.

COLOMBIA. CONGRESO DE LA REPUBLICA Ley 1712 // Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. - Bogotá : Diario Oficial, 6 de Marzo de 2014.

COLOMBIA. CONGRESO DE LA REPUBLICA Ley 1928. - Bogotá : Diario Oficial, 24 de julio de 2018.

COLOMBIA. CONGRESO DE LA REPUBLICA Ley 527 de 1999 // Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. - Bogotá : Diario Oficial, 21 de Agosto de 1999.

COLOMBIA. CONGRESO DE LA REPUBLICA Ley 594 // Ley General de Archivos. - Bogotá : Diario Oficial, 14 de Julio de 2000.

COLOMBIA. CONGRESO DE LA REPUBLICA Ley Estatuaria 1266 // Habeas Data. - Bogotá : Diario Oficial, 31 de Diciembre de 2008.

COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 1341 Ley 1341 // Principios y conceptos sobre la sociedad de la información y la organización de las TIC. - Bogotá : Diario Oficial, 30 de Julio de 2009.

COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 1581 Ley 1581 de 2012 // Protección de Datos Personales. - Bogotá : Diario Oficial, 17 de Octubre de 2012.

COLOMBIA. FISCALIA GENERAL DE LA NACION Manual de procedimientos para cadena de custodia. - Bogotá : [s.n.].

COLOMBIA. MINISTERIO DE DEFENSA Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia // PNPICCN V 1.0. - Bogotá : [s.n.], 2017.

COLOMBIA. MINISTERIO DE INDISTRIA, COMERCIO Y TURISMO Decreto 1377 de 2013. - Bogotá : [s.n.], 2013.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 10] Seguridad y Privacidad de la Información // Guía para la preparación de las TIC para la continuidad del negocio. - Bogotá : MINTIC, 15 de Diciembre de 2010.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 21] Seguridad y Privacidad de la Información // Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. - Bogotá : MINTIC, 2016.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC Decreto 2573 // Lineamientos generales de la Estrategia de Gobierno en línea y reglamentación parcial de la Ley 1341 de 2009. - Bogotá : Diario Oficial, 12 de Diciembre de 2014.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC Decreto 2693 // Lineamientos generales de la estrategia de Gobierno en línea y reglamentación parcial de las Leyes 1341 de 2009 y 1450 de 2011. - Bogotá : [s.n.], 21 de Diciembre de 2012.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC Estructura de los nodos de innovación. - Bogotá : MINTIC, Junio de 2012.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC Guía No. 13 Evidencia Digital. - Bogotá : MINTIC, 2016.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. MINTIC Modelo de Seguridad y Privacidad de la Información. Guías [En línea]. - 2016. - https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

CONPES 3701 Lineamientos nacionales de política en Ciberseguridad. - 2011.

CONPES 3854 Política de Seguridad Digital. - Bogotá : [s.n.], 2016.

COSTAS S. J Seguridad Informática [Libro]. - [s.l.] : RA-MA, 2014.

DIJIN, INTERPOL Frente de Seguridad Empresarial // Informe. - Bogotá : [s.n.], septiembre de 2019.

ESPAÑA. CONSEJO NACIONAL DE CIBERSEGURIDAD Guía Nacional de Notificación y Gestión de Ciberincidentes. - Madrid : [s.n.], 2019.

ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS MAGERIT 3.0 [Libro]. - Madrid : [s.n.], 2012. - Vols. Libro I - Método : 3.

FIRST Foro sobre los Equipos de Respuesta a Incidentes y Seguridad [En línea]. - 1990. - 10 de mayo de 2020. - https://www.first.org/.

HENK Bronk y Hakkaja Marco Thorbruegge y Mehis Como Crear un CSIRT Paso a paso [Libro] / ed. ENISA. - Atenas : Agencia Europea de la Unión para la CiberSeguridad, 2006. - 5.1 : Vols. CERT-D1 : pág. 90.

HERRERA M. Haroldo E. Metodología para evaluación, diagnóstico y diseño de procesos [En línea]. - 22 de febrero de 2007. - 2020. - https://www.gestiopolis.com/metodologia-para-evaluacion-diagnostico-y-diseno-de-procesos/.

ICONTEC GTC-ISO/IEC 27002 // Tecnología De La Información. Técnicas De Seguridad. Código De Práctica Para Controles De Seguridad De La Información. - [s.l.] : ICONTEC, 22 de Julio de 2015.

ICONTEC NTC-ISO/IEC 27001 // Tecnología de la Información. técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). - Bogotá : INCONTEC, 1 de Diciembre de 2013.

ICONTEC NTC-ISO/IEC 27005 // Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. - Bogotá : ICONTEC, 19 de agosto de 2009.

INTERNATIONAL TELECOMMUNICATION UNION Global Cibersecurity Index – GCI 2018 / ed. Publications ITU. - ISBN 978-92-61-28201-1.

INTERNETYA internetya.co [En línea] // ¿Qué es un ataque de denegación de servicios DDoS?. - 30 de 04 de 2018. - 05 de 04 de 2019. - https://www.internetya.co/ataques-de-denegacion-de-servicio-ddos-un-riesgo-real/.

ISO/IEC 17799 Wordpress.com [En línea]. - 15 de 06 de 2005. - 11 de 02 de 2015. - https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf.

ISO/IEC 27000 Tecnología de la Información. Técnicas de Seguridad // Sistema de Gestión de Seguridad de la Información.

LACNIC Proyecto Amparo. Manual: Gestión de Incidentes de Seguridad Informática [Libro]. - 2010.

MIRANDA Jezreel Mejía, & Ramírez, Heltton Estableciendo controles y perímetro de seguridad para una página web de un CSIRT [Libro] / ed. CIMAT Centro de Investigación en Matemáticas. - [s.l.] : RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação, 2016.

OBSERVATORIO COLOMBIANO DE CIENCIA Y TECNOLOGIA Boletín de análisis de indicadores de ciencia, tecnología e innovación No. 1 // La Eficiencia de la Innovación en Colombia frente al mundo: Un análisis desde el Global Innovation Index, 2016 – 2019. - Bogotá : OCyT, Septiembre de 2019.

OEA Buenas Prácticas para establecer un CSIRT nacional [Libro]. - 2016.

OEA, TREND MICRO Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas [Informe]. - 2015.

OECD Estudios Económicos de la OCDE: Colombia 2019 [Libro]. - París : OECD Publishing, 2019.

OECD SME Ministerial Conference // Promoting innovation in established SMEs. Parallel Session 4. - París : OECD Publishing, 26 de Febrero de 2018.

OECD, EUROSTAT Manual de Oslo // Guía para la Recogida e Interpretación de Datos Sobre la Innovación / ed. Ogallal Juan Zamorano. - [s.l.] : Grupo TRAGSA – Empresa de Transformación Agraria S.A., 2005. - Trecera Edición.

PARRA R.G. Proyecto Legal para un Esquema Nacional de Ciber Seguridad [Libro]. - Lima : Universidad de San Martín de Porres, 2016.

PEREZ Eddy Activos, Ataques, Amenazas y vulnerabilidades [En línea]. - 16 de 04 de 2011. - 2011. - http://es.slideshare.net/jonbonachon/activos-ataques-amenazas-y-vulnerabilidades-de-informacin.

POLICIA NACIONAL DE COLOMBIA Amenazas del Cibercrimen en Colombia 2016-2017 [Informe]. - Bogotá : [s.n.], 2018.

POLICIA NACIONAL DE COLOMBIA Balance del cibercrimen en Colombia 2017 [Informe]. - Bogotá : [s.n.], 2017.

POLICIA NACIONAL DE COLOMBIA, CCIT Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020. - Bogotá : [s.n.], 29 de octubre de 2019.

POLICIA NACIONAL DE COLOMBIA, CCIT Informe Tendencias del Cibercrimen primer trimestre 2020. - Bogotá : CCIT, 2020.

ROLDAN F. S Guía de creación de un CERT/CSIRT. [Libro]. - [s.l.] : Centro Criptológico Nacional, 2011.

SANCHEZ Rubén Seguridad en Redes. - [s.l.] : Universidad Autónoma del Estado de Hidalgo.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD Escenario Dos // Enfoque Directivo - Administrativo. - Bogotá : UNAD, 2019.

Anexo A. Resumen Analítica Especializado – RAE

Fecha de Realización:	17/05/2020
Programa:	Seguridad Informática
Línea de Investigación:	Gestión de sistemas (Área: Ciencias de la Computación)
Título:	Diseño Documental para la Formación de un CSIRT
Autor(es):	Benítez Rodríguez Guillermo
Palabras Claves:	CSIRT, incidentes, nivel de servicio, infraestructuras críticas, seguridad
Descripción:	Este documento corresponde al trabajo de grado para optar al título de Especialista en Seguridad Informática, en la modalidad de proyecto aplicado, el cual tiene como objetivo de realizar el diseño documental para la conformación de un CSIRT para la empresa Cibersecurity de Colombia Limitada, con el fin de ofrecer a sus clientes servicios de respuesta a incidentes y de gestión de vulnerabilidades teniendo presente el nivel de servicio contratado.

Fuentes bibliográficas destacadas:

BID, OEA y MINTIC Estudio Impacto de los incidentes de seguridad digital en Colombia 2017.

COLOMBIA. MINISTERIO DE DEFENSA Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia // PNPICCN V 1.0. - Bogotá: [s.n.], 2017.

ESPAÑA. CONSEJO NACIONAL DE CIBERSEGURIDAD Guía Nacional de Notificación y Gestión de Ciber incidentes. - Madrid: [s.n.], 2019.

FIRST Foro sobre los Equipos de Respuesta a Incidentes y Seguridad [En línea]. - 1990. - 10 de mayo de 2020. - https://www.first.org/.

HENK Bronk y Hakkaja Marco Thorbruegge y Mehis Como Crear un CSIRT Paso a paso [Libro] / ed. ENISA. - Atenas: Agencia Europea de la Unión para la CiberSeguridad, 2006. - 5.1: Vols. CERT-D1.

INTERNATIONAL TELECOMMUNICATION UNION Global Cibersecurity Index – GCI 2018 / ed. Publications ITU. - ISBN 978-92-61-28201-1.

OEA Buenas Prácticas para establecer un CSIRT nacional [Libro]. - 2016. POLICIA NACIONAL DE COLOMBIA, CCIT Informe de las Tendencias del Cibercrimen en Colombia 2019 – 2020. - Bogotá: [s.n.], 29 de octubre de 2019. ROLDAN F. S Guía de creación de un CERT/CSIRT. [Libro]. - [s.l.]: Centro Criptológico Nacional, 2011.	
Contenido del documento:	Este documento consigna el diseño documental para la conformación de un CSIRT para la empresa Cibersecurity de Colombia Limitada destinado al nicho de las pequeñas y medianans empresas, el cual contiene una descripción del panorama actual de la Seguridad Digital en Colombia en los últimos tres (3) años, que contribuyó con la identificación del ámbito de actuación del CSIRT y a la creación de la taxonomía de ataques de este, presenta la estructura del Catálogo de Servicios, el cual comprende los diferentes tipos de servicios proactivos y reactivos que prestará el CSIRT, señala las funciones de los perfiles del equipo de trabajo, conforme a la estructura orgánica propuesta para la creación del CSIRT y finaliza con un Manual con las Políticas y Procedimientos Operacionales, en cuanto a gestión de incidentes, gestión de notificaciones, recolección y custodia de evidencias
Marco Metodológico:	Para el desarrollo del presente proyecto se utilizó la metodología para evaluación, diagnóstico y diseño de procesos[74], la cual comprende cuatro (4) etapas: i) Conocimiento, donde se identifican y consultan las fuentes documentales, ii) Interpretación, donde se identifica y clasifica la información consultada para facilitar el análisis y transformación de esta, iii) Análisis, donde se verifica, cuestiona y se revisa la aplicabilidad de la información recolectada y de los diseños implementados en otros CSIRT y iv) Diseño, donde se define el gobierno, organización, políticas y procedimientos del CSIRT.
Conceptos adquiridos:	El desarrollo de este trabajo aportó de manera significativamente en conocimientos para gestión de incidentes de seguridad que permitan dar respuesta

[74] HERRERA M. Haroldo E. Metodología para evaluación, diagnóstico y diseño de procesos [En línea]. - 22 de febrero de 2007. - 2020. - https://www.gestiopolis.com/metodologia-para-evaluacion-diagnostico-y-diseno-de-procesos/.

	a los eventos de ataques informáticos, teniendo como elementos fundamentales la cooperación nacional e internacional y la comunicación oportuna a la comunidad de las situaciones presentadas con el fin de generar un ambiente seguro y confiable entre todos los actores de un CSIRT. También contribuyó en dar pautas sobre la importancia de recolectar y custodiar las evidencias forenses, con el fin primordial de dar solución a incidentes y de paso habilitar a los gestores del CSIRT para tomar las medidas administrativas y jurídicas contra los posibles agresores o delincuentes.
Conclusiones:	Con los aportes consignados en este documento, se contribuye con la política de seguridad del gobierno colombiano, en el ámbito de creación de un CSIRT con la finalidad de que pequeñas y medianas empresas cuenten con mecanismos y servicios de apoyo disponibles en el mercado para dar respuestas a incidentes de seguridad informática