DISEÑO DOCUMENTAL PARA EL FUNCIONAMIENTO DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA.

HERMES MUÑOZ CARVAJAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEDE JOSÉ ACEVEDO Y GÓMEZ
BOGOTÁ D.C
2023

DISEÑO DOCUMENTAL PARA EL FUNCIONAMIENTO DEL CSIRT EN CIBERSECURITY DE COLOMBIA LTDA.

HERMES MUÑOZ CARVAJAL

PROYECTO APLICADO DISEÑO DOCUMENTAL CSIRT
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA

INGENIERO HERNANDO JOSÉ PEÑA HIDALGO
DIRECTOR DE CURSO

INGENIERA YOLIMA MERCADO
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEDE JOSÉ ACEVEDO Y GÓMEZ
BOGOTÁ D.C
2023

NOTA DE ACEPTACIÓN:

_____
_____
_____
_____
_____

_____
Nombre director, orientador, asesor

_____
Jurado

_____
Jurado

Bogotá D.C., julio 2023

DEDICATORIA

Dedico este trabajo (proyecto aplicado), a mis padres, esposa e hijos, quienes, con su apoyo y acompañamiento, me han fortalecido anímicamente para lograr su consecución.

AGRADECIMIENTOS

En primera instancia quiero agradecer a DIOS, por brindarme una bendición más en mi vida, gracias a mis tutores quienes con su acompañamiento y asesoría me enriquecieron profesionalmente y por último agradezco a mi familia, por su incondicional compañía, siendo fuente de inspiración.

RESUMEN

En la actualidad los datos, la información y los recursos informáticos se han convertido en los principales activos de las empresas pues estos respaldan el core del negocio y otorgan estabilidad a las organizaciones. En razón a ello, es cada vez más apremiante asegurar la integridad, confidencialidad y disponibilidad de dichos activos, protegiéndolos de los diferentes ataques informáticos de que pueden ser objeto.

La empresa Cibersecurity de Colombia LTDA, consciente de dicha problemática y con el propósito de hacerle frente, ha propuesto la creación del Centro de Respuesta a Incidentes Cibernéticos en el ámbito CSIRT, el cual, además de responder y solucionar las necesidades de sus clientes, presenta como componente adicional la implementación de un laboratorio de informática forense en el que se aplicará toda la experiencia adquirida en materia de seguridad y protección de la información.

Teniendo claro que un CSIRT, se compone de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información, proporcionando servicios de respuesta ante incidentes a víctimas de ataques en la red, alertas relativas a amenazas y vulnerabilidades, ofreciendo información que ayude a mejorar la seguridad de estos sistemas; Cibersecurity de Colombia LTDA mediante el presente proyecto, plantea la creación del diseño documental como la hoja de ruta para la creación del Centro de Respuestas a Incidentes Cibernéticos, en donde se proyectarán todos y cada uno de los componentes normativos, legales, técnicos y estándares requeridos para la elaboración de este diseño, que permitan a la empresa consolidarse como Centro de Respuesta ante Incidentes Cibernéticos en el ámbito CSIRT.

PALABRAS CLAVE: CSIRT, Ciberseguridad, Incidentes de Seguridad, Confidencialidad, información.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

La era digital ha representado una transformación sin precedentes en el entorno global, proceso que a su vez se ha desarrollado de manera exponencial en el sentido que una nueva innovación tecnológica precede siempre el desarrollo de múltiples avances cada vez más ingeniosos y sorprendentes. Dicha expansión tecnológica ha permitido que aspectos propios de la cotidianidad como las comunicaciones, la educación, las relaciones comerciales sean cada vez más fáciles y accesibles. No obstante, ello también implica el surgimiento de nuevos riesgos relacionados con la confidencialidad y protección de los datos y la información tanto en el plano personal como en el empresarial.

Aunque no se puede negar que Colombia ha presentado importantes avances en materia de seguridad digital, que incluso se han materializado en documentos de política pública como el CONPES 3701[1], CONPES 3854[2] y CONPES 3995[3] en los cuales se han indicado los parámetros, criterios y estándares que deben tenerse en cuenta en el sector público y privado para contrarrestar el riesgo informático que acarrea la cuarta revolución industrial (4RI), no cabe duda que es necesario aumentar los esfuerzos orientados a mitigar el impacto de la cibercriminalidad.

Y es que, en efecto, los actores criminales, que tienen como campo de acción el contexto digital, no se detienen, todo lo contrario, amplían constantemente su radio de acción. Así lo evidencian recientes cifras presentadas por Bautista[4] quién citando a la Fiscalía General de la Nación y a la Dirección de Investigación Criminal, indica que el ciberdelito es la tipología criminal que ha presentado un mayor incremento en Colombia en los últimos años pues ha alcanzado repuntes de hasta el 107% acumulado entre 2019 y 2021, siendo la violación de datos personales y el acceso abusivo a sistemas informáticos las modalidades de mayor incremento, pues para el 2021 registraron una variación porcentual positiva del 45% y el 18% respectivamente.

En ese orden de ideas con la realización del presente trabajo, se pretende trazar una hoja de ruta para la implementación del diseño documental para el funcionamiento del CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informáticas) en la empresa Cibersecurity de Colombia LTDA, con el fin de ofrecer este nuevo servicio y así contribuir a satisfacer las necesidades de sus clientes, convirtiéndose a la vez en un aliado de las entidades gubernamentales y privadas

[1] Lineamientos de Política Pública para Ciberseguridad y Ciberdefensa.
[2] Política Nacional de Seguridad Digital
[3] Política Nacional de Confianza y Seguridad Digital
[4] BAUTISTA GARCÍA, Fredy. Comportamiento del ciberdelito en Colombia durante el 2021. En CCIT, Cibercrimen 2021-2022. Nuevas amenazas al comercio electrónico. Bogotá: Crowdstrike – Fortinet. 2021. PP. 15-24.

que cuentan con un CSIRT, cooperando activamente para hacer del ciberespacio un lugar más seguro.

1. DESCRIPCIÓN DEL PROBLEMA

En cualquier empresa independiente de su Core de negocio o el sector en donde se desenvuelva, después de sufrir un ciberataque se enfrentan a un tedioso proceso de recuperación y restablecimiento de sus operaciones, es ahí en ese escenario, en donde en muchos casos estas organizaciones conciben la importancia de priorizar sus estrategias internas para contrarrestar y mitigar el impacto que ello implica.

Los ciberdelincuentes día a día cambian sus técnicas y formas de ataque en busca de alcanzar sus objetivos delictivos; por esta razón es imperativo que las empresas u organización protejan su información y sus principales activos de tal manera que se garantice en todo momento la continuidad del negocio.

Cibersecurity de Colombia LTDA, empresa dedicada a prestar servicios de seguridad para la protección de los datos y la información, encuentra imprescindible trabajar de la mano con sus clientes y garantizar la confidencialidad, integridad y disponibilidad de su información. Para mejorar sus procesos y estar a la altura de esa responsabilidad con sus clientes Cibersecurity de Colombia LTDA mediante la creación de un Centro de Respuesta a Incidentes Cibernéticos de la mano de un laboratorio de informática forense pretende innovar, mejorar y conocer de una manera más profunda cómo operan los ciberdelincuentes, las nuevas técnicas y herramientas a las que recurren, todo ello con el objetivo primordial de prevenir, identificar, mitigar y saber qué hacer frete a un escenario de ciberataque.

1.1. PLANTEAMIENTO DEL PROBLEMA

¿Cuáles son los componentes normativos, legales, técnicos y estándares requeridos para la elaboración del diseño documental que permitan la creación y puesta en marcha de un Centro de Respuesta ante Incidentes Cibernéticos en el ámbito CSIRT, al interior de la empresa Cibersecurity de Colombia LTDA?

2. JUSTIFICACIÓN

La seguridad de los datos y la información se ha convertido en uno de los principales activos de la empresa moderna, razón por la cual el desarrollo de herramientas idóneas se convierte en una necesidad de primer orden en la actualidad, requerimiento que es más apremiante en un contexto como el Colombiano en el que los ciberdelitos se incrementan día tras día.

Esta realidad justifica el desarrollo de iniciativas como la de Cibersecurity de Colombia LTDA, empresa dedicada a prestar servicios de seguridad para la protección de los datos y la información de sus clientes de conformidad con los parámetros legales que se han delimitado para ello y a partir del desarrollo de prácticas y perímetros de seguridad que generen confiabilidad en cada uno de los procesos o servicios que se ofrecen, para lo cual se tiene presupuestado la ampliación de sus capacidades mediante la creación de un Centro de Respuesta a Incidentes Cibernéticos.

La creación de dicho centro encuentra justificación en las necesidades de los clientes de la empresa que continuamente han expresado su preocupación por el incremento de los incidentes de seguridad y ciberataques dirigidos por medio de técnicas como el rootkit[5], troyanos[6], denegación de servicio o DDoS[7], spam, phishing, virus, gusanos, adware[8], entre otros[9], escenarios que obligan a personas y a empresas a acceder a mecanismos de protección idóneos y especializados, es decir, contar con el respaldo de un aliado que se encargue de preservar la seguridad de sus sistemas y responder en tiempo real a las amenazas, riesgos e incidentes que se presenten en el ecosistema digital.

Cibersecurity de Colombia LTDA busca atender dicha necesidad y a la vez obtener la confianza de sus clientes, gracias a la implementación del Laboratorio de Informática Forense encargado de adquirir, investigar y analizar las evidencias digitales gracias a sus equipos de última tecnología y software especializado en la identificación temprana de los diferentes riesgos informáticos.

En ese orden de ideas, resulta evidente que la necesidad de crear un CSIRT por medio del cual se logren soluciones y respuestas, no solo eficaces sino eficientes, a los riesgos anteriormente mencionados y a los demás que se presenten en las redes informáticas utilizadas por los clientes, razón por la cual el objetivo principal de Cibersecurity de Colombia LTDA para el año 2023 será el de consolidarse como

---

[5] Software que otorga permisos de acceso a ciberdelincuentes. Se caracterizan por ser difíciles de detectar gracias a que cuentan con amplia capacidad para encubrir o enmascarar la intromisión.
[6] Virus que se mimetiza o camufla aparentando ser una aplicación legítima abriendo un backdoor (puerta trasera) que otorga permisos para acceder al sistema.
[7] Ataques por medio de los cuales se busca colapsar el servicio o generar un bloqueo en el sistema, generalmente mediante el lanzamiento simultaneo de peticiones de conexión.
[8] Software de naturaliza publicitaria que genera ventanas emergentes con contenido comercial.
[9] Recuperado el 12 de diciembre de 2022 de https://www.grupoica.com/blog/-/blogs/9-tipos-ciberataque-debes-conocer

uno de los mejores centros de respuesta a incidentes cibernéticos en el ámbito de los CSIRT.

El primer paso para lograr dicho cometido será la elaboración del diseño documental para la creación de un CSIRT, teniendo en cuenta que este se estructura en un equipo, con la capacidad de ofrecer servicios y soporte a un grupo determinado de clientes para prevenir, gestionar y responder a los incidentes de seguridad de la información que puedan surgir; con un componente multidisciplinario de expertos para la gestión de todos aquellos procesos que con anterioridad se han definido, lo que a su vez implica disponer herramientas y medios que se requieran para su implementación. Desde luego, ésta debe llevarse a cabo de manera centralizada y ocuparse de todos aquellos riesgos posibles que puedan impactar los sistemas de los clientes, siendo importante que estos últimos reciban una respuesta oportuna y eficaz ante dichas eventualidades.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar el diseño documental para el funcionamiento del CSIRT en la empresa Cibersecurity de Colombia LTDA.

3.2. OBJETIVOS ESPECÍFICOS

- Analizar el marco normativo y legal en Colombia y a nivel internacional, en donde se establezcan los parámetros que reglamentan la creación de un CSIRT.

- Examinar los estándares y las buenas prácticas implementadas por las Organizaciones Internacionales de Normalización, en donde se regula la estructura y requerimientos de un CSIRT y que contribuyan a consolidar su esquema documental.

- Analizar y comparar los requerimientos documentales implementados en la creación de un centro de respuesta a incidentes informáticos (CSIRT), a nivel nacional e internacional, que sirvan como referente para el diseño documental del CSIRT en la empresa Cibersecurity de Colombia LTDA.

- Examinar los estándares internacionales, en donde se establezca la estructura y requerimientos para la creación e implementación de un laboratorio de informática Forense.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

El surgimiento de cualquier contexto social implica la aparición de conductas criminales que alteran la convivencia y la seguridad, razón por la cual Fernández[10] expone que el delito se considera en sí mismo un hecho social y a la vez un reflejo de las creencias, valores y recursos que establece una sociedad para su pervivencia, lo que convierte al delito en una manifestación de la fractura social y moral.

El entorno digital es también una expresión de sociedad, razón por la cual no es extraño que surjan en sus diferentes infraestructuras conductas criminales. En efecto, una vez se estableció el primer espacio de interacción virtual actual se empezaron a presentar manifestaciones que afectaban su seguridad. Así ocurrió con ARPANET[11] que fue atacada en el año de 1988 por el gusano «Morris8» creado por el estudiante de la Universidad de Harvard Robert Tappan Morris quien logró afectar el 10% de los sistemas conectados a la mencionada red precursora del internet actual, siendo este el primer antecedente de ataque a una infraestructura TIC[12].

Utilizando como medio de reproducción un defecto que tenía el sistema operativo Unix, el mencionado gusano logró infectar decenas de miles de ordenadores que automáticamente quedaron fueron de la red, hecho que ocasionó pérdidas cercanas a los quince millones de dólares durante las 72 horas que tardaron los investigadores para detectarlo. Aunque el incidente dio lugar a que en su momento se solicitaran severos castigos contra Morris, se considera que a él se le debe el inicio de la industria de la ciberseguridad; de hecho, en la actualidad Robert es un reputado profesor de informática[13].

Efectivamente, dicho suceso dio lugar a que la *Defense Advanced Research Proyects Agency* (DARPA9) reconociera la necesidad de contrarrestar de manera organizada y estructurada los riesgos en materia de seguridad informática, razón por la cual el mencionado ente patrocinó el primer equipo para responder a estos incidentes, el cual en su momento fue denominado como *Coordination Center CERT/CC10*, que se instaló en el complejo de la Universidad Carnegie Mellon de Pittsburgh (Pensilvania)[14].

---

[10] FERNÁNDEZ RIQUELME, Sergio. El delito como identidad social. Reflexiones sobre la comunidad y su proceso de integración. En Revista La Razón Histórica, número 35, 2017. p.4

[11] Así se denominó a la red de computadoras que se creó por solicitud del Departamento de Defensa Estadounidense y que se utilizó inicialmente como vía de comunicación entre varias dependencias académicas y gubernamentales. El éxito del proyecto fue tal que

[12] Cibernews en Español. Quien fue el primer hacker de la historia. 2022. Recuperado el 14 de diciembre de 2022 de https://www.youtube.com/shorts/96zYW4lk2Fs

[13] Ibid.

[14] CARNEGIE MELLON UNIVERSITY. Authorized Users of CERT, 2014. Recuperado el 14 de diciembre de 2022 de https://resources.sei.cmu.edu/asset_files/Brochure/2014_015_001_310282.pdf

Estas mismas siglas fueron utilizadas por otras instituciones de educación superior estadounidenses para denominar sus respectivos equipos encargados de estudiar la seguridad de las redes y ordenadores, proporcionar servicios de respuesta ante incidentes y ataques informáticos, publicar alertas relativas a amenazas y vulnerabilidades y ofrecer información que ayudara a mejorar la seguridad de estos sistemas. Complementariamente se empezó a utilizar el concepto de CSIRT que generó valor agregado a los CERT mediante diferentes servicios preventivos y de gestión para ordenadores y redes informáticas[15].

Posteriormente, en los albores de la década de los 90, dichos avances fueron implementados en Europa dónde se contó con el apoyo del programa técnico TERENA que permitió la creación de los CERT, programa que continúa en operación al punto que es el principal foro continental de colaboración, innovación y compartimentación de información orientada a garantizar la seguridad de las infraestructuras de la información y las telecomunicaciones, actividades que hoy por hoy se han fortalecido gracias a que el programa ha implementado un *task forcé* gracias al cual se promueve la cooperación continua entre los diferente4s CSIRT ubicados en la Unión Europea[16].

Actualmente estos programas son liderados en el contexto gubernamental europeo por el CERT-EU cuya función principal es la de contribuir para que la infraestructura TIC de las agencias, órganos e instituciones de la Unión Europea sea más segura gracias a la oportuna atención de las amenazas, incidentes y vulnerabilidades que se contrarrestan gracias a las medidas de protección y de corrección técnica que dicho ente realiza[17]. Es importante acotar que dado que la marca CERT se encuentra registrada, es normal que los programas que cumplen funciones análogas se registren bajo otros acrónimos entre los cuales se destacan los siguientes:

- IRT (Incident Response Team, Equipo de Respuesta a Incidentes)
- CIRT (Computer Incident Response Team, Equipo de Respuesta a Incidentes Informáticos)
- CIRC (Computer Incident Response Capability, Capacidad de Respuesta a Incidentes Informáticos)
- SERT (Security Emergency Response Team, Equipo de Respuesta a Emergencias de Seguridad)

[15] Ibid.
[16] CCN-CERT. Red CERT, garantía de seguridad en todo el mundo. En Revista Auditoría y seguridad. 2007. Recuperado el 14 de diciembre de 2022 de https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/658-red-cert-garantia-de-seguridad-en-todo-el-mundo/file.html
[17] Recuperado el 14 de diciembre de 2022 de https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_es

- ERI (Equipo de Respuesta a Incidentes)
- CSIRT Computer Security Incident Response Team
- CERT Computer Emergency Response Team
- CSIRC Computer Security Incident Response Capability
- IRC Incident Response Center o Incident Response Capability
- SSIRT System Security Incident Response Team
- SIRT Security Incident Response Team
- IHT Incident Handling Team
- CERC Cyber or Computer Emergency Response Capability
- SIRC Security Incident Response Capability
- SERC Security Emergency Response Capability
- ERT Emergency Response Team (Uribe, 2014)[18]

Tomando como referencia los parámetros utilizados en España para la creación de un CSIRT relacionados por el mismo autor consultado, se colige que dicha doctrina es un referente idóneo para el diseño documental del CSIRT que implementará la empresa Cibersecurity de Colombia LTDA. En efecto, dentro de los distintos factores que permitirían el éxito de dicha iniciativa se encuentran la proporcionalidad de los recursos con los que se dote el programa frente a las expectativas de demanda que genere, al igual que en cualquier otro servicio.

El Centro Criptológico Nacional de España, diseñó una guía borrador para la creación de un CSIRT y en ella se expusieron una serie de parámetros que deben tenerse en cuenta al momento de diseñar este tipo de herramientas, entre los cuales se encuentra la categorización de los clientes, el grado de autoridad que se pueda tener sobre los mismos, los servicios a ofertar, una proyección de crecimiento e incluso un plan estratégico. Dichos parámetros y las implicaciones de estos se relacionan en la siguiente tabla:

[18] URIBE RAYAS, Edgar Felipe. Proceso para la definición de servicios iniciales en un equipo de respuesta ante incidencias de seguridad informática (CSIRT) Tesis de grado. 2014. Recuperado el 14 de diciembre de 2022 de https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/437/1/ZACTE42.pdf

Tabla 1. Parámetros para el diseño documental del CSIRT

Clientes destinatarios del servicio	A mayor número de clientes se generarán más peticiones de asistencia en gestión de incidentes y afines como el análisis de evidencia digital en laboratorios de informática forense.
Grado de autoridad sobre los clientes	Si se solicitarán los servicios por propia iniciativa o por imperativo legal, lo que condiciona en este último caso la existencia probable de un mayor volumen de incidentes a gestionar.
Servicios ofrecidos y nivel del servicio	Ofrecer servicio de manera permanente 24 horas al día durante todo el año requerirá un incremento del talento humano y los recursos técnicos disponibles. Del mismo modo se debe considerar los términos del servicio y tiempos de respuesta acordados.[19]
Promoción y comunicación de servicios	El nivel de conocimiento de los clientes acerca de los servicios que se ofrecen implica que la dotación del CSIRT debe progresar a medida que aumenta su impacto, especialmente en los servicios prestados por el laboratorio de Informática Forense.
Proceso de crecimiento	El desarrollo del CSIRT constituye un proyecto a largo plazo razón por la cual debe escalar y ampliarse progresivamente a medida que incrementa la confianza de los clientes y se logra posicionamiento en el mercado.
Plan estratégico	La planificación de la evolución del CSIRT debe tener en cuenta aspectos como su

[19] A manera de ejemplo, la modalidad "best effort" en los que existe compromiso de cumplir peticiones incluso cuando no existe una obligación formal o "next business day" en la que las peticiones se atienden en el siguiente día hábil.

	financiación y sostenibilidad en el mediano y largo plazo. Para ello se debe contemplar la posibilidad de la progresiva implementación de nuevos servicios y los recursos que se requieren para su implementación, promoción y operación.

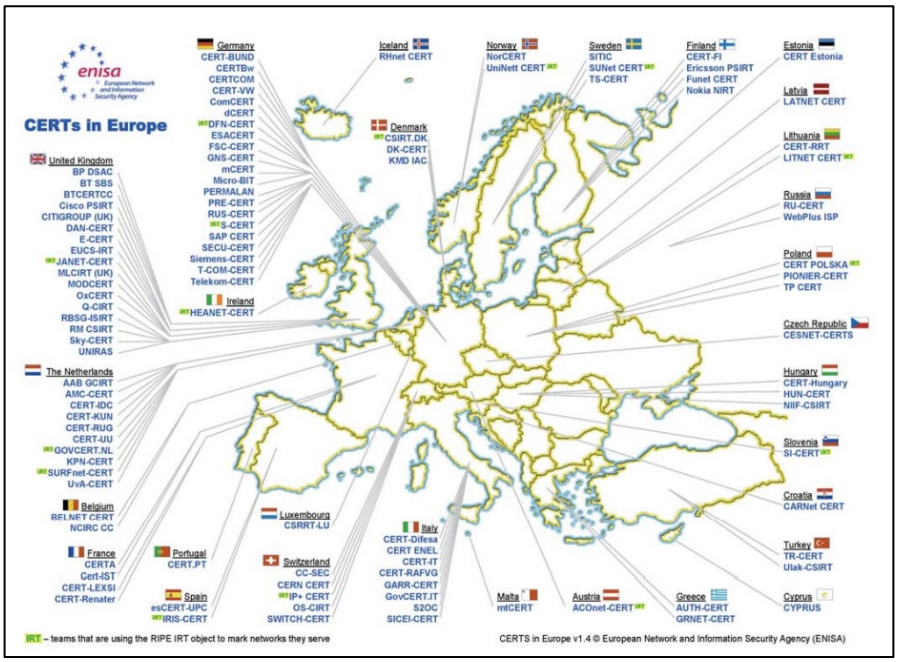
Fuente. Elaboración propia con base en el texto de CCN-CERT[20]

A su vez, la guía consultada indica que en la mayoría de los países de la Unión Europea se cuenta con Equipos de Respuesta a Incidentes de Seguridad. Actualmente se trata de una compleja y amplia red que opera a lo largo y ancho del viejo continente incluyendo países de la Unión e incluso otros que no se encuentran adscrita a la misma pero que coinciden en su interés de salvaguardar la seguridad de la información y los datos informáticos.

Se trata de una intrincada red presente en todo el continente europeo, que tiene un mayor nivel de complejidad en países como Alemania, Reino Unido y Países Bajos según se puede evidenciar en el siguiente mapa recuperado de la mencionada fuente en el que se expone la manera como se han dispuesto los CERT en dicho continente:

[20] Recuperado el 11 de noviembre de 2022 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

Figura 1. Ubicación actual CERT en el continente Europeo



Fuente: https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/658-red-cert-garantia-de-seguridad-en-todo-el-mundo/file.html

Colombia tuvo un importante avance en materia de lucha contra las amenazas informáticas en 2011, año en el que se elevó este tema a la categoría de política pública mediante la expedición del CONPES 3701 «Lineamientos de Política para Ciberseguridad y Ciberdefensa». Dicho documento reconoció, por un lado, la vulnerabilidad que tenía el país en la materia e incluso se apoyó en experiencias internacionales[21] y por otro, el incremento significativo del uso de las tecnologías de la información y las comunicaciones en el país evidenciado en cifras como que tan solo entre 2005 y 2009 aumentaron en un 354% la cantidad de usuarios de internet[22].

Con base en ello, el Documento CONPES 3701 estableció la búsqueda del fortalecimiento de la capacidad estatal para enfrentar las amenazas en materia de seguridad y defensa en el ámbito cibernético como el objetivo de fondo de la política

[21] El CONPES 3701 tomó como ejemplo el ataque cibernético del que fue objeto en abril de 2007 el gobierno de Estonia, su parlamento, ministerios, partidos políticos e incluso dos de sus más representativas entidades financieras. Del mismo modo, el ataque ocurrido en julio de 2009 en contra de la Casa Blanca, el Departamento de Defensa, la Comisión Federal de Comercia y otras importantes dependencias del gobierno estadounidense. También se tuvo en cuenta el desmantelamiento de la red de computadores Zombies BotNet por parte de la Guardia Civil Española, procedimiento en el que se determinó que más de 13 millones de direcciones IP se encontraban infectadas a nivel mundial, siendo Colombia el quinto país más afectado por dicha red criminal.

[22] DNP. Documento CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa. 2011, Recuperado el 2 de diciembre de 2022 de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

pública, propósito para el cual se determinaron tres objetivos específicos, a saber, (i) la implementación de instancias encargadas de prevenir, atender, controlar y generar recomendaciones orientadas a regular emergencias o incidentes cibernéticos a nivel nacional; (ii) diseñar y poner en marcha planes de capacitación en la materia y (iii) robustecer la normatividad y reglamentación en estas materias[23].

Dentro de dichas estrategias se dispuso el establecimiento del Grupo de Respuestas a Emergencias Cibernéticas de Colombia (COLCERT) que en adelante estaría a cargo de la coordinación nacional de todo lo relacionado con la ciberdefensa y la ciberseguridad, brindando apoyo y colaboración a otras instancias, también del orden nacional como el CCP (Centro Cibernético Policial) y el CCOC (Comando Conjunto Cibernético), todo ello bajo el liderazgo de la Comisión Intersectorial que en adelante estaría liderada por el Presidente de la República y conformada por funcionarios de alto nivel como los ministros de Defensa y el de Tecnologías de la Información y las Comunicaciones, así como por los Directores del Departamento Administrativo de Seguridad y de Planeación Nacional[24]. En la siguiente figura se expone el despliegue de dicho modelo relacional:

Figura 2. Modelo Relacional colCERT delimitado en el CONPES 3701 de 2011

Fuente: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

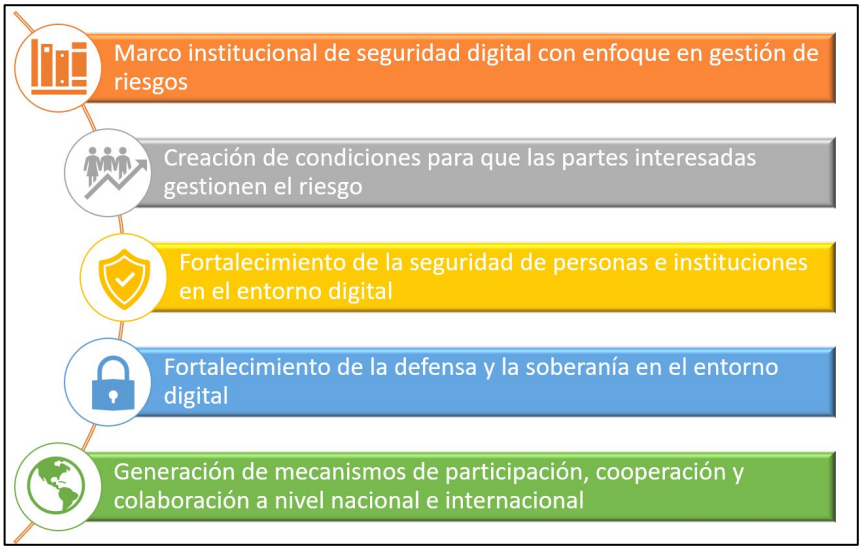
Cinco años después se presentó una nueva política pública sobre seguridad informática en el país. Se trató del Documento CONPES 3854 «Política Nacional de Seguridad Digital» en el que se reconoció que la política de ciberseguridad y ciberdefensa venía generando buenos resultados llegando incluso a posicionar al

[23] Ibid.
[24] Ibid.

país como un líder continental en la materia, no se contaba con criterios claros en materia de gestión de vulnerabilidades en el ecosistema digital, tema en el que se concentró este nuevo documento mediante (i) delimitación del marco institucional sobre seguridad digital, (ii) implementación de medidas para generar ambientes en los que los clientes o interesados contrarresten las vulnerabilidades digitales en cada uno de sus establecimientos o actividades, (iii) fortalecimiento de la defensa y seguridad digital de la nación que trascienda a lo internacional en materia de gestión de riesgos, y (iv) la generación de mecanismos de carácter permanentes orientados a impulsar la colaboración, cooperación y asistencia en seguridad digital[25].

El apartado diagnóstico de este CONPES identificó factores en los que se encontraba rezagado el Estado colombiano en materia de seguridad informática tales como la ausencia de una visión estratégica orientada a la gestión de los riesgos presentes en el ámbito virtual, dificultades para que las partes interesadas (sector público y privado) maximizaran sus oportunidades socioeconómicas en el escenario digital, insuficientes esfuerzos de colaboración cooperación y asistencia (nacional e internacional) en materia de seguridad digital[26] En razón a ello se formuló un plan de acción a partir de cinco lineamientos de política según se describe en la siguiente figura:

Figura 3. Plan de acción Política Nacional de Seguridad Digital



Fuente: Elaboración propia con base en el contenido del CONPES 3854

Por supuesto no se trataba de productos terminados, menos aún si se tiene en cuenta que la tecnología no cesa en su proceso de expansión e innovación, paralelo a lo cual se diversifican y se incrementan de manera continua los riesgos del entorno

[25] DNP, Documento CONPES 3854 Política Nacional de Seguridad Digital, recuperado el 3 de diciembre de 2020 de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
[26] Ibid.

digital. Así lo entendió el Gobierno Nacional y en razón a dicha comprensión emitió el Documento CONPES 3995 «Política Nacional de Confianza y Seguridad Digital» cuyo objetivo fue precisamente el de determinar medidas por medio de las cuales se logrará ampliar la confianza requeridas para una mayor inclusión y competitividad a partir del fortalecimiento de la seguridad digital en el país[27].

El mencionado documento hizo hincapié en las debilidades que afectaban a los ciudadanos, al sector público e incluso al sector privado en materia de seguridad digital; así mismo, al hecho de que a 2020 no se había alcanzado un marco de gobernanza adecuado en la materia y que por el contrario resultaba necesario que se adoptaran estándares, modelos e incluso marcos de trabajo que ampliaran la seguridad digital actualizándolos a las nuevas tecnologías[28].

En resumen, puede señalarse que la evolución de la política pública en materia digital se originó en el reconocimiento de una nueva realidad en la que las herramientas informáticas abarcaban nuevos espacios en la cotidianidad y ello implicaba el incremento de riesgos, los cuales, debían ser debidamente gestionados tanto en el sector público y privado pero además en un escenario de cooperación internacional siendo este un segundo momento de definición de política que culminó (sin decir con ello que ha terminado), con el reconocimiento de dar continuidad a la evolución de las estrategias de defensa de tal manera que estas marcharan a la par de los nuevos avances tecnológicos.

Retomando lo relacionado con los CSIRT, es importante indicar que estos se han definido como una entidad o equipo integrado por especialistas de varias disciplinas, que se encarga de ofrecer servicios y soporte en materia de prevención, gestión y respuesta, rápida y efectiva, a incidentes de seguridad de la información, pero a la vez para contribuir a la mitigación de todos aquellos riesgos que se generan ante la permanente posibilidad de que las redes de comunicación se vean afectadas por ataques cibernéticos[29].

Posteriormente, según lo explica la misma fuente, el concepto evolucionó incrementando los servicios que ofrecían a la comunidad, con lo cual se pasó de atender ataques e incidentes básicos a realizar un proceso de seguimiento más complejo para identificar y contrarrestar el accionar de actores cibernéticos más complejos, razón por la cual en la actualidad los CSIRT incluyen servicios como el análisis forense y la gestión de las nuevas vulnerabilidades que afectan las redes informáticas y de comunicación, para lo cual se desarrollan alertas, sistemas de

[27] DNP. Documento CONPES 3995 Política Nacional de Confianza y Seguridad Digital. Recuperado el 3 de diciembre de 2020 de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf
[28] Ibid.
[29] OEA. Buenas prácticas para establecer un CSIRT nacional, 2016. Recuperado el 9 de diciembre de 2022 de https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

monitoreo, mecanismos de difusión y compartimentación de la información y presentación continua de documentos sobre buenas prácticas[30].

El documento consultado también explica que son centenares los CSIRT que existen a nivel mundial, a la vez que son múltiples sus misionalidades y alcances, razón por la cual no existe una única clasificación, no obstante una manera de realizar dicho ejercicio consiste en agruparlos de acuerdo al sector en el que prestan sus servicios en virtud de lo cual los principales ámbitos son los académicos, las infraestructuras críticas, comercio, gobiernos, militares, pequeñas y medianas empresas, comercio entre otros.

4.2. MARCO CONCEPTUAL

A continuación, se presentan una serie de conceptos asociados a la seguridad informática, los datos y la información que se consideran relevantes para tener una mayor comprensión de la temática planteada.

Seguridad Informática: Garantiza que se preserven los tres valores esenciales de la información que se transmite, procesa y almacena a través de medios computacionales, a saber: (i) su alta confidencialidad, (ii) su permanente disponibilidad y, (iii) su elevada integridad. Vale la pena mencionar el significado de dichos activos esenciales de la seguridad en el contexto informático:

Integridad: Implica mantener la consistencia, precisión y fiabilidad de los datos durante todo su ciclo de vida en el sistema informático, permitiendo que el contenido de estos sea el mismo que se estableció al momento de su creación.

Confidencialidad: Implica que solo la información esté disponible o sea mostrada únicamente a las personas, entidades y procesos autorizados, garantizando que la misma no sea conocida por terceros con independencia de los propósitos que estos llegasen a tener al momento de querer acceder a la misma.

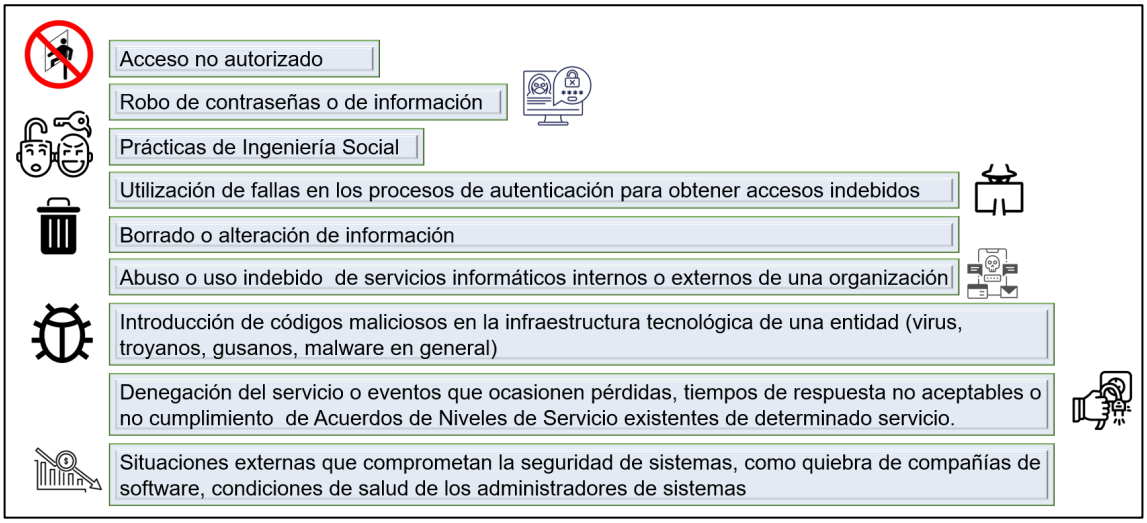
Disponibilidad: Implica la garantía de accesibilidad a los datos y a la información que se debe garantizar a las partes interesadas o a quienes tengan legitimo interés de acceso a los mismos.

Incidente de seguridad de la Información: Es la violación o amenaza inminente a la Política que se ha establecido para garantizar que la información esté segura, seguridad que puede ser implícita o explícita. La norma ISO 27035 los define como eventos indeseados o no esperados que en cualquier caso tienen una posibilidad elevada o altamente representativa de impactar negativamente las actividades

[30] Ibid.

operacionales, negocios y en todo caso, amenazar dichos requerimientos de seguridad[31]. En la siguiente figura se muestran algunos de los más frecuentes casos o incidentes generadores de amenaza o riesgo para la información en el contexto informático:

Figura 4. Principales incidentes de seguridad de la información



Fuente: Elaboración propia con base en CNRISI 2018

Información: conjunto de datos organizados y procesados que funcionan como mensajes, instrucciones y operaciones o cualquier otro tipo de actividad que tenga lugar en una computadora o dispositivo digital.[32]

Confidencialidad: Se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.

Integridad: En seguridad de la información se refiere a cómo los datos se mantienen intactos y libres de modificaciones o alteraciones por terceros, cuando una violación modifica algo en la base de datos o un archivo, sea por accidente o intencionado se pierde la integridad.

Disponibilidad: De la información es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.[33]

[31] CNRISI. Qué es un incidente, 2018. Recuperado el 6 de diciembre de 2022 de https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-un-incidente

[32] https://www.significados.com/informacion/

[33] https://es.m.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Ciberseguridad: Es la capacidad estatal por medio de la cual se minimizan los niveles de vulnerabilidad o riesgo que enfrentan los ciudadanos en materia de seguridad informática en el plano cibernético.[34]

4.3. MARCO LEGAL

- Constitución Política de 1991

De la Norma Rectora se destaca el artículo 15 que eleva a la categoría de derecho fundamental el que todas las personas tengan garantía de reserva respecto de su intimidad personal y familiar, garantía que se extiende al hecho de no ser objeto de conductas que comprometan su buen nombre, a tener conocimiento y posibilidad de realizar trámites para que se rectifique o actualice la información contenida en bases de datos sean estas públicas o privadas, criterios que de acuerdo al mencionado artículo deben darse durante la circulación, tratamiento y la recolección de datos, pero que además implica que existe una reserva superior respecto de la correspondencia y las comunicaciones privadas[35].

El artículo 20 de la misma norma también es relevante en la medida que representa la garantía de libertad que tienen todas las personas de difundir su pensamiento y expresar sus opiniones, informar y recibir información que debe ser verídica e imparcial, e incluso les faculta para fundar medios de comunicación masiva sin ser objeto de censura y sin tener mayores limitaciones que las que imponen los criterios de responsabilidad social. Por otro lado, se encuentra el artículo 61 en el que se establece la responsabilidad estatal de proteger la propiedad intelectual de acuerdo con el contexto temporal y a las formalidades que establece la ley.

- Legislación nacional

Ley 599 de 2000 (Código Penal). Esta norma complementó delitos creados en la normatividad penal de los años 80 como el de “violación ilícita de comunicaciones” mediante el establecimiento de un nuevo bien jurídico: los derechos de autor. Con ello incorporó otras conductas que tenían en cuenta las conductas ilícitas en el contexto informático entre las cuales se puede destacar la compra, venta u ofrecimiento de instrumentos que se utilizan para interceptar comunicaciones privadas.

En esta se mantuvo la estructura del tipo penal de “violación ilícita de comunicaciones”, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas.

[34] https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
[35] Constitución Política de Colombia, 1991.

Ley 1273 de 2009 que modificó el Código Penal mediante la creación de un nuevo bien jurídico al que denominó «Protección de la información de los datos» cuya protección se establecieron nuevos tipos penales por medio de los cuales se penalizan conductas relacionadas con el acceso o uso indebido de sistemas informáticos, su obstaculización, interceptación de datos, daños, entre otros que se presentan en el ámbito de las nuevas tecnologías de la información y comunicación. Adicionalmente, esta norma estableció como circunstancia de mayor punibilidad aplicable a cualquier delito el que se utilicen medios informáticos, telemáticos o electrónicos para su consumación[36]. La siguiente tabla muestra los delitos que fueron creados mediante la referida normatividad.

Tabla 2. Delitos creados por la Ley 1273 de 2009

Delito	Pena
Acceso abusivo a un sistema informático	Prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV
Obstaculización ilegítima de sistema informático o red de telecomunicación	Prisión de 48 a 96 meses y multa de 100 a 1000 SMLMV
Interceptación de datos informáticos	Prisión de 36 a 72 meses
Daño Informático	Prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV.
Uso de software malicioso	Prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV
Violación de datos personales	Prisión de 48 a 96 meses y multa de 100 a 1000 SMLMV.
Suplantación de sitios web para capturar datos personales.	Prisión de 48 a 96 meses y multa de 100 a 1.000 SMLMV
Hurto por medios informáticos y semejantes	Prisión de 6 a 14 años
Transferencia no consentida de activos	Prisión de 48 a 120 meses y multa de 200 a 1.500 SMLMV

Fuente: Elaboración propia

Ley 1431 de 2009. Esta norma se encargó de definir no solos los conceptos, sino también todos aquellos principios que se deben aplicar en una sociedad informática y en la organización de las tecnologías de las comunicaciones y de la información. Su objeto, delimitado en su artículo 1º es el de determinar el marco general para la formulación de las políticas públicas de este sector, la manera como se debe ordenar, el régimen de competencias, los mecanismos de protección a usuarios, cobertura y calidad del servicio e incluso la promoción de inversiones para su fortalecimiento[37] (Ley 1341, 2009).

[36] Numeral 17 del artículo 58 de la Ley 599 adicionado por la Ley 1273 de 2009.
[37] Ley 1341 de 2009, artículo 1º.

Dentro de los aspectos destacables de esta norma se encuentra la creación de la Agencia Nacional del Espectro que de acuerdo con lo indicado en el artículo 25 corresponde a una Unidad Administrativa Especial del orden nacional dependiente del Ministerio de las Tecnologías de la Información y las Comunicaciones creada para brindar soporte técnico para gestionar, planear vigilar y control el espectro electromagnético. Del mismo modo, el establecimiento del Fondo único de Tecnologías de la Información y las Comunicaciones que tiene por objeto, de acuerdo con el inciso segundo del artículo 34 de dicha ley, financiar planes, proyectos y programas que permitan un acceso de todos los habitantes del territorio nacional a las tecnologías de la información y las comunicaciones, así como lograr la apropiación social y productiva de las TIC.

Ley Estatutaria 1581 de 2012. Por medio de este cuerpo normativo se desarrollaron los derechos fundamentales que le asisten a todas las personas en materia de conocimiento, actualización y rectificación de la información que de ellas se recolecte en las bases de datos, así como el derecho a la información uno y otros consagrados en los artículos 15 y 20 de la Constitución Política.

Para ello, la mencionada norma en su artículo 4º estableció ocho principios rectores así: (i) legalidad en materia de tratamiento de datos, (ii) finalidad (debe ser legitima según lo dispuesto en la Constitución y la Ley), (iii) libertad (su tratamiento solo se puede dar previo consentimiento expreso e informado por parte del titular, (iv) veracidad, (v) transparencia, (vi) acceso y circulación restringida, (vii) seguridad y (viii) confidencialidad[38].

- Documentos de política pública

Tal y como se refirió en líneas anteriores, los principales documentos de política pública elaborados por el Consejo Nacional de Política Económica y Social son el CONPES 3701 de 2011, el CONPES 3854 de 2016 y el CONPES 3995 de 2020. A través de ellos se ha venido reconociendo la vulnerabilidad que tienen los sistemas informáticos en el país, su importancia en materia económica y social, la necesidad de gestionar los riesgos que son afines a este entorno y más recientemente, la necesidad de adaptar las medidas de seguridad a los riesgos que surgen de las nuevas tecnologías.

- Disposiciones y documentos institucionales

Resolución 2258 de 2009 de la Comisión de regulación de comunicaciones. Acto administrativo que tiene un enfoque claro en lo que corresponde a la seguridad que se requiere en los servicios de telecomunicaciones, pero también, en lo que tiene que ver con todas aquellas redes que los proveen. Algo a tener en cuenta de este acto administrativo, es que con ella se genera una modificación importante en dos artículos de la Resolución CRT 1732 expedida en el año 2007 (artículos 22 y 23),

[38] Ley 1581 de 2012

pero también, en la Resolución CRT 1740 de 2007, en esta última cambian los artículos 2,4 y 1.8.

Valga la pena mencionar, que dichas disposiciones versan sobre todas aquellas obligaciones que tienen las personas naturales o jurídicas que proveen servicios o redes de telecomunicaciones, en las que claro, se incluyen las que brindan acceso a internet. Dichas compañías, merced a lo contemplado en estas normas reguladoras, deben garantizar la implementación de modelos de seguridad, los cuales deben adecuarse a las características y ante todo a las necesidades específicas de cada red, siguiendo para el efecto los marcos o protocolos de seguridad que ha diseñado la UIT. Además de ello, deben cumplir con los parámetros de confidencialidad, integridad y disponibilidad ya referidos en líneas anteriores. Por último, pero no por ello menos importante, deben contar con medias específicas y eficaces de acceso, no repudio y autenticación., las cuales deben ser acordes a la inviolabilidad de las comunicaciones y la seguridad de la información[39].

Guía No. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de las Tecnologías de la Información y las Comunicaciones. En este documento se describen las características que debe tener un modelo de gestión de incidentes, aspectos relacionados con su detección, evaluación y análisis, así como las estrategias que se deben tener en cuenta para contenerlos, erradicarlos y recuperar información[40].

Todo ello tiene por objeto, según lo resalta el documento consultado, generar un enfoque estructurado y planificado para manejar de manera adecuada los incidentes que se puedan presentar respecto a la seguridad de la información, lo que implica aspectos como la definición de roles y responsabilidades, gestión de eventos, minimización de impactos adversos, consolidación de lecciones aprendidas, definición de mecanismos de monitoreo entre otros[41].

- Tratados internacionales

No puede dejar de mencionarse la Convención de la Naciones Unidas contra la delincuencia organizada transnacional que en su artículo 29 demandó de los Estados parte, medidas de capacitación y asistencia técnica que deben incluir métodos para combatir la delincuencia organizada transnacional utilizando redes de telecomunicaciones, sistemas de cómputo y demás formas desarrollos tecnológicos afines[42].

---

[39] CRC. Resolución 2258 de 2009. Recuperado el 12 de diciembre de 2022 de: https://www.crcom.gov.co/sites/default/files/normatividad/00002258.pdf

[40] MINTIC. Guía para la gestión y clasificación de incidentes de seguridad de la información, 2016. Recuperado el 12 de diciembre de 2022 de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[41] Ibid.

[42] NACIONES UNIDAS. Resolución 55/25, 2000. Recuperado el 16 de diciembre de 2022 de https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

En el mismo sentido, el Convenio sobre la Ciberdelincuencia Budapest suscrito el 23 de noviembre de 2001 en el que se dispusieron mecanismos de cooperación internacional contra la ciberdelincuencia, se presentaron definiciones relacionadas por la seguridad informática aplicables en el contexto global, se estableció un apartado de derecho penal sustantivo en el que se incluyeron delitos como el acceso ilícito, la interceptación ilícita, abuso de dispositivos, ataques contra la integridad de los datos y de los sistemas, falsificación informática entre otros[43].

4.4. MARCO ESPACIAL

Personal Profesional y técnico que integran el área de Seguridad Informática, de Cibersecurity de Colombia LTDA, empresa que tiene sus sedes en el territorio colombiano, especialmente en la zona norte de la ciudad de Bogotá. El objeto social de dicha empresa es el de brindar herramientas y soportes para la seguridad de la información. En términos de visión, la empresa orienta sus esfuerzos a consolidarse (y ser reconocida por ello a nivel nacional), como un eficaz CSIRT (Centro de Respuesta a Incidentes Cibernéticos).

¿Cómo logrará dicho ideal? La política interna de la empresa es alcanzar dicho margen de consolidación y reconocimiento mediante el ofrecimiento de una amplia gama de respuestas a incidentes cibernéticos en los dos escenarios que más demandan los clientes de este tipo de servicios: la gestión del riesgo y la respuesta oportuna y eficaz a los incidentes que se presenten.

[43] CONSEJO DE EUROPA. Convenio sobre la ciberdelincuencia, 2001. Recuperado el 16 de diciembre de 2022 de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

5. METODOLOGÍA

Descriptiva: El tipo de investigación es descriptivo, toda vez que se elaboró el diseño documental incluyendo conceptos, definiciones, estándares y normas nacionales e internacionales que permiten la construcción del producto final. Para ello se acudió a diversas fuentes especializadas en las que se encontraron especificaciones sobre tales puntos, las cuales alimentaron diferentes apartados como el marco referencial y el desarrollo de objetivos con el fin de contar con una base argumentativa para el desarrollo de estos tópicos.

Analítica: En el entendido que se aborda la situación actual que conlleva la creación e implementación de un CSIRT, realizando un análisis comparativo con centros de respuestas a incidentes informáticos nacionales e internacionales en su estructura documental para su creación. De esta manera, la propuesta se desarrolla en torno al análisis que se realizó entre los avances que en esta temática se ha gestado en otras latitudes, haciendo especial hincapié en el caso del continente Europeo, para, a partir de ello plantear la conveniencia de desarrollar estrategias similares en Colombia.

Enfoque cualitativo: La investigación está basada en una necesidad real, aborda documentos, conceptos y procesos con el fin de ser estudiados para generar los resultados deseados y que permitan crear el diseño documental para poner en funcionamiento un CSIRT. En este caso, se privilegiaron las cualidades del problema y no las cantidades o cifras exactas que se pudieran obtener al respecto, pues se consideró que con ello se lograba un texto más comprensible y afín a las características conceptuales que es en todo caso lo que más ocupa la atención del trabajo.

6. DESARROLLO DE OBJETIVOS ESPECÍFICOS

6.1. PRIMER OBJETIVO

Analizar el marco normativo y legal en Colombia y a nivel internacional, en donde se establezcan los parámetros que reglamentan la creación de un CSIRT.

Al entrar a revisar la normatividad que regula un CSIRT, es importante mencionar la siguiente reseña histórica; en noviembre de 1988, un incidente de seguridad informática conocido como "gusano de Internet" puso de rodillas a partes importantes de Internet. La reacción a este incidente fue aislada y descoordinada, lo que resultó en un esfuerzo muy duplicado y en soluciones conflictivas. Semanas después, se formó el Centro de Coordinación CERT. Poco después, el Departamento de Energía de los Estados Unidos formó la Capacidad de Asesoramiento de Incidentes Informáticos CIAC para servir a sus constituyentes.

En el corto plazo, es decir los dos años siguientes, se multiplicaron los equipos establecidos para ofrecer el servicio de respuesta a incidentes, cada uno con su propio propósito, financiamiento, requisitos de informes y circunscripción. No fue fácil la interacción entre dichos equipos pues debían superarse dificultades relacionadas con aspectos como las convenciones transnacionales, los estándares individuales, zonas horarias e incluso el idioma. En octubre de 1989, un incidente importante llamado "gusano Wank" destacó la necesidad de una mejor comunicación y coordinación entre los equipos. El primero se formó en 1990. Desde entonces, ha seguido creciendo y evolucionando en respuesta a las necesidades cambiantes de los equipos de seguridad y respuesta a incidentes y sus circunscripciones.

En 2002, Internet había crecido de 60,000 sistemas de computadoras host a 150 millones en casi todos los países del mundo. Muchas empresas ahora confían en Internet en sus transacciones comerciales diarias. Se siguen formando equipos de respuesta a incidentes y seguridad en todo el mundo, que abarcan una variedad de circunscripciones de países enteros y organizaciones multinacionales. La membresía FIRST consiste en equipos de una amplia variedad de organizaciones, incluidas las educativas, comerciales, de proveedores, gubernamentales y militares.[44]

Las tendencias gubernamentales de los países más avanzados en materia de gestión de la seguridad y lucha contra la delincuencia y el terrorismo, corroborado por entidades supranacionales como la Comisión de la Unión Europea, la ENISA (Agencia Europea de Seguridad de las Redes de la Información), la UIT (Unión

[44] https://www.first.org/about/history

Internacional de Telecomunicaciones e incluso la misma OTAN. Cada una de estas entidades, de manera individual o en conjunto, le han apostado a la idea de formar organizaciones con alta capacidad técnica, que salvaguarden la seguridad de redes y sistemas de información en los contextos nacionales pero que a la vez se constituyen en centros de seguimiento y suministro de información real. Todo ello bajo la premisa que en las circunstancias actuales, la seguridad informática representa un beneficio colectivo invaluable que en gran medida contribuye a que una interacción social armónica.

Así las cosas, en 1992 se creó el primer CERT europeo, el SURFnet-CERT, en Holanda y, un año después, en 1993, se creó el BSI-CERT alemán, que en 2001, al pasar a ser una unidad organizativa propia, se transformó en el CERT-Bund. Es importante precisar que en la creación de un CERT no implica simplemente implementar tecnología, sino adoptar una serie de procesos (compuestos por distintos recursos: humanos, económicos, tecnológicos, etc.), gestionados de acuerdo con unas políticas, normas y procedimientos que persiguen cumplir unos objetivos de negocio concretos.

Entre los distintos factores que contribuyen al éxito de un CERT, se sitúa la proporcionalidad de los recursos con los que se dote con respecto a las expectativas de demanda que genere, al igual que en cualquier otro servicio. Por lo tanto, a la hora de dimensionar correctamente este tipo de equipos deberá considerarse los siguientes parámetros:

- Tamaño de la Comunidad a la que se da servicio: Este es el parámetro principal, puesto que a mayor número de miembros se generarán más peticiones de asistencia en gestión de incidentes y de otro tipo.

- Grado de autoridad sobre los miembros de la Comunidad y el modelo de relación jerárquica entre ambos: Es relevante si se solicitarán los servicios por propia iniciativa o por imperativo legal, lo que condiciona en este último caso la existencia probable de un mayor volumen de incidentes a gestionar.

- Servicios ofrecidos y nivel de servicio: Si se ofrecen servicios en modo 24x7 los 365 días del año se requerirán de muchos más recursos humanos y técnicos que si únicamente se prestan en horario laboral. También hay que considerar los acuerdos de servicio y tiempos de respuesta, como por ejemplo las modalidades de "*best effort*" (el equipo se compromete a cumplir con las peticiones de su Comunidad, aunque no existe una obligación formal) o de "*next business day*" (la petición se atenderá a partir del próximo día laborable), o incluso periodos menores de respuesta.

- Promoción y comunicación de servicios: Uno de los parámetros que más influirá será el grado de conocimiento por parte de la Comunidad de los servicios que se ofrecen. Este aspecto implica que la dotación del CERT

debe ir progresando a medida que aumente su impacto prestando atención a la promoción y comunicación de los nuevos servicios.

- Proceso de maduración. Establecer un CERT es un proyecto a largo plazo, que debe ir madurando y ampliándose en la medida que ofrezca valor a su comunidad y se gane su confianza. Normalmente, no se puede considerar completamente implantado hasta al menos dos años después de su inauguración.

- Plan estratégico: Es conveniente planificar la correcta evolución del CERT, prestando la adecuada atención a los aspectos de financiación y sostenibilidad a largo plazo contemplando la entrada progresiva de nuevos servicios, así como de los recursos necesarios para implantarlos, promocionarlos y operarlos.[45]

En Colombia a través del Documento CONPES (Consejo Nacional de Política Económica y Social) 3701 se establecieron los lineamientos de Política para Ciberseguridad y Ciberdefensa, los cuales se orientaron a contrarrestar la problemática central que se avizoró en dicho momento, a saber, que las capacidades del Estado para hacer frente a las amenazas de orden cibernético no solo eran débiles, sino que claramente se carecía de una estrategia nacional que se ocupara específicamente de su identificación, gestión y prevención[46].

Apuntándole a superar dicha debilidad, y teniendo como soporte una serie de directrices internacionales sobre la materia, se adoptaron tres objetivos primordiales de naturaleza regulatoria, ilustrativa y de legislación así:

i. Diseñar y adoptar un merco de interlocución entre las diferentes entidades e instituciones estatales, orientado a controlar, prevenir, coordinar e incluso suministrar recomendaciones permanentes que permitan enfrentar y anticipar los riesgos y las amenazas en el plano informático.

ii. Ofrecer capacitación permanente y especializada en temas como la seguridad de la información; así mismo, ampliar las líneas investigativas en ciberseguridad y ciberdefensa.

iii. Robustecer el marco legal en materia de ciberseguridad y el que permita ampliar los mecanismos de cooperación internacional, esto último mediante medidas como que Colombia formalice cuanto antes su adhesión a los instrumentos diseñados por la comunidad internacional para contrarrestar este tipo de riesgos.

[45] https://es.scribd.com/document/334910886/810-ENS-Guia-Creacion-CERT
[46] DNP. Documento CONPES 3701 Lineamientos de Política para ciberseguridad y ciberdefensa, 2011. Recuperado el 10 de febrero de 2023 de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

En la parte institucional se diseñaron las siguientes entidades: Comisión Intersectorial, presidida por el presidente de la República, Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), Comando Conjunto Cibernético de las Fuerzas Militares (Ccoc) y el Centro Cibernético Policial (CCP).

Es importante tener en cuenta que el Conpes no creó estas entidades por no tener las facultades para ello, simplemente realizó las recomendaciones al Ministerio de Defensa en ese año (2011). En la siguiente figura se muestra la estructura de la referida Comisión Intersectorial y los parámetros de interlocución que deben tener en cuenta las instituciones comprometidas:

Figura 5. Estructura de la Comisión Intersectorial y el COLCERT

Fuente: Documento CONPES 3701

En ese mismo documento se analizaron las políticas en materia de ciberseguridad y ciberdefensa, y la incorporación de nuevas capacidades tecnológicas y así tenerlos en cuenta un marco de referencia, como por ejemplo en febrero de 2011, el gobierno alemán lanzó su Estrategia de Seguridad Cibernética, en abril de 2011 el Ministerio del Interior puso en marcha el Centro Nacional de Ciberdefensa. AUSTRALIA Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio; CANADÁ a través del Departamento de Seguridad Pública implementó el Centro Canadiense de Repuesta a Incidentes Cibernéticos (CCIRC), y en octubre de 2010 adoptó la Estrategia Canadiense de Seguridad Cibernética.

ESTADOS UNIDOS Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), DHS: National

Cyber Security Division, US-CERT: United States Computer Emergency Readiness Team y la oficina de Seguridad Cibernética de la Casa Blanca y en mayo de 2011 fue adoptada la Estrategia Internacional para el Ciberespacio.

ESTONIA En 2008 creó juntamente con otros países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciber amenazas, en ese mismo año es adoptada una Estrategia de Seguridad Cibernética.

FRANCIA Creó la Agencia de Seguridad para las Redes e Información (ANSSI), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos, en febrero de 2011 fue adoptada una Estrategia de Defensa y Seguridad de los Sistemas de Información.[47]

Por otra parte, es imprescindible indicar que cuando se pone en marcha un CSIRT se debe determinar qué tipo de servicios prestara, teniendo en cuenta que en la actualidad los CSIRT se crean y funciona en diferentes sectores.

- CSIRT sector académico
- CSIRT sector comercial
- CSIRT sector protección información vital e infraestructuras vitales (CIP/CIIP)
- CSIRT sector público
- CSIRT interno
- CSIRT sector militar
- CSIRT sector nacional
- CSIRT sector de la pequeña y mediana empresa (PYME)
- CSIRT de soporte

CSIRT sector académico: Estos se encargan de ofrecer servicios de seguridad a instituciones educativas públicas y privadas, materializando su labor principalmente en los campus virtuales y centros de investigación de las instituciones de educación superior. Las actuaciones en materia de ciberseguridad se dirigen tanto a la protección de las instituciones como de docentes y estudiantes que interactúen en dichos escenarios.

CSIRT comercial: Como lo indica su nombre, tienen como principal campo de acción el sector comercio. En términos prácticos procuran garantizar una interacción segura en el espacio virtual comercial para evitar abusos, afectaciones, defraudaciones y todos aquellos riesgos que puedan afectar la confianza tanto de proveedores como de compradores. Evidentemente se trata de un servicio pago,

[47] https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

que se justifica en la medida que la adquisición del servicio disminuya sustancialmente los riesgos de pérdidas.

CSIRT sector CIP/CIIP: Por regla general, este tipo de CSIRT desarrollan su labor bajo la dirección, en coordinación o en cooperación con entidades o departamentos públicos que tienen deberes legales, misionales y funcionales relacionados con la protección de las infraestructuras vitales y la protección de la información tanto de los ciudadanos individual o colectivamente considerados, organizaciones privadas y el mismo Estado

CSIRT sector público: Los servicios de estos se concentran principalmente en lo que corresponde a la seguridad informática de las agencias estatales y todas aquellas dependencias por medio de la cual se cumplen los fines y propósitos de las autoridades públicas.

CSIRT interno: Estos se encargan de ofrecer servicios de seguridad exclusivamente para la entidad o la organización a la cual se encuentran adscritos, constituyendo por regla general el primer punto de control que se complementa con otros centros del sector en el que llevan a cabo sus operaciones. Se ubican principalmente en entidades financieras y organizaciones de telecomunicaciones que por la complejidad de su labor deben contar con un mecanismo anticipado de defensa y prevención de riesgos informáticos

CSIRT sector militar: Ministerios o carteras de gobierno dedicados a la seguridad nacional suelen ser los principales clientes de estos centros. Por ello, la labor que cumplen estos CSIRT suele ser llevada a cabo por personal especializado y con un amplio margen de confianza dado que su labor se dirige a gestionar riesgos de trascendental importancia como aquellos que tienen relación directa con la seguridad nacional.[48]

Continuando con la normatividad que regula la creación de un CSIRT, se cuenta con una guía de buenas prácticas para establecer un CSIRT nacional; documento originado desde la Organización de los Estados Americanos, que relaciona de manera detallada dicho procedimiento de implementación.

La guía analiza varios tipos de CSIRT, entre ellos los CSIRT a nivel nacional, que responden a incidentes a nivel estado-nación. Por lo general, estos monitorean y responden a incidentes en las redes gubernamentales y también sirven como un coordinador de seguridad de la información para el sector privado u otros sectores e instituciones.

Todos los aspectos relacionados con los CSIRT, similares a la seguridad de la información en sí misma, requieren del amplio entendimiento de una serie de diferentes disciplinas, aparte de la tecnología. También incluyen temas adicionales como la gestión de recursos humanos, los procesos legales, la planificación

[48] https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

financiera, las adquisiciones y muchas otras. La supervisión y la gestión de proyectos son particularmente importantes en la creación y el despliegue de los CSIRT, ya que necesitan funcionar de una manera estructurada, gradual y estratégica durante las fases de planificación, que requiere la colaboración entre los diversos grupos de interés.[49]

La guía es un documento que sirve como referencia para los objetivos de la empresa Cibersecurity de Colombia LTDA, y que se puede adaptar perfectamente a la necesidad de la creación e implementación del CSIRT, claro sin dejar de lado otra normatividad que complementa lo antes referenciado; dicha guía se divide en tres secciones principales: planificación, ejecución y cierre, que describen los principales objetivos y los resultados de cada fase y presentan materiales de apoyo en el proceso.

6.2. SEGUNDO OBJETIVO

Examinar los estándares y las buenas prácticas implementadas por las Organizaciones Internacionales de Normalización, en donde se regula la estructura y requerimientos de un CSIRT y que contribuyan a consolidar su esquema documental.

La guía de buenas prácticas para establecer un CSIRT nacional elaborada por la Organización de las Naciones Unidas, plantea los siguientes aspectos para crear un CSIRT, en donde es necesario definir el marco que guiará y regirá el funcionamiento del equipo, la naturaleza y los objetivos del CSIRT y la comunidad objetivo (gobierno, sector privado, o ambos).

Un CSIRT nacional debe identificar claramente su misión y su visión, estos dos aspectos no solo servirán de guía a los que trabajan en el equipo, sino que servirán como referencia a cualquier persona que reciba sus servicios o colabore con él, en resumen, la misión y el objetivo son las razones por las cuales existe el CSIRT; el marco institucional de un CSIRT establecerá su configuración.

Un CSIRT puede constituirse como una empresa independiente para proporcionar servicios en el ámbito privado, como una unidad dentro de una organización pública o privada para prestar servicios internos o externos, o como una organización en sí misma que no depende de ningún grupo o entidad en particular.

[49] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

6.2.1 Servicios reactivos y proactivos. Este tipo de servicios son los más importantes que ofrece un CSIRT. En esencia, los “servicios reactivos” responden a los incidentes de seguridad cibernética que ocurren en la comunidad del CSIRT o en su propia infraestructura. Se puede brindar una respuesta derivada de una solicitud de asistencia, los principales tipos de servicios reactivos son la gestión de incidentes, la respuesta de la vulnerabilidad y la respuesta a artefactos.

Gestión: las fases de este servicio son cinco: (i) notificación y recepción del incidente; (ii) triage o clasificación; (iii) respuesta, (iv) análisis y (v) resolución. Las primeras fases permiten determinar tanto el tipo de un incidente que atenta contra la seguridad, su potencial impacto. A continuación, se designa el equipo que responderá a la amenaza el cual se encarga de determinar o diseñar el plan de acción por medio del cual se mitiga la afectación o se restauran los sistemas o servicios permitiendo, en este último caso, que se restablezcan y continúen con su funcionamiento normal. Eventualmente y dada la complejidad del incidente, se hará necesario que el CSIRT acuda directamente a inspeccionar el sitio en el que se presentó el evento o incidente generador de inseguridad.

En desarrollo de este servicio pueden participar diferentes actores como los ISP, proveedores de tecnología, entidades estatales de seguridad, departamentos de prensa, e incluso otros CSIRT, sin descartar la participación según lo requiera el incidente, de equipos legales y actores internacionales. Para optimizar estos esfuerzos conjuntos y disminuir los tiempos de respuesta se debe garantizar que exista una efectiva coordinación entre estos actores, labor que estará a cargo del CSIRT, lo que implica que este último conozca con claridad cada una de sus necesidades y requerimientos.

Respuesta a vulnerabilidades: se incluyen en esta todos los procesos por medio de los cuales se gestionan las vulnerabilidades detectadas tras recibir y valorar el incidente. Se incluyen actuaciones como la instalación de parches, aplicación de contramedidas y en general todas aquellas estrategias que tengan como finalidad mitigar el impacto generado por el incidente. En lo que tiene que ver con la instalación de parches, es deber del CSIRT notificar a los interesados. Del mismo modo, debe distribuir los parches y si es necesario, describir las técnicas utilizadas para la implementación de contramedidas, así como coordinar y confirmar que se ejecuten las medidas requeridas para contrarrestar la amenaza.

Respuesta a artefactos maliciosos: Este tipo de respuestas se dan en aquellos incidentes en los que se evidencia que un archivo u objeto está relacionado con un ataque dirigido en contra del sistema o de la misma red, pero también, cuando dichos elementos han sido utilizados con el fin de evadir los mecanismos, medidas o controles de seguridad. Para la gestión de estos elementos es necesario realizar la extracción del sistema u orientar a las partes interesadas acerca de la manera como deben llevar a cabo dicha gestión.

Servicios proactivos: los principales tipos de estos servicios son el seguimiento, la distribución permanente de alertas y los servicios de investigación y desarrollo. Su propósito o finalidad es la de generar mejoras tanto en infraestructura como en la seguridad. En uno y otro caso se procura que la comunidad objetivo prevenga incidentes de seguridad o, en aquellos eventos en que estos ocurren, su impacto sea menor.

Primer nivel: en este se ubican los servicios básicos del CSIRT: alertas y monitoreo. Para llevarlos a cabo se deben implementar sistemas que permitan identificar en tiempo real los incidentes o eventos que generen riesgos para la seguridad, información que es utilizada para la toma de decisiones estratégicas orientadas a mejorar los procesos de respuesta. El efecto de ello son los informes automatizados y procesos de escaneo por medio de los cuales se realiza la búsqueda de vulnerabilidades. Con el fin de lograr lo anterior el CSIRT puede emplear herramientas y/o sensores cuya fuente sea abierta o provenga de terceros, sin perjuicio de la posibilidad de desarrollar soluciones internas.

Segundo nivel: A medida que el CSIRT se desarrolla podrá ofrecer mejores servicios de alerta y vigilancia mediante la instalación de sensores de seguridad en la infraestructura o la interconexión del sistema. Gracias a ello se logra realizar un seguimiento más amplio e integral tanto a la infraestructura como a los sistemas de la comunidad destinataria del servicio. Aunque se trata de alertas y correlación de incidentes de la misma tipología que se ofrece en el monitoreo de primer nivel, no cabe duda que se trata de un seguimiento más cercano a los sistemas de cada cliente, circunstancia que posibilita que las vulnerabilidades, eventos de seguridad y artefactos maliciosos se detecten de manera temprana.

6.2.2 Investigación y desarrollo: se desarrollan en tres niveles según se describe a continuación:

El primero comprende todos aquellos servicios que permiten que el CSIRT y la comunidad objetivo estén al tanto de avances o innovaciones que surjan sobre seguridad de la información y respuesta oportuna a los incidentes que la afectan. Gracias a ello, se logra una actualización continua y en tiempo real sobre todos aquellos aspectos de defensa entre los cuales vale la pena mencionar las amenazas que surgen en el día a día, las normas aplicables a los servicios, buenas prácticas, mantenimiento y operación adecuada de dispositivos, vectores de ataque emergentes, entre otros.

El segundo nivel tiene una relación directa con la madurez operacional del CSIRT. En otras palabras, se trata del proceso gracias al cual las capacidades de este se robustecen, especialmente las de I+D. Una de las bondades que resultan al alcanzar este nivel es que en el marco del mismo, el CSIRT recopila y genera información suficiente para ejecutar actividades de auditorías en los sistemas que vigila, incluyendo en estos protocolos de análisis de infraestructura,

vulnerabilidades, ejecución de pruebas de penetración entre otras que actualmente se han integrado a los estándares internacionales en materia de seguridad informática.

Por último, pero no por ello menos importante, se tiene un tercer nivel en el que los CSIRT que han alcanzado la robustez descrita en el párrafo anterior logran tener un amplio desarrollo de capacidades de I+D al punto que logran llevar a cabo acciones avanzadas como el análisis de códigos maliciosos con lo cual determinan el comportamiento y la naturaleza de este tipo de amenazas y su incidencia en sistemas o equipos determinados.

6.2.3 Servicios de valor agregado. Estos servicios complementan los avisos de monitoreo y alerta emitidos por el CSIRT; en general, los servicios de valor agregado consisten en eventos y cursos de formación en seguridad, iniciativas de sensibilización, análisis de competencias y laboratorios de seguridad; mediante la realización de este tipo de eventos, el CSIRT también genera confianza dentro de la comunidad y crea conciencia del propósito y la función del equipo de respuesta, lo que le permite operar con mayor eficacia.

Uno de los aspectos más importantes de las actividades de capacitación eficientes es identificar las carencias y las necesidades de información de la comunidad objetivo, gran parte de esto se conocerá en la actividad normal cotidiana del CSIRT y en la interacción con sus clientes.

6.2.4 Estructuras organizacionales: corresponde al equipo de seguridad localizada: Esta es la estructura CSIRT menos formal; la teoría que sustenta el “equipo de seguridad” sencillo es que los eventos de seguridad se resuelven con el personal existente en las organizaciones, los miembros del equipo de seguridad no son necesariamente especialistas en respuesta a incidentes o seguridad de la información; pueden ser administradores de sistemas, bases de datos o tienen conocimientos especializados en los diversos componentes o productos que intervienen en los sistemas de TI como cortafuegos y routers, entre otros. En la mayoría de los casos, el equipo de seguridad no tendrá todos los conocimientos y la experiencia necesaria para llevar a cabo operaciones de seguridad sólidas. Por ejemplo, puede resolver un incidente, mas no determinar su causa, y así deja a la organización expuesta a ser explotada de nuevo, la naturaleza de un “equipo de seguridad” por lo general impide la aplicación de mejores prácticas, investigación y desarrollo, monitoreo y actividades de alerta de seguridad.

Equipo de respuesta a incidentes distribuidos: Grandes organizaciones con infraestructuras de TI distribuidas geográficamente o varias unidades de negocios en particular a menudo adoptan estructuras de respuesta a incidentes distribuidos. Estos se componen de un centro de respuesta integral dividido en varios equipos, uno de los cuales coordina las actividades de los demás.

Las funciones de respuesta a incidentes se dividen según el área de conocimiento de cada equipo, en función de la ubicación geográfica donde se producen los incidentes, o en función del sector de la comunidad objetivo afectado.

El papel del equipo de coordinación es esencial para garantizar unos procedimientos de respuesta efectivos y estandarizados, mantener estadísticas de incidentes, aumentar la sinergia y promover el trabajo colaborativo por medio del intercambio de las mejores prácticas y lecciones aprendidas y cómo asignar adecuadamente los recursos de seguridad. Otra de las funciones vitales del equipo coordinador es facilitar la interacción y la cooperación entre los equipos.

Equipo de respuesta a incidentes centralizado: En esta estructura hay un solo equipo responsable de la gestión y respuesta de incidentes de seguridad por medio de una serie de ubicaciones que pertenecen a una organización más grande; este modelo sería apropiado, por ejemplo, en una empresa, esta estructura es apropiada para organizaciones cuya infraestructura de TI no está dispersa geográficamente.

En estas estructuras, hay un equipo de respuesta definido con personal dedicado y capacitado en el manejo de seguridad de la información y la respuesta a incidentes de seguridad, estos equipos interactúan con especialistas en los productos o servicios.

Equipo coordinado: Este modelo es similar al modelo de equipos de respuesta distribuidos, pero a nivel de centros de respuesta; la diferencia es que el coordinador de centro de respuesta no necesariamente tiene que intervenir en las gestiones de otros equipos coordinados.

Este tipo de modelo surge de la necesidad de los centros de respuesta de interactuar de forma coordinada para lograr un objetivo común, o generar sinergias entre los centros de sectores similares o regiones, empresas o agencias de un mismo gobierno.

Su principal función es la de coordinar la eficacia de la respuesta y la interacción. Para ello ejecuta actos de gestión, coordinación y colaboración. Del mismo modo, suministra análisis integrales respecto a los factores de riesgo, genera boletines informativos e incluso presenta soportes estadísticos y formula estrategias o buenas prácticas dirigidas a anticipar y prevenir las amenazas.

Es importante tener en cuenta que con el fin de definir el modelo de CSIRT por implementar, es esencial analizar los servicios que desean ofrecer, ciertos modelos de CSIRT no son adecuados para la prestación de algunos de los servicios antes mencionados, en particular los servicios que requieren recursos permanentes.

Es importante definir el tipo de modelo de CSIRT por implementar, ya que esto tendrá una consecuencia directa sobre el tamaño de la organización.[50]

6.2.5 Funciones y responsabilidades: para definir la estructura de un CSIRT se debe tener claro las funciones del personal a cargo y sus responsabilidades dentro del equipo de trabajo, teniendo claro que son múltiples actividades las que se deben realizar en un CSIRT para cumplir con los objetivos y servicios trazados, entre ellos se deben garantizar la gestión de incidentes cibernéticos, el análisis de vulnerabilidades, análisis de la situación de ciberseguridad, entre muchos otros, es por ello que deben estar muy bien definidos los roles y funciones de las personas que se desempeñan dentro del mismo de tal manera que se garantice su funcionamiento y operatividad permanentemente, en ese orden de ideas es importante precisar que las personas (recurso humano) y el talento con el que cuentan de cada uno de ellos, pasan a ser el componente más valioso dentro de la conformación de un CSIRT.

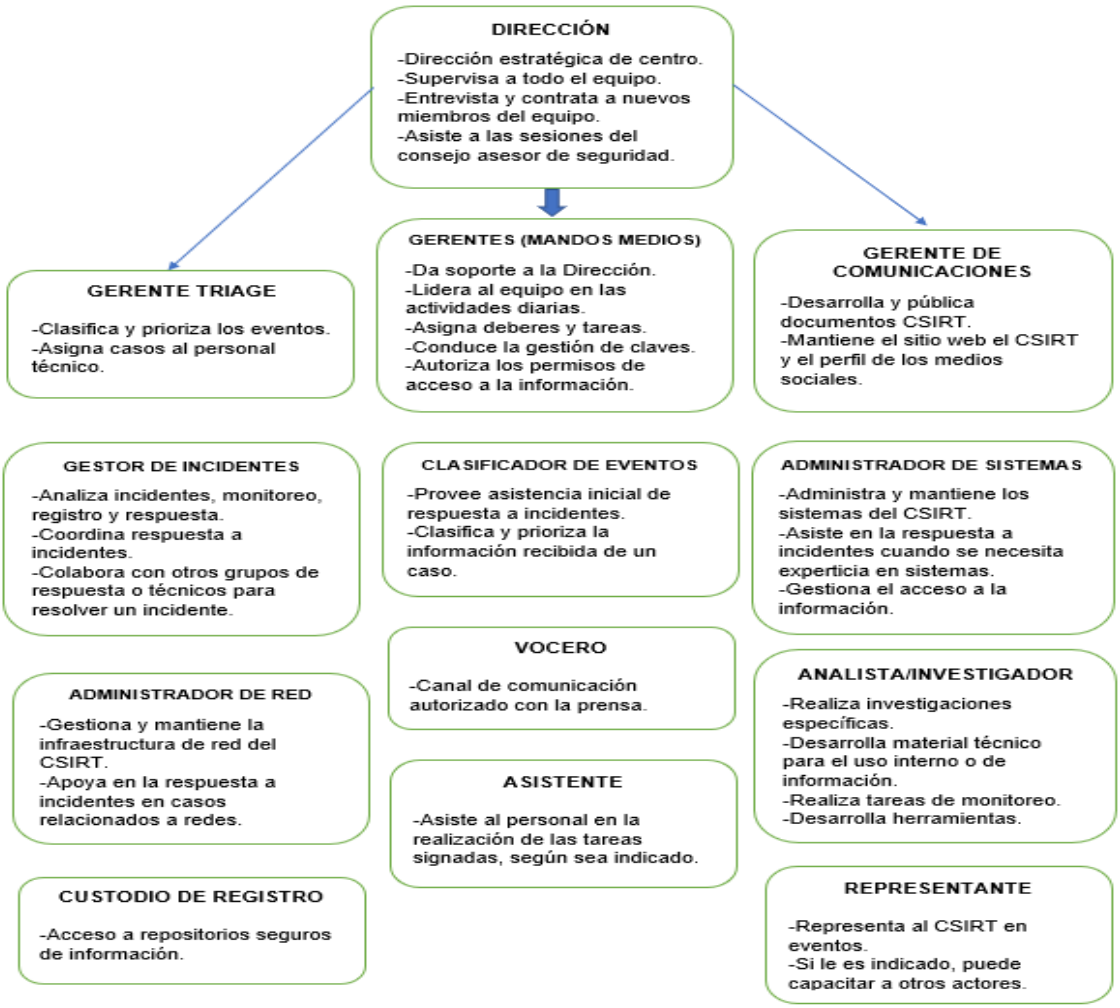
Sin dejar de lado que bebe existir sinergia dentro del equipo de trabajo, esto independiente de los diferentes perfiles o roles que confluyen, así se garantizara el cumplimento del objeto del negocio, dentro de estos perfiles se tienen los siguientes:

- Dirección
- Gerentes (mandos medios)
- Gerente de Triage
- Gerentes de comunicaciones
- Gestor de incidentes
- Clasificador de eventos
- Administrador de sistemas
- Administrador de red
- Vocero
- Analista (investigador)
- Custodio de registro
- Representante
- Asistente

En el siguiente esquema se muestra cada uno de los anteriores perfiles, funciones y responsabilidades.

[50] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Figura 6. Funciones y responsabilidades en la estructura del CSIRT



Fuente: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

6.3 Tercer objetivo

Analizar y comparar los requerimientos documentales implementados en la creación de un centro de respuesta a incidentes informáticos (CSIRT), a nivel nacional e internacional, que sirvan como referente para el diseño documental del CSIRT en la empresa Cibersecurity de Colombia LTDA.

Dentro de los requerimientos documentales implementados en la creación de un CSIRT, bien sea nacional o internacional se incorpora la realización de una taxonomía de ataques para la actuación del CSIRT, es así que con el fin de modelar el diseño documental para el funcionamiento del CSIRT en la empresa Cibersecurity

de Colombia LTDA; a continuación, se presenta una clasificación o taxonomía de los posibles incidentes de seguridad, no sin antes mencionar que no todos los incidentes poseen las mismas características, ni tampoco cuentan con las mismos alcances, por tal razón es imprescindible contar con una taxonomía de estos incidentes, que permitan al CSIRT una vez presentado el ataque, poder lograr realizar un análisis, contención y la eliminación del mismo.

6.3.1 Taxonomía de los incidentes de seguridad informática: Antes de entrar a proponer la taxonomía de los incidentes informáticos o de seguridad a tener en cuenta en Cibersecurity de Colombia LTDA, es importante entender que un incidente de seguridad informática es un evento o serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio; provocando una pérdida o uso indebido de información, interrupción parcial o total de los Sistemas, siendo los más comunes, la infección por malware, phishing, etc. [51]; acto seguido se presenta el ciclo de vida en la gestión y respuesta a un incidente de seguridad; modelo a tener en cuenta y que es propuesto por parte del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

En la siguiente figura se muestra como debe ser el ciclo de vida en materia de gestión y respuesta a incidentes de seguridad informática desde la fase previa hasta la culminación del incidente, aspecto fundamental para el adecuado diseño de la estrategia.

Figura 7. Modelo ciclo de vida en gestión y respuesta a incidentes de seguridad informática

Fuente: Ministerio de las Tecnologías de la Información y las comunicaciones (2016).

[51] https://www.uv.mx/csirt/que-es-un-incidente-de-ciberseguridad/

Ahora bien, tomando como referencia las políticas de ciberseguridad del Gobierno de España, en donde se define una taxonomía de ciber incidentes, la cual está a disposición como referente para cualquier entidad o empresa privada o pública y una vez realizado un análisis al mismo, se logra establecer que la presente guía, se ajusta a los requerimientos de la empresa Cibersecurity de Colombia LTDA, sirviendo como un marco de referencia para ajustar la presente clasificación a los propósitos de análisis, contención y eliminación de los posibles ataques o incidentes presentados en los clientes de la organización.

A continuación, se presenta una tabla que se compone de la clasificación, los tipos de incidente y la descripción de estos, conceptos que deben ser tenidos en cuenta al momento de desarrollar el ciclo antes mencionada a fin de que las actividades de contención, erradicación y recuperación que se adopten sean las idóneas para el logro de dichos propósitos de seguridad cibernética.

Tabla 3. Clasificación taxonómica de los incidentes informáticos

Clasificación	Tipo de incidente	Descripción
Contenido abusivo	Spam	Correo electrónico masivo no solicitado; el receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito	Contenido difamatorio o discriminatorio; algunos ejemplos, ciberacoso, racismo, amenazas a una persona o colectivos, etc.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil o se haga apología a la violencia, etc.
Contenido dañino	Sistema infectado	Sistema infectado con malware; Ej. Sistema, computadora o teléfono móvil infectado con un rootkit.
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.
	Malware dominio DGA	Nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).

Obtención de información	Escaneo de redes (snanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado. Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Disponibilidad	DoS (Denegación de servicio)	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
		Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o

Compromiso de la información	Acceso no autorizado a información	mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Perdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
	Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
Vulnerable	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Ej. Telnet, RDP o VNC. Acceso público a servicios en los que potencialmente pueda relevarse

	Revelación de información	información sensible. Ej: SNMP o Redis. Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
	Sistema vulnerable	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	Otros	
Otros	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
	Ciberterrorismo	Uso de redes o sistemas de información con fines de carácter terrorista.
	Daños informáticos PIC	Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

Fuente: Recuperado el 4 de diciembre de 2022 de: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

Sumado a lo anterior se deben implementar los indicadores de peligrosidad a las posibles amenazas que podrían pasar a ser incidentes o ataques informáticos, en ese orden de ideas los incidentes deben estar asociados a alguno de los siguientes niveles de peligrosidad que de acuerdo a la misma fuente son cinco y se identifican mediante una escala cromática según se muestra en la siguiente figura:

Figura 8. Niveles de peligrosidad de los incidentes informáticos

Fuente: Recuperado el 4 de diciembre de 2022 de: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

Establecidos los niveles de peligrosidad, se hace necesario asignar un determinado nivel de peligrosidad a los incidentes de seguridad, con el fin de facilitar su gestión; a continuación, se relacionan los mencionados criterios.

Tabla 4. Criterios de determinación del nivel de peligrosidad de un incidente informático

Nivel	Clasificación	Tipo de Incidente
CRÍTICO	Otros	APT Ciber terrorismo Daños informáticos PIC
MUY ALTO	Código dañino	Distribución de malware
		Configuración de malware
	Intento de intrusión Intrusión Disponibilidad	Ataque desconocido Robo Sabotaje
		Interrupciones
ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino Intento de intrusión	Sistema infectado
		Servidor C&C (Mando y Control)
		Malware dominio DGA Compromiso de aplicaciones
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
		Phishing

MEDIO	Fraude Contenido abusivo Obtención de información Intento de intrusión Intrusión	 Contenido difamatorio o discriminatorio Ingeniería social Explotación de vulnerabilidades conocidas Intento de acceso con vulneración de credenciales Compromiso de cuentas con privilegios
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
BAJO	Contenido abusivo Obtención de información	Spam Escaneo de redes (Scanning) Análisis de paquetes (sniffing)
	Intrusión	Compromiso de cuenta sin privilegios
	Otros	Otros

Fuente: Recuperado el 4 de diciembre de 2022 de: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

Aunado a lo anterior es importante asociar a los incidentes informáticos el impacto y sus posibles consecuencias en la organización, empresa o institución atacada o afectada; para tal fin se tienen en cuenta aspectos como posibles consecuencias bien sean materializadas o no y que desemboca en una amenaza a la infraestructura informática o los sistemas de la organización afectada. (Pública, privada o particulares); así las cosas, a continuación, se describen los criterios a tener en cuenta y su nivel de impacto, de acuerdo a los siguientes parámetros.

- Impacto en la Seguridad Nacional o en la Seguridad Ciudadana.

- Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costos propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputacionales asociados.

En ese orden de ideas, a los incidentes se les debe asociar el nivel de impacto el cual también cuenta con una delimitación cromática según se aprecia en la siguiente figura:

Figura 9. Niveles de impacto asociados al incidente informático

Fuente: Recuperado el 4 de diciembre de 2022 de: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

Por consiguiente, se debe incluir una tabla de consulta en la que debe reposar la información del incidente y su nivel de impacto, como se muestra a continuación.

Tabla 5. Criterios de determinación del nivel de impacto de un incidente informático

NIVEL	DESCRIPCIÓN
CRÍTICO	Afecta apreciablemente a la Seguridad Nacional.
	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	Afecta a una Infraestructura Crítica.
	Afecta a sistemas clasificados SECRETO.
	Afecta a más del 90% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios. El incidente precisa para resolverse más de 30 Jornadas-Persona.
	Impacto económico superior al 0,1% del P.I.B. actual. Extensión geográfica supranacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales. Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.

MUY ALTO	Afecta apreciablemente a actividades oficiales o misiones en el extranjero. Afecta a un servicio esencial.
	Afecta a sistemas clasificados RESERVADO. Afecta a más del 75% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios.
	El incidente precisa para resolverse entre 10 y 30 Jornadas-Persona
	Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual.
	Extensión geográfica superior a 4 CC.AA. o 1 T.I.S. Daños reputacionales a la imagen del país (marca Colombia).
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
ALTO	Afecta a más del 50% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios.
	El incidente precisa para resolverse entre 5 y 10 Jornadas–Persona.
	Impacto económico entre el 0,03% y el 0,07% del P.I.B. actual.
	Extensión geográfica superior a 3 CC.AA.
	Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros. Afecta a más del 20% de los sistemas de la organización.
MEDIO	Interrupción en la presentación del servicio superior al 5% de usuarios. El incidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
	Impacto económico entre el 0,001% y el 0,03% del P.I.B. actual. Extensión geográfica superior a 2 CC.AA.
	Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
BAJO	Afecta a los sistemas de la organización.
	Interrupción de la prestación de un servicio.
	El incidente precisa para resolverse menos de 1 Jornadas-Persona.
	Impacto económico entre el 0,0001% y el 0,001% del P.I.B. actual.
	Extensión geográfica superior a 1 CC.AA
SIN IMPACTO	Daños reputacionales puntuales, sin eco mediático. No hay ningún impacto apreciable.

Fuente: Recuperado el 4 de diciembre de 2022 de: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

6.3.2 Políticas y procedimientos operacionales: Dentro de los aspectos más importantes a implementar y materializar dentro de la creación de un CSIRT hacen parte las políticas y procedimientos operacionales; es así que en atención a tan importante requisito y una vez consultada la documentación que se relaciona con dicho aspecto, se logra evidenciar que la Organización de los Estados Americanos a través de la guía de buenas prácticas para la conformación de un CSIRT, esboza las siguientes políticas y procedimientos operacionales, que hacen referencia a directrices que deben ser acatadas y seguidas por parte del personal en la ejecución de las operaciones y que rigen el funcionamiento y las actividades del centro de respuesta y así garantizar la confidencialidad, la disponibilidad y la integridad de la información y de los recursos del CSIRT, sin dejar de lado la calidad en la prestación de los servicios.

6.3.2.1 Políticas mínimas obligatorias: En primer lugar, se encuentra la política de clasificación de información: Esta política define cómo el CSIRT clasifica la información basada en distintos niveles de criticidad.

Política de protección de datos: Esta política define la forma de proteger la información de acuerdo con su nivel de criticidad.

Política de retención de información: Esta política define el tiempo que el CSIRT debe mantener registros u otra información de que disponga.

Política de protección de destrucción de información: destruye información, registros, medios, dispositivos, etc., para garantizar que la información esté protegida cuando su ciclo de vida o los medios que lo contienen llegan a su fin.

Política de divulgación de información: Esta política debe especificar cómo y cuándo el CSIRT puede compartir o distribuir la información interna o externamente.

Política sobre el acceso a la información: Esta política establece quién puede acceder a la información del CSIRT, teniendo en cuenta el personal, miembros de la comunidad objetivo o el personal de la organización matriz del CSIRT (si lo tiene).

Política de uso apropiado de los sistemas del CSIRT: Esta política define el uso aceptable de los sistemas y recursos del CSIRT.

Definición de incidentes de seguridad y política de eventos: Esta política describe los criterios que determinan la definición de un nuevo evento o incidente de seguridad y la clasificación de cada uno según el tipo y la gravedad.

Política de gestión de incidentes: Esta política debe definir cómo se lleva a cabo la gestión de incidentes, incluyendo el tipo de incidentes a los que el CSIRT responderá, el tiempo de respuesta aceptables, los procedimientos que se van a aplicar, etc.

Política de cooperación: Esta política define las otras entidades con las que cooperará el CSIRT y cómo lo harán, particularmente otros equipos de respuesta a incidentes.

6.3.2.2 Otras políticas: Adicional de las políticas mínimas requeridas para un CSIRT, pueden adicionarse otras con el fin de mejorar la calidad de los servicios y el funcionamiento del centro.

- Política de uso de Internet.
- Política de notificación de incidentes.
- Política de comunicación del CSIRT.
- Política de capacitación y entrenamiento.
- Política de seguridad de computador personal.
- Política de seguridad de la red.
- Política de uso de correo electrónico.
- Política de uso de dispositivos móviles.
- Política de seguridad de equipo de telecomunicaciones.
- Política de copias de seguridad.
- Política de segregación de funciones.
- Política de control de cambio.
- Política de contraseñas.[52]

6.4 CUARTO OBJETIVO

Examinar los estándares internacionales, en donde se establezca la estructura y requerimientos para la creación e implementación de un laboratorio de informática Forense.

Si bien es cierto el objetivo principal de la empresa Cibersecurity de Colombia LTDA, es la creación de un Centro de Respuesta a Incidentes Cibernéticos en el ámbito CSIRT; dentro de la presente propuesta se incluye un componente adicional, que trata sobre la implementación de un laboratorio de informática forense; aspecto de suma relevancia, toda vez que dicho laboratorio entraría a fortalecer el trabajo a realizar en el CSIRT, generando aún más confianza en los clientes de la organización en el entendido que podrán contar con servicios adicionales como el análisis de evidencias digitales entre otros; procedimientos que son imprescindibles en la lucha contra los ataques informáticos y los delitos cibernéticos.

Es importante precisar que a nivel mundial es constante el crecimiento del uso de medios digitales y Colombia no es la excepción, de acuerdo al datos presentados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, entre el año 2010 y 2045, Colombia pasó de tener 200 a 1078 municipios

[52] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

conectados con fibra óptica, con conexiones de internet de 2 Mb a 10.1 Mb, de igual manera se reportó en ese momento un incremento de 67 % de Mipymes conectadas pasando del 7% al 74 %; de igual manera los hogares conectados pasaron del 17% al 50% .

Sumado a lo anterior, se mencionó que los pagos electrónicos en el año 2014 crecieron en un 30 %, los trámites online con el estado se incrementaron en un 400%; un 65 % de ciudadanos interactuaron por medios electrónicos con el estado durante el año 2014, al igual que en ese mismo año el 81 % de empresas interactuaron por medios electrónicos con el estado. [53]

En ese mismo orden, los ataques cibernéticos al igual que los delitos informáticos se incrementan a pasos agigantados; anotando que los delincuentes en la actualidad tienen más acceso a herramientas tecnológicas que no requieren de demasiados conocimientos informáticos y que contribuyen a la comisión de las diferentes actividades delictivas; como consecuencia de este actuar delictivo los cálculos de los daños materiales, económicos y personales son incalculables.

Es así que, al momento de adelantar las investigaciones correspondientes, entra a jugar un papel muy importante la Informática Forense, la cual “se encarga de la aplicación de técnicas científicas y analíticas especializadas en entornos tecnológicos que facilitan la identificación, preservación, análisis y presentación de datos" (Noblett, 2000).

En el ejercicio de esta actividad, se hace necesario el análisis de la evidencia digital que resulta de la comisión de un delito informático o el actuar delictivo relacionado con medios tecnológicos y su consumación, es aquí en donde cobra gran relevancia contar con un laboratorio de Informática Forense en donde se pueda llevar a cabo dichos estudios y análisis, sin dejar de lado que se debe contar con personal idóneo y profesional que desarrolle dicha tarea.

En ese orden de ideas se hace necesario examinar los estándares internacionales, en donde se establece la estructura y requerimientos para la creación e implementación de un laboratorio de Informática Forense, con el fin de ser adecuado en Cibersecurity de Colombia LTDA.

[53] https://sistemas.uniandes.edu.co/images/forosisis/foros/fcs/lunes3Agosto/Ciberseguridadparalagente.pdf

6.4.1 Normas internacionales y nacionales que acreditan un laboratorio de Informática Forense: La Norma ISO 17025 proporciona los requisitos necesarios que deben cumplir los laboratorios de ensayo y calibración, facilitando la congruencia de criterios de calidad; dentro del objetivo principal de la norma, es garantizar la competencia técnica y la fiabilidad de los resultados analíticos con el fin de evaluar factores relevantes a la habilidad de un laboratorio de producir resultados de pruebas y calibración precisos y correctos, en donde se incluyen calificaciones, entrenamiento y experiencia del personal, equipo apropiado, calibrado y mantenido correctamente. Procedimientos adecuados de aseguramiento de la calidad, métodos y procedimientos de pruebas válidos y apropiados, trazabilidad de la medición a normas nacionales, procedimientos apropiados para reportar y registrar resultados, facilidades apropiadas para efectuar pruebas; los anteriores aspectos contribuyen a que un laboratorio sea técnicamente competente para llevar a cabo sus pruebas.[54]

Ahora bien, dentro de los estándares internacionales se encuentra la acreditación ASCLD-LAB (American Society of Crime Laboratory Directors / Laboratory Accreditation Board).
La Junta de Acreditación de Laboratorios de la Sociedad Estadounidense de Delitos, es una organización sin fines de lucro especializada en la acreditación de laboratorios de delitos públicos y privados, desde 1982, contribuyen con el apoyo continuo de la educación y la supervisión de las instalaciones que luchan por la excelencia en el análisis forense, el propósito de la organización es fomentar interés profesionales, ayudar al desarrollo de principios y técnicas de gestión de laboratorio, adquirir, preservar y difundir información forense, mantener y mejorar la comunicación entre los directores de laboratorios de delitos. Es importante tener en cuenta que, si el laboratorio en cuestión no solicite la acreditación, no quiere decir que sea un laboratorio improcedente o que los resultados que arroje no sean confiables.[55]

IAAC (Cooperación Interamericana de Acreditación): La Cooperación Interamericana de Acreditación es una asociación regional de organismos de acreditación y de otras organizaciones interesadas en la evaluación de la conformidad en América. La misión de IAAC es promover la cooperación entre los organismos de acreditación y las partes interesadas en América, enfocada al desarrollo de las estructuras de evaluación de la conformidad para lograr el mejoramiento de productos, procesos y servicios.

La IAAC fue creada en 1996, en Montevideo, Uruguay, y se estableció legalmente en 2001 como una asociación civil de acuerdo a la ley mexicana. IAAC es un organismo no lucrativo que funciona con base en la cooperación de sus miembros y partes interesadas. IAAC obtiene recursos de las cuotas de membresía, contribuciones voluntarias de sus miembros, y aportaciones de proyectos por parte

[54] https://www.icsa.es/laboratorios-analiticos/consultoria-de-laboratorios/norma-iso-17025
[55] https://www.ascld.org/

de organizaciones regionales, como la Organización de Estados Americanos y el PTB de Alemania. Los documentos básicos de IAAC son el Memorándum de Entendimiento y los Estatutos.

Los principales objetivos de IAAC son:

- Promover la aceptación regional e internacional de las acreditaciones otorgadas por sus miembros.

- Promover la aceptación regional e internacional de certificados de conformidad, informes de inspección, y resultados de calibración y pruebas, emitidos por los organismos de evaluación de la conformidad acreditados.

- Desarrollar una infraestructura de acreditación regional y una infraestructura de evaluación de la conformidad eficiente y confiable.

- Establecer un sistema regional de acuerdos de reconocimiento multilaterales entre los organismos de acreditación.

- Facilitar el comercio entre las economías de América a través de un sistema eficiente de evaluación de la conformidad.

- Promover la equivalencia de los programas regionales de acreditación con las guías internacionales de acreditación.[56]

ICONTEC es una organización privada, sin ánimo de lucro, con amplia cobertura internacional; creado en 1963 con el objetivo de responder a las necesidades de los diferentes sectores económicos, a través de servicios que específicos al desarrollo y competitividad de las organizaciones, mediante la confianza que se genera en sus productos y servicios.

La primera institución acreditada por el Organismo Nacional de Acreditación en Colombia (ONAC), busca certificar sistemas de gestión, productos, procesos y servicios. Es importante resaltar que la acreditación otorgada a ICONTEC por ONAC permite ofrecer los servicios de certificación en producto bajo normas técnicas voluntarias en más de 34 sectores económicos.[57]

De igual manera como se mencionará anteriormente se cuenta con el Organismo Nacional de Acreditación de Colombia desde 2008 (ONAC), que es una corporación sin ánimo de lucro, regida por el derecho privado, constituida en 2007 y que por disposición estatutaria se organizó bajo las leyes colombianas dentro del marco del Código Civil y las normas sobre ciencia y tecnología.

[56] https://www.iaac.org.mx/index.php/es/acerca-de-iaac/introduccion
[57] https://www.icontec.org/quienes-somos/

ONAC tiene como objeto principal acreditar la competencia técnica de Organismos de Evaluación de la Conformidad, ejercer como autoridad de monitoreo en buenas prácticas de laboratorio de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y desempeñar las funciones de Organismo Nacional de Acreditación de Colombia.[58]

6.4.2 Implementación de un laboratorio de informática forense:

Esta acción es determinante para garantizar la eficacia del CSIRT razón por la cual debe atender aspectos técnicos e incluso condiciones ambientales que permitan que las labores que se llevarán a cabo en el mismo se puedan realizar de manera adecuada. Por esta razón, aspectos como las condiciones ambientales y de instalaciones adquieren particular relevancia. Aspectos como la fuente de energía a utilizar, el sitio en el que se realizarán las calibraciones y ensayos, su iluminación, deben ser acordes a la labor que se llevará a cabo.

En términos prácticos, debe tratarse de un laboratorio en el que se garantice que las condiciones ambientales no afectarán la valides de los resultados que se obtengan en los análisis ni comprometan los estándares de calidad que deben cumplir las actividades de medición. Vale la pena señalar que frente a la eventual posibilidad de que los muestreos, ensayos y mediciones se realicen en lugares distintos al laboratorio, debe existir un protocolo o estrategia preventiva que genere la misma garantía respecto a los resultados.

En ese orden de ideas, tanto en el laboratorio como en las labores externas, se deben preservar condiciones que impidan que factores como la suciedad, el polvo, la interferencia electromagnética, humedad, estabilidad en el suministro de electricidad, radiación, humedad, ruido, vibraciones, temperatura entre otros, impacten negativamente en los resultados. Ante la posibilidad de que alguno de dichos factores o aquellos semejantes, afecten el análisis, el estudio debe interrumpirse de manera inmediata.

Por otro lado, es importante que se tomen medidas para evitar sucesos negativos para el proceso de análisis como la contaminación cruzada ya que con ello se pueden alterar significativamente los resultados de las actividades de análisis. En ese sentido, debe garantizarse una separación de áreas, especialmente en aquellas en las que se realizan actividades diferentes. Esto implica la necesidad de contar con restricciones de acceso y uso que debe ser limitado al personal autorizado y además debe contar con un protocolo de acción diferenciado acerca de las posibilidades de actuación de cada integrante del equipo.

[58] https://onac.org.co/presentacion

Por supuesto, no se puede pasar por alto la toma de decisiones que garanticen el orden, la limpieza y adecuada disposición de equipos en el laboratorio, lo que demandará incluso, la necesidad de diseñar procedimientos especiales[59].

Tabla 6. Infraestructura interna

Área control de acceso	Área de almacenamiento	Área de análisis	Área mecánica
Ingreso de visitantes	Área de control de acceso y entrada	Zona con acceso a internet	Desmontaje de equipos
Ingreso de personal autorizado (Acceso de forma biométrica, con tarjetas de proximidad entre otros)	Estanterías	Zona sin acceso a internet	Ensamblaje de equipos
	Puertas con cerradura	Hardware forense	Uso de herramientas
	Persona responsable	Software forense	

Fuente: Elaboración propia

Paralelo a lo anterior se deben procurar por que se den una serie de condiciones ambientales relacionadas con aspectos como la interferencia electromagnética, el suministro de energía eléctrica, el ruido y la vibración, la humedad, la refrigeración e incluso los sistemas de extinción de incendios. Ello con el fin de disminuir los riesgos asociados a la infraestructura interna que pueden reducirse mediante la adopción de recomendaciones que disminuyan su impacto y probabilidad de ocurrencia tal y como se ejemplifica en la siguiente tabla:

Tabla 7. Condiciones ambientales recomendables

Condición	Recomendación
Interferencia electromagnética	Protección con Jaula de Faraday
Suministro energía eléctrica	Adquirir UPS, generador eléctrico
Ruido y vibración	Usar materiales aislantes del ruido
Sistema de refrigeración	Mantener la Temperatura 22º C
Humedad	Controlarla para que no supere el 65%
Incendios	Extintores de polvo químico seco, bióxido de carbono, espuma y/o INERGEN

Fuente. Elaboración propia.

Seguridad física: El Laboratorio de Informática Forense debe tener control del acceso a personal no autorizado para poder asegurar la integridad de la información

[59] ICSA, Norma ISO 17025 Requisitos generales para la competencia de los laboratorios de ensayo y calibración, 2019. Recuperado el 29 de noviembre de 2022 de https://www.icsa.es/laboratorios-analiticos/consultoria-de-laboratorios/norma-iso-17025

que se maneja allí, la seguridad física es un elemento fundamental para la estrategia de seguridad global dentro del Laboratorio para así prevenir ataques como:

- Ejecución de código malicioso (por ejemplo, activar un gusano desde el interior del laboratorio).

- Robo de información de seguridad crítica (por ejemplo, material probatorio, segundos originales, cintas de copia de seguridad y diagramas de red). Como parte de la estrategia de administración de riesgos, debe determinar el nivel de seguridad física apropiado para su entorno.

A continuación, se describen las medidas mínimas de seguridad física a tomar:

a) Establecer seguridad física para todas las áreas del edificio (esto puede incluir tarjetas de acceso, dispositivos biométricos y guardias de seguridad).

b) Requerir a los visitantes que vayan acompañados en todo momento.

c) Requerir a los visitantes que firmen un registro de entrada de todos los dispositivos informáticos.

d) Requerir a todos los integrantes del Laboratorio que registren cualquier dispositivo portátil de su propiedad.

e) Fijar físicamente todos los equipos de sobremesa y portátiles a las mesas.

f) Requerir que se registren todos los dispositivos de almacenamiento de datos antes de sacarlos del laboratorio.

g) Ubicar los servidores en salas separadas a las que sólo tengan acceso los administradores.

h) Conexiones a Internet, alimentación, sistemas antiincendios, etc.

i) Protección contra desastres naturales y ataques terroristas.

j) Establecer seguridad para las áreas en las que se puede dar un ataque por denegación de servicio (por ejemplo, las áreas en las que el cableado sale del Laboratorio).

k) Se debe contar con un sistema adicional de suministro de energía (UPS).

Todo lo anterior implica la necesidad de especificar los procedimientos y métodos que se deben aplicar en cada uno de los ensayos y calibraciones que se realicen en el laboratorio. Por supuesto, no se trata de una determinación general, sino del establecimiento de una ruta de actuación concreta para cada una de las actividades

que allí se desarrollan (manipulación, muestreo, almacenamiento, transporte, preparación de ítems, entre otros), incluso, resulta sumamente valioso que estimen aspectos como las técnicas estadísticas que se utilizaran al momento de analizar los datos y un estimativo de la incertidumbre que se pueda presentar en el marco de las mediciones.

De lo anterior se desprende la importancia de las instrucciones que deben ser una constante en el laboratorio. Estas deben diseñarse tanto para las actividades que impliquen el uso y puesta en funcionamiento de equipos, como las actividades de preparación y manipulación de los ítems que se someterán a estudio.

Procedimientos del Laboratorio de Informática Forense

Continuando con los procedimientos, se procede a señalar las diferentes actividades que actualmente se realizan en los Laboratorios de Informática Forense.

- Análisis técnico factico.
- Identificar de los medios de almacenamiento implicado en la investigación.
- Inicio de la conservación de la evidencia digital.
- Adquisición de imágenes forenses.
- Análisis a imágenes forenses.
- Recolección de datos volátiles.
- Extracción de información a equipos terminales móviles.
- Análisis de código malicioso.
- Análisis a bases de datos.
- Captura de los medios almacenamientos originales.
- Volcado de las imágenes forense en el laboratorio.
- Recuperación de datos borrados y de ambiente.
- Filtrado y análisis de documentos relevantes.
- Identificar y extracción de las pruebas.
- Reconstrucción de la cadena de acontecimientos.

- Presentación de resultados, elaboración del informe final o base opinión pericial a quien corresponda.

- **Equipos.**

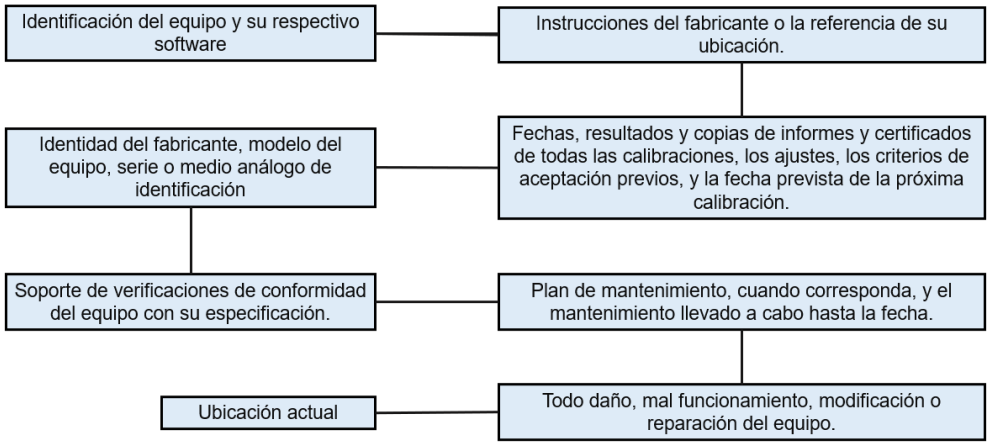
Este es otro factor que requiere la mayor cualificación pues no de otro modo se garantiza la eficacia del laboratorio. En procura de ello, éste debe proveerse con equipos apropiados de medición, ensayo y muestreo, los cuales deben obedecer a estándares de calidad definidos en normas internacionales, requerimiento que debe suplirse incluso en aquellos eventos en los que las circunstancias hagan que el laboratorio se apoye en equipos externos sobre los cuales no tenga permanente control.

Sí algo fortalece lo anterior es que por la naturaleza de la labor que cumple el laboratorio cada uno de los procedimientos que allí se realicen deben procurar el nivel máximo de exactitud tanto en el muestro, los ensayos y desde luego en las calibraciones. Esto implica que tanto el software como los equipos que se utilicen para efectuar dichas actividades, cumplan las especificaciones técnicas requeridas para dicho propósito. En el mismo sentido, cuando los valores o magnitudes de los instrumentos comprometan o afecten de manera significativa los resultados, se deben efectuar los programas de calibración correspondientes. A dichos requerimientos, se suma el que se debe suplir previo a la utilización de dichos equipos, esto es, el de efectuar el protocolo de calibración correspondiente pues gracias a este se garantiza que la exactitud de las pruebas e incluso se disminuyen las posibilidades de que los resultados sean objeto de controversia en contextos como los procedimientos judiciales.

El talento humano encargado de la operación de los equipos a los que se ha venido haciendo referencia debe ser idóneo y desde luego, debe contar con las debidas autorizaciones. Dicho en otras palabras, debe ser personal que cuente con los conocimientos técnicos, debidamente certificados, sobre el uso de los equipos y la interpretación de resultados. Gregariamente, este personal debe tener acceso, al momento del procedimiento, a todos aquellos documentos técnicos de soporte tales como manuales de instrucciones, de mantenimiento y/o de operación según sea el caso.

La identificación del software y del equipo tiene también una especial relevancia en los procesos que se desarrollan en el laboratorio. En razón a ello, dichos dispositivos deben contar con una identificación que garantice su univocidad. Complementariamente deben existir registros de la totalidad de los componentes de software y equipamiento. En la tabla que se presenta a continuación se relacionan los elementos o requerimientos que deben suplirse al momento de ubicar cada uno de estos registros:

Figura 8. Contenido de los registros de software y equipo



Fuente: Elaboración propia

Las previsiones deben extenderse en todas las demás etapas del proceso. De esta manera, deben orientarse a garantizar aspectos como la manipulación, el almacenamiento, transporte, mantenimiento y uso de equipos. Cada uno de dichos momentos deben garantizar tanto la seguridad de las personas y de los equipos, como un funcionamiento adecuado, sin descontar que deben dirigirse también a prevenir el deterioro precoz o la contaminación de los equipos. Se itera que el uso de equipos de medición en exteriores o en otras dependencias diferentes al laboratorio, implica también la determinación de medidas de seguridad previas. Por esta razón, no se puede perder de vista la posibilidad de disponer procedimientos adicionales para dichos eventos.

Eventualmente se debe tomar la decisión de poner fuera de servicio o dar de baja los equipos privilegiando con ello las garantías que debe ofrecer el laboratorio. Por regla general, se trata de una determinación que procede en aquellos eventos en los que el equipo ha sufrido el impacto de una sobre carga o los efectos negativos de un uso inadecuado. Lo propio ocurre cuando se acredite que los equipos son defectuosos, o no se encuentran en el marco de los límites en punto a las especificaciones que deben cumplir.

Lo anterior implica el aislamiento y rotulación del equipo utilizando marcas visibles y legibles que den cuenta de que se trata de medios que se han dejado fuera de servicio. Dichas medidas deben ser permanentes y solo se podrán suprimir cuando se han cumplido los procedimientos de reparación y cuando las respectivas calibraciones o ensayos den fe de que se han restablecido al punto de tener garantía sobre su adecuado funcionamiento. En todo caso, el laboratorio realizará el examen de lo anterior dando aplicación al procedimiento de control de trabajo no conforme.

El procedimiento de rotulación debe aplicarse a todos los equipos que necesiten ser calibrados. Dicha actividad debe convertirse en una herramienta para determinar el estado de calibración del equipo, la fecha en que este procedimiento se realizó por última vez y la fecha futura en la que se deba realizar nuevamente.

Las verificaciones intermedias que eventualmente deban realizarse como garantía de confianza de los equipos y su estado de calibración, también debe contar con un protocolo o procedimiento delimitado previamente. Por otro lado. las calibraciones den lugar a un conjunto de factores de corrección, el laboratorio debe tener procedimientos para asegurarse de que las copias (por ejemplo, en el software), se actualizan correctamente.

Se deben proteger los equipos de ensayo y de calibración, tanto el hardware como el software, contra ajustes que pudieran invalidar los resultados de los ensayos y/o de las calibraciones.

Por otra parte, existen varias herramientas de software usadas en el análisis forense digital, a continuación, se señalan algunas herramientas y sus características.

FTK (Forensic toolkit): Es una plataforma de investigaciones digitales aprobada por tribunales, que está diseñada para ser veloz, analítica y contar con escalabilidad de clase empresarial. Conocida por su interfaz intuitiva, el análisis de correo electrónico, las vistas personalizadas de datos y su estabilidad, FTK establece el marco para una expansión sin problemas, por lo que su solución de informática forense puede crecer de acuerdo con las necesidades de su organización. Adicionalmente, AccessData ofrece nuevos módulos de expansión, entregando el primer software de esta industria con capacidad de análisis y con visualización de última generación. Estos módulos se integran con FTK para crear la plataforma de informática forense más completa en el mercado.

ENCASE (Encase Forensic): es una herramienta usada en la investigación digital por los profesionales forenses que necesitan llevar a cabo la recolección eficiente de datos y las investigaciones mediante un proceso automatizado y comprensible. Dentro de los objetivos del software se encuentras los siguientes:

- Proporcionar a los examinadores la mayor eficiencia, potencia y resultados. Este software es aceptado por las cortes y permite.

- Adquirir datos de la más amplia variedad de dispositivos.

- Mostrar las posibles pruebas con el análisis forense a nivel de disco.

- Producir informes detallados sobre los hallazgos realizados.

- Mantener la integridad de la evidencia en un formato de confianza ante los tribunales.

Los beneficios que tiene la herramienta es buscar, analizar e informar sobre las posibles pruebas de manera rápida además de adquirir y analizar los datos en una amplia variedad de ordenadores, teléfonos inteligentes y tabletas, descubrir las pruebas potenciales por medio de búsqueda avanzadas, aumenta la productividad mediante la pre visualización de los resultados a medida que se adquieren datos, una vez que se crean los archivos de imagen, se puede buscar y analizar varias unidades o los medios de comunicación de forma simultánea. Adicional a eso permite preservar la integridad de la evidencia con la creación de imágenes de discos en los formatos L01 y E01.

SECURE VIEW 3: herramienta desarrollada por la firma Susteen, la cual permite realizar análisis forense a dispositivos móviles como Iphone, Android, Blackberry, entre otros.

CERBERUS: Es una tecnología de clasificación de malware que está disponible como accesorio para FTK 4. El primer paso hacia la ingeniería inversa automatizada. Cerberus califica las amenazas y hace un análisis de desmontaje para determinar tanto el comportamiento como la intención de binarios sospechosos.

Visualización: Vista de datos en varios formatos, incluyendo líneas de tiempo, gráficas de clúster, gráficas circulares y más. Permite determinar rápidamente las relaciones en los datos, encontrar piezas claves de información y generar informes de fácil comprensión por los abogados, los Oficiales de Información (CIOs) u otros investigadores.

Algunas herramientas especiales para equipos móviles son:

UFED 4PC: es la solución de software de análisis forense de dispositivos móviles de Cellebrite, el cual está diseñado para entidades que requieren extracción lógica, económica rápida y simplificada para analizar datos probatorios de una amplia variedad de dispositivos móviles como (teléfonos antiguos, comunes, inteligentes tablets entre otros). La ventaja es que puede instalarse en cualquier PC basada en Windows, también brinda las herramientas necesarias para extraer rápidamente los datos de una memoria SIM y de la memoria del teléfono en forma adecuada.

XRY COMPLETE: Es el sistema integral de análisis forenses de móviles de Micro Systemation; una combinación de nuestras dos soluciones lógicas y físicas en un solo paquete. XRY completa permite a los investigadores el acceso completo a todos los métodos posibles para recuperar los datos desde un dispositivo móvil. XRY es un software que se diseñó especialmente para análisis forense móvil basado en Windows, que incluye todo el hardware necesario para la recuperación de datos de los dispositivos móviles, de una manera segura en el ámbito forense. Con XRY Complete puede lograr más y profundizar en un dispositivo móvil al detalle para recuperar datos vitales. Con una combinación de herramientas de análisis

lógicos y físicos disponibles para los dispositivos compatibles; XRY complete puede crear informes combinados los cuales pueden contener datos actuales y eliminados de que proceden de la misma terminal.

FTK IMAGER: Permite montar prácticamente todo tipo de formatos de imagen forenses habituales, como Encase, SnapBack, Safeback, Expert Witness, Linux DD, ICS, Ghost, SMART, Access Data Logical Image y Advanced Forensics Format (AFF), con un soporte 105 muy extenso para sistemas de ficheros de unidades ópticas, discos duros cifrados y sistemas de fichero de disco. Para la elección final del software que se va a usar en el laboratorio de Informática Forense se tuvo en cuenta, además de los requerimientos da cada equipo, las características en el costo de las licencias, pues al estar acreditadas proporcionan una mayor confianza ante las autoridades judiciales. Por tal motivo se escogieron ENCASE y FTK, ambas son muy completas y lo que quizá falte en una, se complementa con la otra.[60]

Responsable Laboratorio Forense:

Dentro del propósito principal del responsable del laboratorio de Informática Forense, se encuentra la de administrar el laboratorio con el fin de ofrecer productos técnicos científicos que apoyen adecuadamente los objetivos de la organización, de acuerdo con la normativa vigente. Dentro de sus funciones se pueden enumerar las siguientes:

- Verificar la capacidad instalada del laboratorio para el apoyo eficiente en la prestación del servicio, de acuerdo con la normativa vigente.

- Supervisar las actividades desarrolladas por los peritos que conlleven a la efectiva ejecución de los procedimientos establecidos.

- Verificar la entrega oportuna de los productos siguiendo los estándares establecidos.

- Realizar seguimiento a las obligaciones contraídas mediante los convenios de cooperación, apoyo, ayuda y asistencia técnica, para el cumplimiento de los compromisos acordados.

- Analizar las nuevas herramientas tecnológicas que permitan la mejora continua de los procedimientos que se desarrollan en el laboratorio, de acuerdo a la normativa vigente.

[60] http://repositorio.ucp.edu.co/bitstream/10785/3653/1/CDMIST92.pdf

CONCLUSIONES

Mediante la elaboración del presente proyecto se logra evidenciar que, con relación a la creación de un CSIRT, se cuenta con buen insumo referencial, en el entendido que es un tema de actualidad y de gran importancia, no solamente para los gobiernos y el sector privado, sino de igual manera para las organizaciones que pretenden proteger sus activos.

Se logró proyectar la hoja de ruta para la creación del diseño documental para la creación y puesta en marcha de un Centro de Respuesta ante Incidentes Cibernéticos en el ámbito CSIRT, al interior de la empresa Cibersecurity de Colombia LTDA.

A través de la investigación realizada, se analizó información y normatividad vigente que permiten orientar y materializar la creación de un CSIRT, en cualquier ámbito en donde exista la necesidad de contrarrestar la cibercriminalidad y permitir que los clientes asistidos cuenten con un organismo que cubre sus requerimientos, logrando establecer las políticas y procedimientos operacionales del centro, al igual que la taxonomía de los incidentes de seguridad informática.

Se establecieron diferentes estándares nacionales e internacionales que contribuyen a la acreditación de un laboratorio de Informática Forense con el objetivo de implementar uno en Cibersecurity de Colombia LTDA, señalando los diferentes requerimientos que se exigen para ponerlo en marcha.

RECOMENDACIONES

Seguir las orientaciones brindadas por la normatividad vigente nacional e internacional y las guías que dan cuenta sobre la creación de un CSIRT; de tal forma que se conviertan en un instrumento eficaz, permitiendo la consolidación del CSIRT para la empresa Cibersecurity de Colombia LTDA; realizando los ajustes necesarios que compaginen con las pretensiones y el objeto de negocio de Cibersecurity de Colombia LTDA.

Ajustar el diseño documental para el funcionamiento del CSIRT en Cibersecurity de Colombia LTDA, a las directrices establecidas en las guías de ámbito internacional, que orientan de manera acertada los parámetros que deben ser tenido en cuenta en la consecución de un CSIRT.

Implementar el laboratorio de Informática Forense en la empresa Cibersecurity de Colombia LTDA, siguiendo las pautas establecidas en la normatividad que rige dicho procedimiento, teniendo en cuenta las buenas prácticas.

BIBLIOGRAFÍA

BAUTISTA GARCÍA, Fredy. Comportamiento del ciberdelito en Colombia durante el 2021. En CCIT, Cibercrimen 2021-2022. Nuevas amenazas al comercio electrónico. Bogotá: Crowdstrike – Fortinet. 2021. PP. 15-24. {En línea}. {12 de noviembre de 2022} disponible en: (https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf)

CARNEGIE MELLON UNIVERSITY. Authorized Users of CERT, 2014. {En línea}. {14 de diciembre de 2022} disponible en: (https://resources.sei.cmu.edu/asset_files/Brochure/2014_015_001_310282.pdf)

CCN-CERT. Red CERT, 2007. Garantía de seguridad en todo el mundo. Revista Auditoría y Seguridad (12), 50-52. {En línea}. {14 de diciembre de 2022}, disponible en: (https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/658-red-cert-garantia-de-seguridad-en-todo-el-mundo/file.html)

CENTRO CRIPTOLÓGICO NACIONAL. Guía de creación de un CERT/CSIRT, 2011. {En línea} {22 de noviembre de 2022} disponible en: (https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf)

CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA. Qué es un incidente, 2018. {En línea}. {6 de diciembre de 2022} disponible en: (https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-un-incidente)

CIBERNEWS. Quien fue el primer hacker de la historia, 2022. {En línea}. {14 de diciembre de 2022}, disponible en: (https://www.youtube.com/shorts/96zYW4lk2Fs)

CONSEJO DE EUROPA. Convenio sobre la Ciberdelincuencia, 2001. {En línea}. {14 de diciembre de 2022} disponible en: (https://www.oas.org/juridico/english/cyb_pry_convenio.pdf)

COLOMBIA. CONSTITUCIÓN POLÍTICA DE COLOMBIA. Asamblea Nacional Constituyente 20 de julio de 1991.

CRC. Resolución 2258, 2009. {En línea}. {12 de diciembre de 2022}, disponible en: (https://www.crcom.gov.co/sites/default/files/normatividad/00002258.pdf)

DNP. Documento CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa, 2016. {En línea}. {2 de diciembre de 2022} disponible en: (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf)

DNP. Documento CONPES 3854 Política Nacional de Seguridad Digital, 2016. {En línea}. {3 de diciembre de 2022} disponible en: (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf)

DNP. Documento CONPES 3995 Política Nacional de Confianza y Seguridad Digital, 2020. {En línea}. {4 de diciembre de 2022} disponible en: (https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf)

FERNÁNDEZ RIQUELME, Sergio. El delito como identidad social. Reflexiones sobre la comunidad y su proceso de integración. La Razón Histórica. Revista hispanoamericana de historia de las ideas (35), 1-19, 2017. {En línea}. {29 de noviembre de 2022} disponible en: (https://digitum.um.es/digitum/bitstream/10201/55827/3/Sergio%20Fern%c3%a1ndez%20Riquelme.%20El%20delito%20como%20Identidad%20social.%20LRH%2035.pdf)

GRUPO ICA. Los 9 tipos de ciberataque que deberías conocer, 2019. {En línea}. {14 de diciembre de 2022} disponible en: (https://www.grupoica.com/blog/-/blogs/9-tipos-ciberataque-debes-conocer)

ICSA. Norma ISO 17025 Requisitos generales para la competencia de los laboratorios de ensayo y calibración, 2019. {En línea}. {29 de noviembre de 2022} disponible en: (https://www.icsa.es/laboratorios-analiticos/consultoria-de-laboratorios/norma-iso-17025)

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, Enero, 2009) Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado-denominado “de la protección de la información y de los datos”. Bogotá D.C., 2009

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (30, Julio, 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. Bogotá D.C., 2009. No. 47426

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581. (17, Octubre, 2012) Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C., 2012. No. 48587

MINTIC. Guía para la gestión y clasificación de los incidentes de seguridad de la información, 2016. {En línea}. {5 de diciembre de 2022} disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

NACIONES UNIDAS. Convención de las Naciones Unidas contra la delincuencia organizada transnacional, 2000. {En línea}. {13 de diciembre de 2022} disponible en:(https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf)

OEA. Buenas prácticas para establecer un CSIRT nacional, 2016. {En línea}, {9 de diciembre de 2022} disponible en: (https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf)

UNIÓN EUROPEA. Equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la Unión Europea (CERT-EU), 2019. {En línea}, {14 de diciembre de 2022} disponible en: (https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_es)

URIBE RAYAS, Edgar Felipe. Proceso para la definición de servicios iniciales en un equipo de respuesta ante incidencias de seguridad informática (CSIRT), 2014. {En línea}, {14 de diciembre de 2022} disponible en: (https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/437/1/ZACTE42.pdf)