DISEÑO DOCUMENTAL PARA LA CREACION DEL CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS DE LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

JOSE DE LOS REYES DIAZ PADILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

DISEÑO DOCUMENTAL PARA LA CREACION DEL CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS DE LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

JOSE DE LOS REYES DIAZ PADILLA

Ing Fernando Zambrano Hernández

Director Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA

2021

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, Marzo de 2021

DEDICATORIA

Dedico el trabajo de esta tesis a Dios como fuerza principal que me motiva para valorar cada momento de sacrificio y dedicación que requirió este proceso de formación académica y profesional y a mis padres.

AGRADECIMIENTOS

A mi madre quien me apoyo todo el tiempo, convirtiéndose en ese motor que le da vida a mis ideales, su constancia, su sacrificio, sus oraciones, buenos deseos y consejos; permitieron que no me desanimara cuando pensaba que me iba a rendir.

A mí querido padre, ese guerrero incansable, luchador y buen amigo, que hoy no se encuentra físicamente pero que está siempre conmigo en cada momento, en cada circunstancia, en cada decisión que tomo, por medio de sus frases y consejos que me ayudan a ser un hombre de bien con principios y valores.

A mi compañera sentimental que a pesar de todo se mantuvo a mi lado en este proceso, sin importar los desacuerdos que pudimos tener por el sacrificio de tiempo y espacio familiar que requería mi formación.

A mí querida hija Isabella, que se convirtió en el pilar fundamental y en mi fuerza del día a día para no desvanecer en este camino.

A cada uno de los tutores que hizo parte de mi proceso de formación y quienes con su conocimiento guiaron y orientaron mis objetivos como profesional idóneo y capacitado para afrontar los desafíos en mi profesión y vida.

José De los Reyes Díaz Padilla.

TABLA DE CONTENIDO

LISTA DE TABLAS

GLOSARIO

AMENAZAS: Son las causas que se consideran potencial para generar un incidente no deseado, provocando daños en los sistemas[1].

ANTIVIRUS: Es un software que tiene como finalidad proteger el sistema operativo de los virus, supervisa en tiempo real eliminando o dejando en cuarentena el malware detectado[2].

EXPLOITS: Son programas intrusos que se valen de las brechas de seguridad de los sistemas, utilizando técnicas para atacar la red evadiendo las seguridades[3].

FIREWALL: Es un sistema de seguridad que tiene como función bloquear todo el tráfico malicioso en la red que se instala, mediante el bloqueo de puertos protege las conexiones no autorizadas a la red[4].

INGENIERÍA SOCIAL: Es una metodología que utiliza técnicas de engaño, su función es engañar al eslabón más débil que es el usuario para poder tomar acceso al sistema, unas de las técnicas que utiliza es el phishing el cual consiste en enviar correos spam, esperando que la víctima acceda al link que conlleva a la instalación de un malware que permite el control del equipo al atacante[5].

MALWARE: Son todos los programas informáticos que tienen la función de dañar el equipo tanto en software como hardware, entre ellos encontramos los virus, troyanos y gusanos. Su forma de reproducción es por medio de internet, USB, correos entre otros[6].

---

[1] Guía para la Implementación de Seguridad de la Información en una MIPYME. [En línea]. Bogotá: MINTIC. 2016., 31 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf.
[2] Ibíd. p. 6
[3] Ibíd. p. 8
[4] Ibíd., p. 9
[5] BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia. Facultad de educación, 2015. 116 p
[6] Ibíd. p. 17

RESUMEN

Los cambios tecnológicos que se han desarrollado en los últimos años en todo el mundo, han hecho que se haga necesario estar a la vanguardia de esta nueva era digital, creando la necesidad de acceder al ciberespacio y con ella simultáneamente la alternativa de vulneración de la información por parte de aquellas personas que solo esperan una oportunidad para realizar ataques cibernéticos y apropiarse o manipular la información privada.

Es por esto que Colombia, ha creado lineamientos y políticas de ciberseguridad para que se haga uso adecuado del entorno digital por medio de los documentos CONPES 3701 de 2011 y CONPES 3854 de 2016; a esto se le suma la labor del Ministerio de Tecnologías de la Información y Comunicación por medio de investigaciones que analizan el estado actual de los sectores que son afectados por ataques cibernéticos e incidentes informáticos.

El presente trabajo bajo proyecto aplicado, deja a consideración la creación de una empresa que preste los servicios de centro de respuestas a las del distrito capital de Colombia para que puedan prevenir y atacar los incidentes cibernéticos.

Palabras claves: Amenazas, cibernéticos, cibercrimen, incidentes, malware firewall, phishing**.**

ABSTRACT

The technological changes that have developed in recent years around the world have made it necessary to be at the forefront of this new digital era, creating the need to access cyberspace and with it simultaneously the alternative of information breach by those people who just wait for an opportunity to carry out cyber attacks and appropriate or manipulate private information.

For this reason Colombia has created cybersecurity guidelines and policies so that proper use of the digital environment is made through documents CONPES 3701 of 2011 and CONPES 3854 of 2016; To this is added the work of the Ministry of Information and Communication Technologies through investigations that analyze the current state of the sectors that are affected by cyber attacks and computer incidents.

The present work under applied project, leaves to consideration the creation of a company that gives the services of center of answers to those of the capital district of Colombia so that they can prevent and attack the cybernetic incidents.

Keywords: Threats, cybernetics, cybercrime, incidents, malware firewall, phishing**.**

1 INTRODUCCION

El dar respuesta a los diferentes incidentes de seguridad informática, resulta una labor un poco complicada para las empresas que han sido víctimas, haciéndoles necesario el implementar una serie de lineamientos y actividades que se demandan en Colombia para el manejo de datos y que tengan la capacidad de prevenir y resolver los eventos inesperados que afectan a los activos de información en las organizaciones.

El presente trabajo analiza el proceso de Diseño de un Centro de Respuesta a Incidentes Cibernéticos para la puesta en marcha de un CSIRT en la empresa **Cibersecurity de Colombia Ltda.**, lo cual incluye diferentes criterios y consideraciones, que se requieren para definir su constitución, un plan estratégico, misión, visión, políticas organizacionales, portafolio de servicios, mapa de procesos, definición del organigrama, manual de funciones, así como también sus aspectos legales y jurídicos.

Con el fin de que la documentación diseñada en la presente propuesta, describa los parámetros y procedimientos para que el CSIRT pueda gestionar las funciones de respuestas a incidentes cibernéticos, ofreciendo servicios de soporte a respuestas de incidentes cibernéticos o gestión a vulnerabilidades.

Para el diseño documental se tienen en cuenta los requerimientos mínimos solicitados, donde se debe definir el ámbito de actuación del CSIRT, taxonomía de ataques relevantes, tipos de servicios reactivos y proactivos, requisitos y perfiles del equipo de trabajo, así como también las políticas y procedimientos operacionales; para con todo esto, definir la estructura orgánica sugerida para el CSIRT.

También se aconseja que para cumplir de manera eficiente las funciones, un CSIRT debería contar con un laboratorio de investigación de las nuevas amenazas[7], así como brindar capacitación técnica constante al personal que lo conforma.

Es importante resaltar que uno de las principales limitantes para la creación de un CSIRT es el presupuesto. Los altos costos son el principal impedimento en las pequeñas y medianas empresas (PyMEs) a la hora de crear un CSIRT propio o contratar los servicios que estos prestan.

No queriendo decir que las empresas no puedan dar el primer paso, iniciando por la elaboración del plan de negocios, la creación de manuales operativos y organizacionales que les permita garantizar que el personal cuente con el conocimiento acerca de cómo atender incidencias, y les ayude a minimizar costos por la necesidad de contratar personal especializado fijo para desempeñar este tipo de labor.

[7] WELIVESECURITY. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [en línea]. 2015. [Citado 13-septiembre-2018]. Disponible en https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

2 PLANTEAMIENTO DEL PROBLEMA

ANTECEDENTES

Nace del requerimiento especifico por parte de la empresa **Cibersecurity de Colombia LTDA**, empresa colombiana que presta servicios de seguridad para la protección de la información; la cual tiene como propósito consolidarse en un Centro de Respuestas a incidentes cibernéticos que brinde soluciones a las demandas de clientes que son víctimas de incidentes cibernéticos en el país.

Es por esto, que se elaboró el Diseño del Centro de Respuesta a incidentes Cibernéticos, la cual contiene la descripción de los requerimientos necesarios.

El centro de respuestas a incidentes cibernéticos nace de la necesidad que tienen las empresas a nivel nacional e internacional después de un ciberataque, daño que no solo se refleja en lo económico y productivo, sino en la reputación y hasta en temas legales por la pérdida de información confidencial lo que conlleva a perder confiabilidad en los clientes actuales y los potenciales a tener.

De acuerdo al estudio Tendencias del Cibercrimen 2019-2020, presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial, presenta “las cifras y modalidades de los ciberdelitos en 2019 y las tendencias que enfrentaran las empresas Colombianas y los ciudadanos en 2020”[8], el estudio publica los datos más relevantes e identifica los delitos más denunciados en Colombia a saber:

1. El hurto por medios informáticos: con un total de 31058 casos, los delincuentes saben que lo potencial para ellos está en las cuentas bancarias.

[8] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT, TicTac, Programa SAFE. Tendecias cibercrimen en Colombia 2019-2020. 2019., 5 p. [Citado 24-abril-2020]. Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

2. Violación de datos personales: 8037 casos que demuestran que Colombia es vulnerable al robo de identidad.
3. Acceso abusivo a sistema informático: con 7994 casos, el cibercriminal compromete los sistemas informáticos ganándose el acceso al mismo.
4. La transferencia no consentida de activos: 3425 casos nos avisan que esto solo les facilita a los delincuentes los robos y transferencias de cantidades de dinero de manera fácil.
5. Uso de software malicioso: 2387 casos representan los denuncios por parte de las personas que se encuentran amenazados por este tipo de delito.

El mismo estudio informa que el 45% de las denuncias de los ciberdelitos se realizan a través de la aplicación a denunciar, plataforma virtual que permite realizar la acción correspondiente para que las autoridades den comienzo a la investigación pertinente.

De acuerdo a los resultados del anterior estudio, se buscó que la empresa Cibersecurity de Colombia LTDA pueda crear un Centro de Respuesta a Incidentes Cibernéticos que ofrezca alternativas de solución a las grandes, medianas y pequeñas empresas, contribuyendo a la protección de la información por medio de un equipo de trabajo, que brinde seguridad, confianza, y protección a las empresas que han sido afectadas por ataques cibernéticos y a aquellas que aún no han sido atacadas, pero quieren evitar este tipo de amenazas.

Lo cual hace que surja la pregunta:

¿Cómo el diseño documental de un centro de respuesta de incidentes informáticos contribuye en la creación y pautas para dar desarrollo a los servicios propuestos por la empresa Cibersecurity de Colombia LTDA con el fin de brindar servicios que favorezca el entorno digital de las Empresas?

3 JUSTIFICACIÓN

Uno de los inventos de la humanidad en el último siglo que han permitido la evolución y el desarrollo, es sin ninguna duda la tecnología, la cual ha mejorado la calidad de vida del ser humano presentándole un sin número de herramientas que al ser utilizadas pueden cambiar la sociedad, es innegable que la tecnología de la información seguirá reestructurando el mundo en formas difíciles de adivinar[9].

Es necesario mencionar que la información, son el activo más importante para las empresas al igual que el talento humano, su protección se convierte en un proceso fundamental, que puede significar el triunfo o fracaso de la entidad que busca sostenibilidad y crecimiento[10], por ello es crucial aplicar normas de seguridad adecuada para la protección de los datos, teniendo en cuenta los posibles ciberataques e identificando las técnicas que se aplican para sustraer información confidencial[11] .

La empresa Cibersecurity de Colombia LTDA**.**, por medio de la implementación de un CSIRT busca solucionar los problemas de incidentes cibernéticos que se presenten en las empresas, a través de los informes encontrados se confirma la utilidad de diseñar una entidad que a través de los servicios de asesoría genere una cultura en seguridad informática, previniendo futuros ciberataques, así mismo que brinde el servicio de respuesta de incidente y recuperación de información.

Al identificar, cuáles son las técnicas que más se aplican para sustraer la información de las empresas, se hace determinante capacitar al talento humano para que tengan claro cuán importante es la seguridad de los activos informáticos y brinden la relevancia que esta se merece, Cibersecurity de Colombia LTDA deberá analizar cuál es el personal más vulnerable, evaluando su conocimiento sobre que

[9] EL TIEMPO. Tecnologías evolución y futuro [en línea]. Bogotá: 2018. Disponible en https://m.eltiempo.com/archivo/documento/MAM-219859

[10] COHEN KAREN, Daniel. Importancia de la información para las empresas [En Línea]. Argentina: 2018. Disponible en https://www.grandespymes.com.ar/2014/10/03/importancia-de-la-informacion-para-las-empresas/

[11] HANSEN, Denis. SAVE Social Vulnerability & Assessment Framework [en Línea]. 2017., 42-49 p. Disponible en http://www.fak.dk/publikationer/Documents/Project%20SAVE.pdf

son los incidentes de seguridad informática; la propuesta de este trabajo no es novedosa pero si puede ser muy efectiva a la hora de presentar a las empresas el portafolio de servicios ya que por medio de la implementación del CSIRT se busca ofrecer un centro de respuestas a incidentes cibernéticos con personal calificado que coordinen normas jurídicas y garanticen la protección de datos que pueden ser tratados como evidencias digitales.

Así mismo Cibersecurity de Colombia LTDA contribuirá en conocimiento para el cliente en el manejo de los conceptos técnicos con el fin de preparase a futuro para situaciones que requieran pronta solución, con esto se busca que el cliente pueda resolver situaciones sin hacer requerimientos innecesariamente lo cual minimizará el impacto y todo el esfuerzo que se tiene al ser víctimas del cibercrimen, ayudando al ahorro de costos dentro de la empresa.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar la documentación requerida para la implementación de un Centro de Respuesta a Incidentes Cibernéticos de la Empresa Cibersecurity de Colombia LTDA

4.2 OBJETIVOS ESPECIFICOS

Identificar el ámbito de actuación y los documentos de constitución que darán soporte legal a las actividades del CSIRT

Estructurar los perfiles y funciones que conformarán el CSIRT los cuales serán los encargados de dar respuesta a los servicios propuestos

Definir los servicios, las políticas y el código de ética que permitirán dar desarrollo a las actividades del CSIRT los cuales darán respuesta a las necesidades presentadas por las partes interesadas o comunidades objetivo.

Establecer los recursos financieros y la estructura tecnológica que dará soporte a las acciones del equipo de respuesta

5 MARCO TEORICO

Las empresas grandes, medianas o pequeñas, tienen algo en común y es que buscan la seguridad y la protección de sus activos informáticos, saben muy bien que son parte fundamental de su patrimonio, cuidan que los equipos que tienen en sus instalaciones cuenten con programas que les proporcione un alto grado de seguridad, teniendo muy poco en cuenta, que los software son controlados por seres humanos que al no ser capacitados se convierten en un blanco de los cibercriminales en seguridad informática.

El CSIRT es un centro de respuestas ante incidentes informáticos, quienes buscan que las empresas puedan volver a sus operaciones de forma normal, actuando desde el momento que un riesgo se presente para así reducir las secuelas con el menor impacto posible. De acuerdo a las buenas prácticas de un CSIRT, el modelo incluye temas como: los procesos legales, de planificación financiera, de gestión de los recursos humanos, la adquisición de activos informáticos, la gestión y supervisión de los proyectos de tecnología, entre otros de tipo administrativos, también se debe tener en cuenta los lineamientos que sugiere el gobierno nacional en nuestro caso Colombia, frente a las estructuras de los equipos de respuesta a los incidentes de seguridad de la información y la guía para la creación de un CERT o CSIRT[12] .

Para poder hablar del Centro de respuestas a incidentes cibernéticos, hay que entender ciclas y conceptos que son trascendentales, hacen parte de la seguridad de la información y se debe tener en cuenta como lo son:

[12] (ENS), Guía de creación de un CERT/CSIRT. Se recuperó en septiembre de 2011 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-sep11.pdf (Ens, 2011)

CERT: (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas. (Universidad Carnegie – Mellon)[13]

Ciberdefensa: Capacidad del Estado[14] para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberdelincuencia: Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia)[15]

Ciberdelito / Delito Cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)[16]

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009)[17].

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas[18].

TIC (Tecnologías de la Información y las Comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios; que

---

[13] RIQUELME, Rodrigo. (2018) Que es un equipo de respuestas ante emergencia informáticas. El Economista [en línea]. 2018. [Citado 22-enero-2018]. Disponible en https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html

[14] DOCUMENTO CONPES 3701. Lineamientos de política para la ciberseguridad y ciberdefensa. 2011. 2 p. Disponible en https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[15] Ibíd., p.14.

[16] Ibíd. p., 38.

[17] Ibíd., p.14.

[18] Ibíd. p., 38.

permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC)[19]

Riesgo Informático: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía 73:2002)[20]

Incidente Informático: Cualquier evento adverso real o sospechado en relación con la seguridad de sistemas de computación o redes de computación[21]

Ramsomware: un software sofisticado y dañino, que le permite al atacante la habilidad de bloquear el equipo desde cualquier lugar, su propósito es encriptar los archivos o documentos prohibiendo el acceso de toda la información almacenada el equipo que fue infectado[22] nos indican que "El virus envía una ventana emergente que solicita el pago de un rescate, dicho pago se debe hacer generalmente en moneda virtual"[23].

Decoy o señuelos: estos virus tienen una interfaz parecida al programa o sitio web original, su propósito es la de capturar la información de autenticación que utiliza el usuario en su ingreso al suministrar los datos necesarios, esta información es utilizada por el atacante para futuras visitas al sistema[24].

---

[19] MINTIC. Tecnologías dela información y telecomunicaciones TIC. [en línea]. Bogotá: 2020., [Citado 7-septiembre-2020]. Disponible en https://www.mintic.gov.co/portal/inicio/5755:Tecnolog-as-de-la-Informaci-n-y-las-Comunicaciones-TIC

[20] DNP. Guía para la administración de riesgos de la seguridad de la información. [en línea]. Bogotá: 2016., [Citado 23-septiembre-2016]. Disponible en https://.dnp.gov.co/CDT/DNP/ScolaboracionE-G02%20Guía%20metodológica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf

[21] Ibíd. p., 39.

[22] (Camilo Guzman, Cristhian Angarita) Protocolos para la mitigación de ciber ataques en el hogar, Se recuperó en noviembre, 2017 de https://repository.ucatolica.edu.co/bitstream/10983/15321/1/Cibersecurity%20Home.pdf (GUZMAN & ANGARITA, 2017)

[23] (n.d.). ¿Qué es un Ransomware? - PandaSecurity. Se recuperó el noviembre 15, 2013 de https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/ (Pandasecurity, 2013)

[24] (Ruben Bustamante) Seguridad en redes, Se recuperó en 2014 de https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad en redes.pdf (Bustamante, 2014)

6 MARCO LEGAL

Desde 2009, la Comisión de Regulación de Comunicaciones (CRC) ha trabajado para desarrollar un marco regulatorio adecuado en materia de seguridad digital, estos esfuerzos iniciaron con el proyecto “Aspectos regulatorios asociados a la ciberseguridad”, que culminó con la expedición de la Resolución CRT 2258 de 2009, en la cual se establecieron por primera vez las medidas que deben implementar los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) en sus redes, medidas que se mantienen vigentes actualmente. Los principales aspectos desarrollados estaban orientados a establecer las características generales para garantizar la seguridad de la red y la integridad de los servicios[25]. Específicamente, se estableció la obligación de implementar modelos de seguridad que contribuyesen a mejorar la seguridad de las redes de acceso de los proveedores de servicio de internet, de acuerdo con los marcos de seguridad definidos por la UIT en lo que respecta a las recomendaciones pertenecientes a las series X.800. Inicialmente, estas medidas se encontraban dentro del Régimen de calidad vigente en ese momento (Resolución CRT 1740 de 2007).

De otra parte, en esta misma Resolución se establecieron las características generales que deben tener los modelos de seguridad de los PRST, involucrando aspectos como inviolabilidad de las comunicaciones y privacidad de los datos personales mencionados en el Art 53 de la ley 1341 de 2009. Estas previsiones se integraron dentro del Régimen de Protección a los Usuarios vigente en ese momento (Resolución CRT 1732 de 2007).

Posteriormente, en 2011, a través del CONPES 3701, Colombia adoptó una política nacional de ciberseguridad y ciberdefensa, denominada “Lineamientos de política para ciberseguridad y ciberdefensa”. El objetivo general fue desarrollar una

[25] COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución CRT 2258 de 2009. .[En Línea].2018.Disponible en https://normativa.colpensiones.gov.co/colpens/docs/resolucion_crc_2258_2009.htm

estrategia nacional que contrarrestara el incremento de las amenazas informáticas que afectaban al país e incluyera un fortalecimiento institucional y disposiciones dirigidas a diferentes entidades de gobierno.

Las funciones de un CCOC, según el documento CONPES 3701[26] tiene como fin endurecer las habilidades técnicas y operativas del país, frente a las amenazas informáticas y ataques que se puedan presentar, cumpliendo con procesos que permitan la defensa mediante software y hardware en el tema de la ciberdefensa, también deben de velar por la infraestructura critica que tiene el país y mitigar los riesgos que están asociados a esta infraestructura.

Documento CONPES 3701[27], en 2011, estableció los Lineamientos de política para ciberseguridad y ciberdefensa, bajo los auspicios del Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), el Ministerio de Defensa Nacional, el Departamento Nacional de Planeación (DNP) y otras instituciones nacionales clave. Esta estrategia se centró en el establecimiento de instituciones nacionales necesarias para el desarrollo de la capacidad cibernética en Colombia.

Luego, en el año 2014, el Gobierno nacional llevó a cabo una revisión a fondo del Documento CONPES 3701 y solicitó apoyo internacional en la revisión y el desarrollo de una nueva estrategia de seguridad nacional digital.

Las funciones de un CCOC, según el documento CONPES 3701 tendrá como fin endurecer las habilidades técnicas y operativas del país, buscando que dichas habilidades puedan hacer frente a las amenazas informáticas y ataques que se puedan presentar, cumpliendo con todos los procesos que permitan la defensa mediante software y hardware en el tema de la ciberdefensa.

[26] (Conpes 3701 de 2011). Lineamientos de política para la Ciberseguridad y Ciberdefensa - Conpes. Se recuperó el julio 23, 2011 de https://mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

[27] MINTIC. Lineamientos de política para ciberseguridad y ciberdefensa. [En Línea].Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. Bogotá D.C., 14 de julio de 2011.Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

En abril de 2016, se aprobó la nueva Política Nacional de Seguridad Digital, contemplada en el documento CONPES 3854, el cual articula una visión estratégica en la que se alienta a los distintos actores involucrados a hacer un uso responsable del entorno digital y fortalecer las capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

Con el Documento CONPES 3854 Colombia se convierte en el primer país de América Latina, y uno de los primeros en el mundo, en incorporar plenamente las recomendaciones y mejores prácticas internacionales en materia de gestión de riesgos de seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos (OCDE). El CONPES 3854 identificó que la CRC debía ajustar, dentro del marco de sus competencias, el marco normativo del sector TIC en el periodo inicial de implementación de dicha política 2017-2018 teniendo en cuenta el enfoque de gestión de riesgos de seguridad digital.

La Ley 1273 del 5 de enero de 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”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. La ley 1273 resaltan aspectos generales como:

• Artículo 269A. Acceso Abusivo a Un Sistema Informático: se acceda a la información sin autorización.

• Artículo 269B. Obstaculización Ilegítima De Sistema Informático O Red De Telecomunicación. Bloquee o afecte la red de comunicaciones.

• Artículo 269C. Interceptación De Datos Informáticos. Sin orden Judicial intercepte la información.

• Artículo 269D. Daño Informático. Dañar, alterar la información de los datos.

• Artículo 269E. Uso De Software Malicioso. El que venda, compre utilice virus o programas con fines maliciosos.

• Artículo 269F. Violación De Datos Personales. El que extraiga sin autorización la información de los datos personales, incluye la venta y divulgación de esta.
• Artículo 269G. Suplantación De Sitios Web Para Capturar Datos Personales. El que cree páginas web falsas para el robo de información.
• Artículo 269H. Circunstancias De Agravación Punitiva, abusar de la confianza o facultades que se tiene sobre la información que maneja.
• Artículo 2691. Hurto por medios informáticos y semejantes. El que supere las medidas de seguridad para fines maliciosos.
• Artículo 269J: Transferencia No Consentida De Activos. El que tenga información de forma no consentida con el ánimo de lucro.

El numeral 7 del artículo 22 de la Ley 1341 de 2009[28], faculta a la CRC para definir las normas técnicas aplicables al sector TIC, incluidas aquellas para la protección de las comunicaciones de los usuarios, garantizando la inviolabilidad y el secreto de las comunicaciones. En ese estudio buscó determinar el rol de los operadores de telecomunicaciones en la gestión de riesgos de seguridad digital, y las medidas a tomar desde el punto de vista regulatorio. Para ello se realizó un benchmark internacional con el fin de conocer las mejores prácticas de gestión de riesgos de seguridad digital, se realizaron, además, encuestas especializadas a los operadores colombianos para evaluar el estado de implementación de modelos de seguridad en sus redes, y se realizó un análisis detallado de la regulación vigente ley 1273, ley 1581 y Convenio Budapest.

Así mismo la NTC ISO 27001 norma técnica colombiana diseñada y enfocada para las diferentes organizaciones privadas o públicas, aseguren la confidencialidad, integridad y disponibilidad de la información que poseen[29].

[28] MINTIC. Ley Nº1341 del 30 Jul de 2009. [En Línea].Colombia. Disponible en: https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf
[29] (Isotools) ¿Qué es la NTC ISO 27001? Se recupero en el 2019 de https://www.isotools.com.co/normas/ntc-iso-27001/ (Isotools, 2019)

La ISO 27001:2013 en su versión actualizada, cuyo fin es realizar el sistema de gestión de seguridad de la información SGSI. Su objetivo principal es examinar los riesgos y aplicar los controles necesarios para reducirlos y mitigarlos. Al aplicar la norma ISO 27001, da un aumento profesional y competitivo frente a otras organizaciones, esto genera confianza a los clientes ya que, mediante su certificación, indica que cuenta con los estándares de calidad más exigentes y vigentes.

7 MARCO CONTEXTUAL

FIRST: Se define como el foro de equipos de respuesta a incidentes en seguridad informática (por sus siglas en inglés Forum for Incident Response and Security Teams) el cual busca fomentar la cooperación y colaboración a través del intercambio de información entre los miembros que lo conforman y la comunidad en general[30].

CSIRT: Es un equipo de respuesta a incidentes en seguridad informática (por sus siglas en inglés Computer Security Incident Response Team) Cuando se habla de CSIRT corresponde a una organización que tiene como objetivo primordial brindar servicios de respuestas a incidentes en seguridad informática a una comunidad en particular[31].

[30] FIRST INPROVING SECURUTY TOGETHER. Acerca de FIRST. [en línea]. 2015. [Citado 15-noviembre-2020]. Disponible en https://www.first.org/about/organization/

[2] ORGANIZACIÓN PARA LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional [en línea]. 2016. [Citado 15-noviembre-2020]. Disponible en https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

LOS TIPOS DE CSIRT COLOMBIANOS

En 2011 a través del documento CONPES 3701[32], el gobierno determina los parámetros de la política de ciberdefensa y ciberseguridad para mitigar y dar trato al aumento de las incidencias informáticas y en este documento desarrolla unos procesos que permite actuar frente a este tipo de eventualidades con cooperación internacional[33].

Entre los CSIRT´S en Colombia se pueden mencionar los siguientes:

- El Comité de Ciberdefensa de las Fuerzas Militares y las Unidades cibernéticas del Ejercito Nacional. El grupo de respuesta a emergencias cibernéticas de Colombia colCERT[34] del Ministerio de defensa Nacional. El Centro Cibernético Policial de Colombia- CCP[35]. Ofrece información, protección y apoyo ante las violaciones cibernéticas. En sus funciones tiene que ofrecer servicios de investigación, atención, prevención de delitos informáticos del país, también debe ofrecer información sobre las vulnerabilidades cibernéticas conocidas y esta institución recibirá lineamientos y trabajara en conjunto con el colCERT.
- El comando conjunto cibernético del comando general de las fuerzas militares de Colombia (CCOC)[36].
- El equipo de respuesta a incidentes de seguridad informática de la policía nacional (CSIRT PONAL)[37].

---

[32] (Conpes 3701 de 2011). Lineamientos de política para la Ciberseguridad y Ciberdefensa - Conpes. Se recuperó el julio 23, 2011 de https://mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011 (Conpes_3701, 2011)

[33] (Conpes). El Consejo Nacional de Política Económica y Social, CONPES - Conpes. Se recuperó en diciembre 26, 2016 de https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx (CONPES, 2016)

[34] (n.d.). colCERT Grupo de Respuesta a Emergencias Cibernéticas.... Se recuperó el septiembre 28, 2019 de http://www.colcert.gov.co/ (colCERT, 2019)

[35] (n.d.). Centro Cibernético Policial - Policía. Se recuperó el 3 octubre, 2019 de https://caivirtual.policia.gov.co/

[36] (n.d.). Comando Conjunto Cibernético - CCOC. Se recuperó el 3 octubre, 2019 de https://www.ccoc.mil.co/ (CCOC, 2019)

[37] (n.d.). CC-CSIRT - Policía. Se recuperó el 3 octubre, 2019 de https://cc-csirt.policia.gov.co/ (Policia_CC-CSIRT, 2019)

- La Delegatura de protección de datos en la Superintendencia de Industria y Comercio.
- El centro cibernético policial (CCP)[38] de la policía nacional de Colombia.
- La Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones.
- CSIRT ASOBANCARIA
- CSIRT Gobierno de Colombia

Según la NCSI (National Cyber Security Index)[39], Colombia se encuentra en el puesto 54 a nivel mundial y en el puesto 8 a nivel del continente americano.

El informe presentado por la NCSI, permite identificar que este puesto lo ocupa debido a las deficiencias que se tienen en los tiempos de respuesta frente a los incidentes cibernéticos, a las decisiones y acciones tomadas frente a la crisis, las estrategias desarrolladas en ciberseguridad, las publicaciones e informes anuales que presentan, el aporte realizado a la ciberseguridad a nivel mundial, la protección frente a los servicios esenciales, se evidencia que falta mucho por abarcar a nivel de ciberseguridad y que se necesita tener una cooperación nacional entre las entidades privadas y públicas para poder ofrecer un buen servicio de seguridad informática, frente a los incidentes digitales que se presenten en el país.

[38] (n.d.). Centro Cibernético Policial - Policía. Se recuperó el 3 octubre, 2019 de https://caivirtual.policia.gov.co/ (Policia_CCP, 2019)
[39] (NCSI, 2019) National Cyber Security Index 2019. Obtenido de https://ncsi.ega.ee/

Tabla 1 Cuadro Comparativo entre CERT - SOC – CSIRT

CERT	SOC	CSIRT
(Computer Emergency Response Team) Equipo de Respuesta para Emergencias Informáticas, los cuales tiene como objetivo atender las emergencias informáticas llevando a cabo tareas de investigación con el propósito de atender y mejorar la seguridad informática. Es importante aclarar que estos han venido evolucionando con el tiempo y han ampliado cada vez sus funciones. No solo prestan servicios de incidentes de una organización si no que prestan otros servicios adicionales como análisis de riesgos o vulnerabilidades entre otros.	(Security Operation Center) Centro de Operaciones de Ciberseguridad, es una plataforma que permite de manera centralizada la supervisión y administración de la seguridad de los sistemas de información de una empresa u organización, cuentan con una arquitectura tecnológica mucho más robusta que los normales departamentos de TI. Administra tareas relacionadas con la gestión y autorización de identidades, el firewall y el mantenimiento del conjunto de reglas de filtrado, el soporte de investigación y de forense, o cualquier otro aspecto de la seguridad operativa.	(Computer Security Incident Response Team) equipo de respuesta a incidentes en seguridad informática, en una organización cuyo objetivo primordial es atender eventos o incidentes de seguridad informática, estos están conformados por especialistas multidisciplinarios, de manera que respondan, en forma rápida y efectiva, a incidentes de seguridad, además de contribuir a mitigar el riesgo de los ataques cibernéticos. Se destaca el hecho de que los CSIRT aunque en esencia prestan servicios de “respuestas” estos ha evolucionado considerablemente adoptando una posición más Proactiva.

Fuente: ISACA, Ed. CERT Vs CSIRT Vs SOC: ¿Cuál es la diferencia?

La Tabla número 1 presenta el significado de las siglas CERT, CSIRT y SOC, así mismo describe las características de cada uno de ellos presentándolo al lector a través de un cuadro comparativo.

CLASIFICACIÓN DE LOS CLIENTES POTENCIALES QUE PUEDE ADOPTAR EL CSIRT:

Tabla 2 Tipos de Entidades

Tipo de Entidad	Descripción	Grupo de clientes
Académico	Centros académicos, universidades, colegios, instituciones educativas	Personal administrativo, estudiantes de las instituciones
Comercial	Son las empresas que adquieren el servicio por pago	Se rige por SLA y presta el servicio a los clientes que pagan por el servicio
Infraestructura Critica	Colaboran con el sector público para proteger al ciudadano, como las empresas del sector público de energía, comunicaciones, agua, gas, etc.	Se puede tener interacción con la fuerza pública, militar, gubernamental.
Gubernamental	Son las instituciones del gobierno y los servicios que se prestan a los habitantes	Las gerencias de los servicios y las agencias se pueden compartir CSIRT entre las instituciones
Militar	Instituciones militares y de fuerza publica	Instituciones militares y de fuerza publica
Nacional	Es un punto de contacto nacional	Desempeña un punto intermedio para todo el país
Pequeñas y Medianas empresas	Prestar sus servicios a empresas de un ramo o de un grupo de interesados similar	PYMES y particular
Soporte	Desarrollo de herramientas para eliminar vulnerabilidades y mitigarlos	Dueño de los productos.

Fuente: ENISA, Como crear un CSIRT Paso a Paso

La Tabla número 2 describe cada uno de los diferentes tipos de clientes que puede tener un centro de respuesta a incidentes cibernéticos.

8 DISEÑO METODOLOGICO

El diseño metodológico consiste en una revisión documental, entendiéndose que la investigación documental es una disciplina instrumental, como cualquier otra a metodología que consiste en la revisión o consulta de documentos ya sean (documentos escritos como tesis, libros, memorias, investigaciones, revistas indexadas, periódicos, actas, tratados, encuestas, conferencias escritas, memorias y documentos fílmicos como películas, diapositivas, documentos grabados, como discos, cintas y casetes entre otras).

Tancara (1993) refiere que la revisión documental permite hacerse una idea del desarrollo y las características de los diferentes procesos, así mismo permite disponer de información existente que confirme o desmienta el tema que se esté investigando. En la revisión documental el procesamiento y almacenamiento de la información permite presentar información a quién lo requiera.

FUENTES

La fuente primaria consiste en una revisión documental, se tomó información de medios como Internet, hemerotecas universitarias, bibliotecas y libros. La asesoría designada por la universidad, será el soporte para el desarrollo de la investigación con aportes del tutor profesional, experto en el tema.

MÉTODOS DE RECOLECCIÓN DE LOS DATOS

De acuerdo al tema de investigación y los objetivos propuestos, el diseño metodológico de la recolección de datos, se realiza a través de un proceso sistemático donde se enuncian las fuentes bibliográficas encontradas y toda la información solicitada por la norma para referenciarla en los trabajos escritos.

9 DESARROLLO DE LOS OBJETIVOS ESPECÍFICOS PROPUESTOS

Objetivo Especifico 1: Identificar el ámbito de actuación y los documentos de constitución que darán soporte legal a las actividades del CSIRT

9.1 PLAN ESTRATEGICO DEL CENTRO DE RESPUESTAS A INCIDENTES CIBERNÉTICOS

9.1.1 MISIÓN

Cibersecurity de Colombia LTDA es un centro de respuestas a ataques cibernéticos que busca controlar y mitigar los daños causados a los sistemas informáticos de las organizaciones públicas y privadas, desarrollando actividades orientadas a prevenir incidentes similares, fomentando la cultura de la seguridad informática haciendo uso de las herramientas tecnológicas, capacitación y apoyo en la atención de incidentes.

9.1.2 VISIÓN

Cibersecurity de Colombia LTDA en el año 2027 habrá alcanzado su propósito de ser un referente nacional en la promoción y prevención de incidentes cibernéticos, en el conocimiento apalancado en innovación y tecnología, buenas prácticas en el uso de los datos y los bienes informáticos, con los más altos estándares de calidad de sus servicios de información.

9.1.3 OBJETIVOS ESTRATEGICOS DEL CSIRT

1. Brindar respuesta a los diferentes incidentes informáticos.
2. Atender de manera oportuna los eventos inesperados que afectan los activos de las organizaciones.

3. Contar con personal idóneo en experiencia, capacidad y entrenamiento para afrontar las incidencias.
4. Poseer herramientas tecnológicas para el desempeño de las actividades.
5. Promover procesos de educación y cultura del cuidado de los datos y bienes informáticos.
6. Impulsar una cultura de responsabilidad social empresarial.
7. Impulsar procesos y escenarios de formación en la protección e innovación de las tecnologías.
8. Liderar procesos de control y mitigación de incidentes cibernéticos.
9. Posicionarse en el mercado de los centros de ayuda a incidentes cibernéticos.

9.1.4 POLITICAS ORGANIZACIONALES

1. **Política de confidencialidad y manejo de datos:** Como base de todo el trabajo, basado en los derechos y deberes del equipo de trabajo.

2. **Política de gestión ambiental:** Promoción de una cultura ambiental promoviendo la conservación, cuidado y aprovechamiento de los recursos naturales.

3. **Política de sistema de gestión de calidad:** Compromiso de cumplir con los requisitos legales y de sistema de gestión de calidad buscando una mejora continua.

4. **Política de sistema de gestión de la seguridad y salud en el trabajo:** Cumplimiento de los requisitos legales, previniendo los riesgos laborales buscando una mejora continua.

5. **Política de gestión del riesgo:** Crear conciencia de los riesgos a los que se enfrenta el equipo en cuanto a la seguridad de la información.

9.1.5 COMUNIDAD OBJETIVO

La comunidad objetivo para CIBERSECURITY LTDA son pequeñas y medianas empresas MIPYME y otros ciudadanos del distrito capital ciudad Bogotá.

La comunidad objetivo CSIRT es el grupo de personas o entidades que recibirán los servicios por parte del equipo, es decir, los clientes.

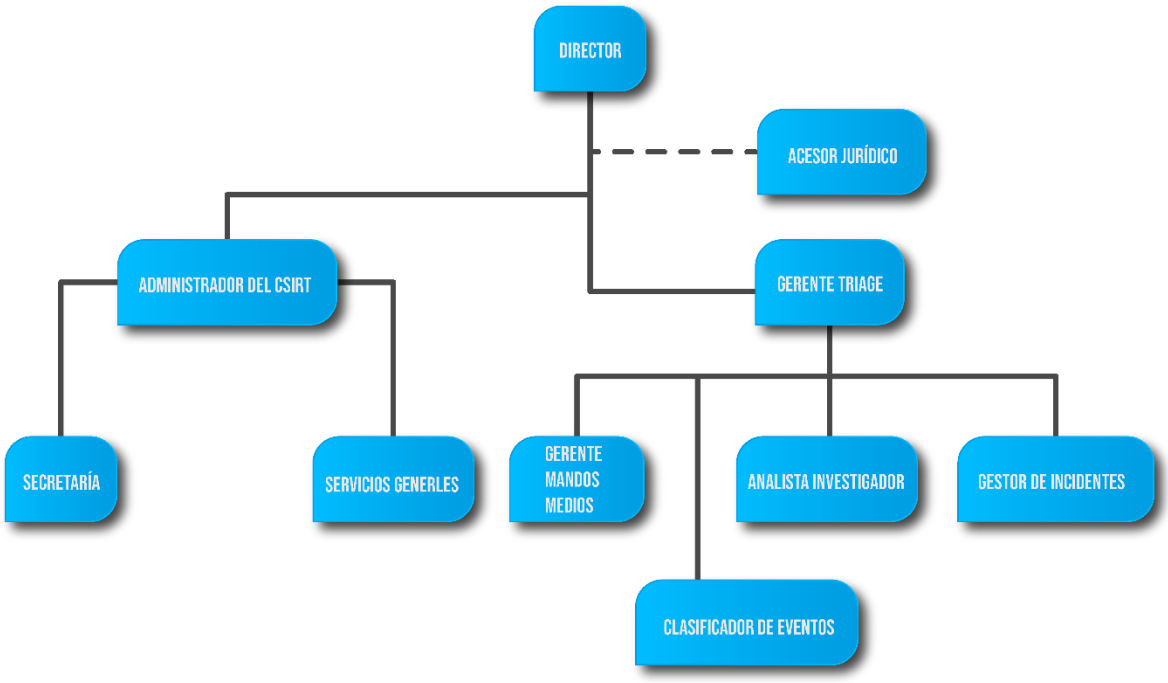
Objetivo 2: Estructurar los perfiles y funciones que conformarán el CSIRT los cuales serán los encargados de dar respuesta a los servicios propuestos

9.2 MANUAL DE FUNCIONES Y DESCRIPCION DE CARGOS DEL CSIRT

El manual presentado a continuación presenta el organigrama jerárquico, así como la descripción de las funciones, competencias y perfiles correspondientes a cada cargo del personal del Centro de Respuesta a incidentes Cibernéticos.

9.2.1 ORGANIGRAMA:

Este está basado en un modelo CSIRT centralizado.



Fuente: El autor

9.2.2 DESCRIPCIÓN DE LAS FUNCIONES DE LOS CARGOS

Director general: Encargado de la dirección estratégica del CSIRT, así como también de la supervisión de todo el equipo de trabajo. Está delegado junto con el área de Recursos Humanos a los procesos de contratación de nuevos miembros del equipo.

Asesor jurídico: Encargado de prestar los servicios jurídicos en cada uno de los contratos, las cláusulas de confidencialidad y en los casos que sean necesario las asesorías.

Administrador del CSIRT: Es el que administra y mantiene los sistemas funcionando del CSIRT.

Gerente TRIAGE: Es el encargado de clasificar y priorizar los eventos de incidentes para los cuales se solicitan servicios asignando los casos al personal técnico correspondiente.

Gerente de mandos medios: Encargado de gestionar y mantener la seguridad en las plataformas y el sistema. Gestiona y monitorea los equipos de hardware y software para evitar que sean vulnerados, asiste las respuestas de incidentes cuando el caso lo amerite, gestiona la información y supervisa directamente las solicitudes de incidentes, verificando que se hayan cumplido las asistencias técnicas. Lidera el equipo en las actividades diarias. Asigna deberes y tareas. Conduce la gestión de claves. Autoriza los permisos de acceso a la información

Analista Investigador: Realiza investigaciones específicas, desarrolla material técnico para el uso interno o de información general, analiza y monitorea incidentes para la elaboración y desarrollo de herramientas.

Gestor de Incidentes: Analiza incidentes, monitoreo, registro y respuesta; coordinando respuestas a incidentes y colaborando con otros grupos de respuesta o técnicos para resolver un incidente.

Clasificador de eventos: Es el encargado de solucionar los incidentes que se presentan, brindando la información oportuna y personalizada con cada cliente. Trabajando de la mano con el cliente y ofreciendo la asesoría y servicio técnico necesario para solucionar el incidente que se presente. Es quien brinda el primer acompañamiento en la respuesta a incidentes. A partir de ello clasifica la información y luego prioriza según el caso.

Secretaria: Será la persona encargada de recibir documentos, atender llamadas telefónicas, atender a los clientes cuando lleguen al centro de ayuda, es quién se encargará de archivar documentos, informes.

Auxiliar de servicios generales: Será el encargado de efectuar labores de aseo y limpieza en oficinas, baños, comedores, pasillos, patios, bodega y, en general, mantener limpias las áreas administrativas y de uso público. Apoyará en labores de mensajería y compras en los casos en que sean necesarios.

9.2.3 FUNCIONES Y PERFILES DE LOS CARGOS:

Tabla 3 perfil y funciones del director

Nombre del cargo: Director general
Perfil: Ingeniero de sistemas con estudios de posgrado especialización en seguridad informática, o seguridad de la información experiencia de 60 meses en cargos relacionados.
Funciones
• Llevar a cabo la dirección estratégica del CSIRT. • Prospectar y contactar potenciales clientes, para ofrecer los servicios de la empresa. • Negociar los lineamientos presupuestados, precios y condiciones con los clientes. • Dirigir las mesas de trabajo con el equipó quincenalmente para evaluar indicadores de eficiencia y efectividad. • Elaborar la planeación estratégica, objetivos e indicadores de gestión. • Capacitar al equipo de trabajo en nuevos programas, software, equipos informáticos y tecnológicos. • Realizar análisis de la idoneidad de los perfiles en las hojas de vida recibidas, para ser contratados y puedan hacer parte del equipo de trabajo. • Brindar el aval a la contratación de personal para el equipo de talento humano

Fuente: El autor

La anterior tabla presenta los requisitos del perfil del director y las funciones que debe desempeña.

Tabla 4 Perfil y funciones del asesor jurídico

Nombre del cargo: Asesor jurídico
Perfil: Abogado especializado en derecho informático.
Funciones

• Asesorar jurídicamente a la empresa en los temas relacionados con derecho informático. • Asesorar las negociaciones en temas jurídicos • Participar en la construcción y elaboración de documentos contractuales y los documentos legales requeridos. • Realizar el acompañamiento jurídico en el manejo de los incidentes que lo ameriten. • Todas las demás que le sean necesarias desde el área jurídica.

Fuente: El autor

La tabla número 4 presenta los requisitos del perfil del asesor jurídico y las respectivas funciones.

Tabla 5 Perfil y funciones administrador CSIRT

Nombre del cargo: Administrador del CSIRT
Perfil: Administrador de empresas, administrador financiero o afine con experiencia mínima de 36 meses en cargos afines.
Funciones
• Administrar o gestionar el presupuesto del CSIRT • Hacer buen uso del presupuesto del Centro de respuesta. • Realizar el plan de compras de artículos administrativos y de uso operativo. Supervisar el equipo de trabajo. • Supervisar la programación y asignación de recursos. • Velar por el aprovechamiento de las capacidades operativas del centro de respuestas. • Realizar la rendición de cuentas ante los entes de control a los que haya

Fuente: El autor

La tabla número 5 presenta los requisitos del perfil del administrador y las respectivas funciones.

Tabla 6 Perfil y funciones del Gerente TRIAGE

Nombre del cargo: Gerente TRIAGE
Perfil: Profesional en ingeniería de sistemas con experiencia mínima de 36 meses cargos relacionados
Funciones
• Brindar la asistencia inicial de respuesta a incidentes informáticos. • Clasificar los incidentes recibidos y priorizarlos de acuerdo al caso la información recibida y los procedimientos establecidos. • Gestionar la información y supervisar directamente las solicitudes de incidentes.

Fuente: El autor

La tabla anterior presenta los requisitos del perfil del Gerente TRIAGE y las funciones que desempeñará.

Tabla 7 Perfil y funciones del gerente de mandos medios

Nombre del cargo: Gerente mandos medios
Perfil: Ingeniero de sistemas con posgrado de especialización en seguridad informática, experiencia mínima de 36 meses en temas relacionados.
Funciones
• Brindar soporte al director • Liderar el equipo en las actividades diarias • Asignar y hacer seguimiento a las tareas y deberes diarios o semanales. • Asignar las claves de los procesos. • Administrar y generar los permisos de acceso a la información.

Fuente: El autor

La tabla número 7 enuncia el perfil y funciones del gerente de mandos medios.

Tabla 8 Perfil y funciones analista investigador

Nombre del cargo: Analista investigador
Perfil: Ingeniero de sistemas y/o electrónico con especialización en informática forense. Experiencia mínima de 36 meses en cargos relacionados.
Funciones
• Realizar investigaciones específicas • Desarrollar material técnico para el uso interno o de información general. • Analizar y monitorea incidentes para la elaboración y desarrollo de herramientas.

Fuente: El autor

La tabla número 8 hace referencia al perfil y funciones del analista investigador

Tabla 9 Perfil y funciones de gestor de incidentes

Nombre del cargo: Gestor de incidentes
Perfil: Ingeniero de sistemas y /o electrónico con experiencia mínima de tres años en cargos con funciones relacionadas.
Funciones
• Analizar incidentes, monitorear, registrar y dar respuesta a los mismos. • Coordinar respuestas a incidentes de acuerdo a los procedimientos establecidos. • Colaborar con otros grupos de respuesta o técnicos para resolver un incide

Fuente: El autor

La tabla número 9 presenta el perfil y las funciones del gestor de incidentes.

Tabla 10 Perfil y funciones de clasificador de incidentes

Nombre del cargo: Clasificador de incidentes
Perfil: Ingeniero de sistemas y/o electrónica con certificación ISO270001 experiencia mínima tres años.

Funciones
• Gestionar y dar solución a los incidentes que se presentan, brindando la información oportuna y personalizada con cada cliente Analiza incidentes, monitoreo, registro y respuesta • Trabajando de la mano con el cliente • Brindar la asesoría y servicio técnico necesario para solucionar el incidente que se presenten.

Fuente: El autor

La tabla número 10 hace referencia al perfil y funciones del clasificador de incidentes

Tabla 11 Perfil y funciones de la secretaria

Nombre del cargo: Secretaria
Perfil: Técnico en secretariado ejecutivo, o técnico en auxiliar administrativo, o técnico en archivo, técnico en auxiliar contable.
Funciones
• Recibir y enviar la documentación • Mantener actualiza la agenda de su superior inmediato, recordando con antelación los compromisos, reuniones programadas. • Atender llamadas telefónicas y los visitantes de la empresa. • Administrar y mantener organizada la documentación generada.

Fuente: El autor

La tabla número 11 hace referencia al perfil y funciones de la secretaria

Tabla 12 Perfil y funciones de auxiliar de servicios generales

Nombre del cargo: Auxiliar de servicios generales
Perfil: Bachiller académico con experiencia de mínimo un año en trabajo relacionados de aseo, cafetería.
Funciones
• Desempeñar labores de aseo y limpieza en oficinas, baños, comedores, pasillos, patios, bodega y, en general, todas las áreas del CSIRT. • Mantener limpias las áreas administrativas y de uso público. • Preparar café, aromáticas y pasar a los empleados y clientes cuando se le solicite.

Fuente: El autor

La tabla número 12 presenta el perfil y funciones del auxiliar de servicios generales.

Objetivo 3: Definir los servicios, las políticas y el código de ética que permitirán dar desarrollo a las actividades del CSIRT los cuales darán respuesta a las necesidades presentadas por las partes interesadas o comunidades objetivo

9.2.4 PORTAFOLIO DE SERVICIOS

A continuación, se presenta el portafolio de servicios que ofrecerá el centro de respuestas CIBERSECURITY de Colombia LTDA, a las diferentes entidades:

Tabla 13 Portafolio de Servicios del CSIRT.

Servicio	Procesos
Servicios Reactivos	1. Servicio software de alertas. 2. Gestión de incidentes. • Análisis de incidentes. • Respuesta a incidentes en sitio. • Soporte de respuesta a incidentes. • Coordinación de respuesta a incidentes. 3. Gestión de vulnerabilidades. • Análisis de vulnerabilidades. • Respuesta a vulnerabilidades. • Coordinación de respuesta a vulnerabilidades. 4. Gestión de Artefactos (*). • Análisis. • Respuesta. • Coordinación de la respuesta
Servicios Proactivos	• Vigilancia tecnológica. • Auditorías de seguridad o evaluaciones. • Configuración y mantenimiento de seguridad, herramientas y aplicaciones e infraestructura. • Desarrollo de herramientas de seguridad. • Servicios de detección de intrusos. • Difusión de información relacionada con la seguridad.
Calidad de los servicios de gestión de la seguridad	• Análisis de riesgos. • Continuidad de negocio y plan de recuperación de desastres. • Consultoría de seguridad. • Sensibilización en seguridad. • Educación / Entrenamiento. • Evaluación de productos o certificación

Fuente: AQUINO LUNA, Rubén, *et al.* Manual básico de Gestión de Incidentes de Seguridad Informática.

9.2.5 CODIGO DE ETICA

“Trabajo con integridad y ética, mi compromiso con CIBERSECURITY de Colombia LTDA”

Propósito

La finalidad es construir una empresa que productiva, confiable y humana; que buscará la fidelización de nuestros clientes y lealtad de los colaboradores; para ello se establece el código de ética. El presente documento busca convertirse en un mapa de ruta de la conducta, postura y criterios en diferentes temas relacionados según nuestra actividad económica.

Alcance

Esta política aplica a todo el equipo de trabajo directo e indirecto, independientemente del cargo, tipo de contrato siempre y cuando trabajen para la Empresa.

Nuestros compromisos

Con los clientes

Su satisfacción es esencial para nuestro éxito. Por lo tanto, la calidad y confidencialidad de nuestros trabajos, así como nuestro servicio son el principal compromiso con ellos.

Con nuestro equipo de trabajo

Buscamos que cada integrante del equipo de trabajo como los contratistas sea respetado y que cuenten con un espacio adecuado y las herramientas necesarias para su desarrollo tanto en el ámbito profesional como en el personal. Respeto, justicia, confianza y afecto.

a) Respeto a la individualidad

Entendiendo que cada persona es única y contribuye a la empresa no se permite ningún tipo de discriminación aplicando este valor en la etapa de selección o contrato.

b) Desarrollo y valores

Se fomentará el aprecio a los valores morales y normas éticas

c) Seguridad y bienestar

Propiciar ambientes de trabajo seguro, sano, y mantener una cultura de seguridad y bienestar.

d) Claridad y responsabilidad en las funciones

Transmitir información veraz, oportuna para el cumplimiento de las funciones

e) Confidencialidad

Cuidado y uso responsable de la información a la que tenga acceso proveyendo seguridad de la información la cual puede ser propiedad intelectual, secretos industriales o información financiera etc.

f) Integridad

No se aceptan actos de corrupción, no sobornamos, no ofrecemos ni damos dinero, bienes, favores o servicios a persona alguna, con el fin de obtener de algún tipo de beneficio.

g) Conducta

Todo colaborador debe regirse por el presente código, objetivos misionales y políticas organizacionales.

h) Austeridad

Hacer uso eficiente de los recursos disponibles, evitando perdidas, daños por mal uso, buscando mantenerlos en perfecto estado de funcionamiento, y aprovechar el tiempo en el horario laboral.

i) Información

Se debe reportar la información, facilitar el acceso a la información pública completa, veraz, oportuna y comprensible a través de los medios destinados para ello generada, producto de su labor, en forma honesta, segura y oportuna, decir la verdad, incluso cuando cometan errores, porque es humano cometerlos, pero no es correcto esconderlos.

9.2.6 Con nuestros proveedores

a) Trato

Con los proveedores se tendrá el compromiso de llevar a cabo negociaciones honestas y equitativas, sin discriminaciones y/o imposiciones.

b) Selección y desarrollo

Todas las propuestas que los proveedores presenten en el momento de requerirlos serán revisadas de manera integral considerando el precio, el valor agregado, la calidad y el servicio que ofrezcan.

c) Condiciones

Consideramos que uno de nuestros principales compromisos con nuestros proveedores es el pago oportuno por sus servicios y productos. Para ello establecemos acuerdos claros en materia de condiciones de pago y definimos procesos estables, simples y transparentes que no se presten a interpretaciones o malas prácticas.

d) Integridad

Los proveedores son participes de este principio de integridad personal y por ello se les solicita que asuman la responsabilidad de no ofrecer retribuciones o regalos a los colaboradores, adhiriéndose a nuestro código de conducta para proveedores y otros terceros.

Con nuestra competencia

CIBERSECURITY de Colombia LTDA comprometidos en competir en el mercado basados en precio, calidad y servicio, en un marco de integridad, respetando a nuestros competidores en todos los sentidos. Utilizará publicidad basada en la verdad sin emplear información o argumentación engañosa.

La relación con la competencia será siempre apegada a nuestras políticas, así como a la legislación aplicable de los países en los que operamos, por lo que en caso de tener contacto o coincidir con sus representantes, nos comportaremos en forma profesional y no compartiremos información de la compañía.

Con el gobierno

a) Respeto a las leyes

Cibersecurity de Colombia se mantendrá informada de las leyes y normatividad generada sobre seguridad y manejo de la información para no incurrir en ninguna violación.

Dentro del marco legal, se colaborará con las autoridades en su actuar con un trato amable y respetuoso, por lo que evitamos cualquier acto con cualquier nivel de Gobierno que pudiera interpretarse como corrupción o soborno.

Objetivo 4: Establecer los recursos financieros y la estructura tecnológica que dará soporte a las acciones del equipo de respuesta

9.3 POLITICAS MINIMAS OBLIGATORIAS CSIRT CIBERSECURITY LTDA

Política de clasificación de información

De acuerdo a los niveles de criticidad el CSIRT clasifica la información. El equipo de trabajo aplica la clasificación de la información al momento de manipular los activos informáticos, de acuerdo a los lineamientos para tal fin, cuando esta información llega de fuentes externos el responsable de dicha clasificación será del oficial de seguridad.

Política de protección de datos

Esta política hace referencia a la forma de proteger la información. Es responsable por la forma correcta de brindar tratamiento a los datos a los cuales pueda acceder al ofrecer su servicio, así mismo debe garantizar la administración de las bases de datos que almacena.

Política de retención de información

Esta política define el tiempo que el CSIRT debe mantener registros u otra información de las empresas. De acuerdo a la ley de archivos, o a solicitud de los clientes, se hará la disposición de la información manejada durante el desarrollo del servicio.

Política de destrucción de información

Esta política define la manera que ha dispuesto el CSIRT para destruir la información relacionada con el caso y que garantice que la información esté protegida hasta el tiempo definido para ser destruida. Toda la información que se edite o manipule o que sea custodia de la empresa, incluyendo medios físicos o electrónicos como registros impresos, log de eventos, mensajes de alertas, estadísticas, documentos o registros clasificados como confidencial o restringida, que contengan información empresarial, personal, privada deben cumplir los lineamientos definidos para la eliminar correctamente de la información.

Política de propiedad de la información

Quien tiene la facultad de otorgar el acceso a la información es del responsable del área que genera o custodia dicha información.

La propiedad de la información no puede ir en contra del carácter legal de la misma, lo que significa que la información generada por la empresa debe estar disponible en situación de requerimientos legales internos o externos a la empresa.

Política de divulgación de información

Esta política define las condiciones por las cuales es necesario compartir la información del caso ya sea interna o externamente, los empleados, directivos y terceros deben mantener la confidencialidad de la información que se les encomiende a excepción de los casos en que la divulgación quede autorizada o sea exigida por la ley.

Política de gestión de incidentes

Esta política define el protocolo de respuesta en tiempos y procedimientos de acuerdo a la clasificación de incidente, describe el paso a paso de las actividades que se deben desarrollar en cada uno de los casos que llegan al centro de respuestas.

Política confidencialidad de la información

Toda la información que se produzca en la empresa es de su propiedad y de uso exclusivo de la empresa, permitiendo que el área que la genera, tenga la responsabilidad de la custodia y uso, tiene además la obligación y la autoridad de clasificar la información de acuerdo con la “Política de clasificación de información” y los lineamientos de seguridad.

Los empleados, directivos y terceros deben mantener la confidencialidad de la información que les encomiende la organización, empleados, clientes y proveedores, a excepción de los casos en que la divulgación quede autorizada o sea exigida por la ley.

Definición de incidentes de seguridad y política de eventos

Esta política describe la definición de un evento o incidente de seguridad de acuerdo a los criterios del CSIRT y los clasifica de acuerdo al tipo y la gravedad.

9.4 RECURSOS FINANCIEROS

Tabla 14. Recursos Necesarios

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Director	$ 5.500.000
	Asesor Jurídico	$ 3.900.000
	Administrador CSIRT	$ 4.500.000
	Gerente TRIAGE	$ 3.900.000
	Gerente mandos medios	$ 3.700.000
	Analista investigador.	$ 3.600.000
	Gestor de incidentes	$ 3.600.000
	Clasificador de eventos	$ 3.600.000
	Secretaria	$ 2.100.000
	Servicios Generales	$ 1.400.000

Equipos y Software	Radware: Sistema de mitigación de ataques informáticos en tiempo real, que permite la protección de la plataforma tecnológica.	$ 79.748,59
	SIEM Arcsinght: Es un gestor/correlacionador de eventos de seguridad de la información, el cual realiza de manera automática el monitoreo en tiempo real, correlación de eventos y almacenamiento de logs de seguridad para análisis y presentación del comportamiento de la plataforma Tecnológica.	$ 220.000,00
	ForcePoint: Herramienta que registra la consulta de páginas Web de los usuarios finales del sistema, categorizándolas según el tipo y riesgo que cada una representa. Contiene un módulo que registra logs de seguridad sobre los archivos extraídos de los equipos de cómputo a medios de almacenamiento externo y/o Nube.	$ 550.000,00
	Firewall Paloalto: Registra los accesos tanto internos como externos realizados desde y hacia la plataforma tecnológica de la entidad, permitiendo identificar tanto el bloqueo de accesos no autorizados como las comunicaciones autorizadas en el canal principal.	$ 130.000,00
	FireEye: Herramienta que permite identificar y bloquear Amenazas Avanzadas Persistentes (APT) que puedan ser desplegadas al interior de la plataforma tecnológica, mediante la descarga de código malicioso que puede realizarse por cualquier funcionario que consulte páginas Web previamente comprometidas por ciberdelincuentes.	$ 85.000,00
	Trend Micro OfficeScan: Consola de antivirus de la entidad, que registra las acciones tomadas ante la presencia de malware en los sistemas computacionales.	$ 55.000,00

	Office Scan Vulnerability Protection: proporciona una protección temprana de los puntos de conexión más sólida al complementar la seguridad antimalware y de amenazas de escritorio con la aplicación proactiva de parches virtuales. Un motor de alto rendimiento que supervisa el tráfico en busca de nuevas vulnerabilidades con filtros de prevención de intrusiones (IPS) basados en host y supervisión de ataques de día cero. Vulnerability Protection impide que estas vulnerabilidades puedan ser explotadas gracias a la aplicación de filtros fáciles y rápidos de implementar que ofrecen una protección completa antes que se puedan implantar parches o incluso de que estén disponibles.	$ 75.000,00
	Firewall Check point: Registra los accesos tanto internos como externos realizados desde y hacia la plataforma tecnológica de la entidad, permitiendo identificar tanto el bloqueo de accesos no autorizados como las comunicaciones autorizadas en el canal alterno.	$ 58.800,00
Viajes y Salidas de Campo	Viajes a capacitaciones del personal Técnico y administrador del Equipo de Respuesta de Incidentes.	$ 3.500.000
Materiales y suministros	Internet DNS Web Hosting Servidores. Sistema Operativo Linux Herramientas y paquetes presentes en Linux Sistema de Control Equipos de Oficina	$15.000.000
TOTAL		$ 55.553.548.59

Fuente: Departamento Administrativo de la Presidencia de la República DRAPE 2019, Lineamientos Recursos Financieros.

10 RESULTADOS ESPERADOS

Tabla 15. Resultados Esperados

RESULTADO/PRODUCTO ESPERADO	INDICADOR	BENEFICIARIO
Diseño para la creación de un Centro De Respuesta A Incidentes Cibernéticos que se encargará de definir planes y políticas de seguridad TICs a nivel Nacional.	Documento que presente el diseño	- Cibersecurity de Colombia LTDA - Empresas afectada por ataques cibernéticos a nivel Nacional
Conformación de un equipo de técnicos responsable del desarrollo de medidas Preventivas y Reactivas ante incidencias de seguridad en los sistemas de información.	Organigrama y manual de funciones.	- Cibersecurity de Colombia LTDA - Empresas afectada por ataques cibernéticos a nivel Nacional
Propuesta de la Infraestructura de Tecnologías de manejo de información y comunicaciones que puedan servir de base para el manejo de eventos en el escenario de Seguridad.	Documento que plantee la infraestructura tecnológica	- Cibersecurity de Colombia LTDA - Empresas afectada por ataques cibernéticos a nivel Nacional
Definición de políticas que apoyaran al manejo de los escenarios de la Seguridad de la información y las Comunicaciones.	Listado de políticas definidas para el desarrollo de las actividades del CSIRT	- Cibersecurity de Colombia LTDA - Empresas afectada por ataques cibernéticos a nivel Nacional - colCERT.

Fuente: El autor

RECOMENDACIONES

Elaborar un plan estratégico para el centro de respuestas a incidentes cibernéticos el cual permita identificar el ámbito de actuación, y donde se definan, la Comunidad objetivo, los objetivos estratégicos del CSIRT, políticas organizacionales, Misión y visión.

Brindar capacitación y entrenamiento al talento humano en término de la ciberseguridad.

Establecer alianzas con equipos de respuestas en termino de contribuir en el desarrollo de métricas y estrategias para procesos de inteligencia de amenazas.

Asignar recursos presupuestales para la ciberseguridad.

Dar una mirada a las herramientas de Open Source como infraestructura lógica para dar un primer paso en términos de respuestas a incidentes, con la consolidación de un SOC.

CONCLUSIONES

- Es importante indicar los diferentes documentos que se necesitan para la constitución de un CSIRT, que definan una modalidad, y que sirvan de soporte legal para establecer la formalidad y el ámbito de Actuación que tendrá la empresa.
- Se debe definir la estructura de los Perfiles y las funciones del personal que conforma al CSIRT, para seleccionar profesionales idóneos en cada tarea, que brinde una atención adecuada y posibilite lograr los objetivos, misión y visión de la empresa y así dar respuestas a las solicitudes y servicios de los usuarios/clientes.
- Es fundamental que se definan las políticas de la empresa, así como el código de ética que regirá la prestación de los servicios, las cuales deben instruir buenas prácticas y eficiencia en el desarrollo de las actividades para generar clientes satisfechos y una prestación de servicios con parámetros de calidad establecidos.
- Para determinar si la constitución y formalización de un CSIRT que se encargue de brindar asistencia, acompañamiento y soluciones a los diferentes tipos de incidentes de las empresas Nacionales e internacionales, es fundamental establecer un presupuesto que identifique cuantos recursos financieros, tecnológicos, operativos y de funcionamiento se necesitan, y especificar de donde se obtendrán cada uno de estos recursos

BIBLIOGRAFIA

AQUINO LUNA, Rubén, *et al.* Manual básico de Gestión de Incidentes de Seguridad Informática. [En Línea]. Edición 201.México 2012 23 p ISBN 978-9974-98—741-8 Disponible en https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia.2015. 17, 116 p [En Línea].Colombia 2015 Disponible en https://repository.unad.edu.co/handle/10596/3629

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES CCIT, TicTac, Programa SAFE. Tendencias cibercrimen en Colombia 2019-2020.5 p. [En Línea].Colombia 2019 Disponible en https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

COHEN karen, Daniel. Importancia de la información para las empresas [En Línea]. Argentina: 2018. Disponible en https://www.grandespymes.com.ar/2014/10/03/importancia-de-la-informacion-para-las-empresas/

COMISIÓN DE REGULACIÓN DE COMUNICACIONES. Resolución CRT 2258 de 2009. [En Línea] 2018.Disponible en https://normativa.colpensiones.gov.co/colpens/docs/resolucion_crc_2258_2009.htm

DACCACH, José Camilo. Ley de Delitos Informáticos en Colombia [En Línea].2018.Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

DNP. Guía para la administración de riesgos de la seguridad de la información. [En línea]. Bogotá: 2016 Disponible en https://.dnp.gov.co/CDT/DNP/ScolaboracionE-

G02%20Guía%20metodológica%20para%20la%20admon%20de%20riesgos%20del%20SGSI.Pu.pdf

DOCUMENTO CONPES 3701. Lineamientos de política para la ciberseguridad y ciberdefensa. [En Línea] Colombia 2011. 2,14, 38, 39 p. Disponible en https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

ENISA, Como crear un CSIRT Paso a Paso. [En Línea] España 2006 Disponible en https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

EL TIEMPO. Tecnologías evolución y futuro [En línea]. Bogotá: 2018. Disponible en https://m.eltiempo.com/archivo/documento/MAM-219859

Guía para la Implementación de Seguridad de la Información en una MIPYME. [En línea]. Bogotá: MINTIC. 2016, 6, 8,9 31 p. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf

HANSEN, Denis. SAVE Social Vulnerability & Assessment Framework [En Línea] Dinamarca 2017, 42-49 p. Disponible en http://www.fak.dk/publikationer/Documents/Project%20SAVE.pdf

ISACA, Ed. CERT Vs CSIRT Vs SOC: ¿Cuál es la diferencia? [En Línea] EEUU 2019, Disponible en https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia#:~:text=Entre%20las%20diferencias%3A%20CERT%20es,un%20equipo%20de%20negocios%20multifuncional.

MINTIC. Tecnologías dela información y telecomunicaciones TIC. [En línea]. Bogotá: 2020 [Citado 7-septiembre-2020]. Disponible en https://www.mintic.gov.co/portal/inicio/5755:Tecnolog-as-de-la-Informaci-n-y-las-Comunicaciones-TIC

MINTIC. Lineamientos de política para ciberseguridad y ciberdefensa. [En Línea].Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación. Bogotá D.C., 14 de julio de 2011.Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

MINTIC. Ley Nº1341 del 30 Jul de 2009. [En Línea].Colombia.2019 Disponible en: https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

RAMIREZ, María carolina. El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia [En Línea].Bogotá: Especiales La república, Informe tecnología. 28 de Junio de 2019. Disponible en: https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067

RIQUELME, Rodrigo. Que es un equipo de respuestas ante emergencia informáticas. El Economista [En línea]. Colombia 2018. [Citado 22-enero-2018]. Disponible en https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html

TANCARA, Constantino. La investigación documental. [En línea]. Bolivia 1993. [Citado diciembre- 1993]. Disponible en http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S0040-29151993000100008

WELIVESECURITY. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [En línea]. Colombia 2015. [Citado 13-septiembre-2018]. Disponible en https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/