DISEÑO DOCUMENTAL PARA LA IMPLEMENTACIÓN DEL CSIRT PARA EL CASO DE ESTUDIO DE LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA.

WILLIAM ANDRÉS ROSERO NARVÁEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUERTO ASÍS, COLOMBIA
2021

DISEÑO DOCUMENTAL PARA LA IMPLEMENTACIÓN DEL CSIRT PARA EL CASO DE ESTUDIO DE LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA.

WILLIAM ANDRÉS ROSERO NARVÁEZ

Proyecto aplicado

Trabajo de grado para optar al título de:
Especialista en seguridad informática

ASESOR
M.SC. JOHN F. QUINTERO T.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUERTO ASÍS, COLOMBIA
2021

Nota de aceptación:

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Puerto Asís, (02 de junio de 2021)

AGRADECIMIENTOS.

Mis agradecimientos más profundos a la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA por formarme como un profesional íntegro inicialmente como ingeniero de sistemas y ahora con el desarrollo de este proyecto como especialista en seguridad informática para con ello poder desenvolverme en el mundo laboral que hoy en día es tan competitivo.

Al ingeniero EDUARD ANTONIO MANTILLA TORRES por ser el pilar para el inicio de este proyecto mediante el curso de proyecto de seguridad informática I, gracias por toda su dedicación y entrega en cada una de sus intervenciones y sus realimentaciones; de igual forma mis agradecimientos a la ingeniera YENNY STELLA NUÑEZ por todas sus asesorías, correcciones y realimentaciones a lo largo del curso de proyecto de seguridad informática II logrando así que este documento quede con la menor cantidad de errores.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AMENAZA: violación en contra de la seguridad, se presentan cuando hay ciertas situaciones, acciones o eventos que pueden causar daño.

APLICACIÓN: programa que permite desarrollar procesos o funciones para un usuario.

ANTIVIRUS: permite realizar detección y eliminación de software o código malicioso.

AUTENTICACIÓN: proceso mediante el cual se da fidelidad de algo o alguien.

BOT: programa o código que permite realizar acciones en automático.

CIBER: prefijo que antecede términos de la informática en situaciones actuales.

CONSULTA: orden o petición de información hacia un sistema.

CONTRASEÑA: caracteres que formar una palabra de seguridad.

CÓDIGO MALICIOSO: software que se ejecuta para perjudicar sistemas informáticos.

DESASTRE NATURAL: sistemas que pueden inhabilitar estructuras tecnológicas.

DOS: ataque de denegación de servicios, su función es sobrecargar sistemas informáticos.

ESCANEO DE PUERTOS: peticiones para saber qué servicios están activos en una red o en un equipo.

EVENTO: ocurrencia en un sistema o una infraestructura tecnológica

FIREWALL: elemento de red cuya función es prevenir el acceso no autorizado.

GNU: permite la distribución de software con su código fuente, respetando los derechos de autor.

INCIDENTE: evento que perjudica una infraestructura tecnológica.

ISO: acrónimo de organización internacional de normalización

INGENIERÍA SOCIAL: técnicas no legitimas para obtener información a partir de usuarios que tiene acceso a los sistemas.

INTEGRIDAD: propiedad que permite validar la información, garantizando que esta llegue tal como se envió.

MANEJO DE INCIDENTES: planes de acción para gestionar eventos que perjudican los activos de información.

PERMISOS: grado de actuación que tienen otros usuarios a parte del propietario sobre la información.

POLÍTICAS DE SEGURIDAD: reglas y prácticas que permiten garantizar la seguridad de los activos de información.

PISHING: técnicas que permiten el robo de identidad y la posterior suplantación.

RESPUESTA: reacción ante un estímulo o evento.

RIESGO: grado de probabilidad de que una amenaza ocurra.

SEGURIDAD: aseguramiento de los activos de información de una organización.

SGSI: por sus siglas se define como sistema de gestión de la seguridad de la información

SOFTWARE: programas que son ejecutados por el hardware.

SUPLANTACIÓN: intento de hacerse pasar por alguien más.

USUARIO: persona u organización que accede a los servicios de la infraestructura tecnológica.

VULNERABILIDAD: fallos en los activos de información que pueden ser explotados por los atacantes.

RESUMEN

Actualmente en Colombia se tiene un alto índice de crímenes cibernéticos, el cual afecta desde el ciudadano promedio hasta las grandes empresas privadas e incluso organizaciones gubernamentales, muchas de estas no tienen un plan de contingencia ante estos hechos, a veces por desconocimiento o incluso por falta de recursos, es por ello que desde el caso de estudio CIBERSECURITY de Colombia Ltda. se ha planteado cubrir esta necesidad con el desarrollo de un centro de respuesta a incidentes de seguridad informática (CSIRT), esta es una organización que cuenta expertos que se encargan de la coordinación y el apoyo para la respuesta ante un evento o incidente de seguridad informática con métodos sistemáticos que permitan reducir al máximo los riesgos o mitigar el impacto de un incidente en curso. En el desarrollo de este proyecto se realizara el diseño documental para la implementación del CSIRT para el caso de estudio de la empresa CIBERSECURITY de Colombia LTDA, esto, a partir de una investigación aplicada que permita mostrar las actividades propias del CSIRT para la empresa, con la descripción de los diferentes campos de aplicación, la definición de los roles del personal que integrará el equipo con sus respectivas funciones, el diseño del catálogo de servicios a prestar, el manual de operaciones y finalmente la estructura orgánica que tendrá el CSIRT.

PALABRAS CLAVE: CISRT, vulnerabilidad, amenaza, riesgo, SGSI, base de datos, incidente.

ABSTRACT

Currently in Colombia there is a high rate of cyber crimes, which affects everything from the average citizen to large private companies and even governmental organizations, many of these do not have a contingency plan in the face of these facts, sometimes because of lack of care or even lack of resources, that is why since the case of study CIBERSECURITY of Colombia Ltda. has considered to cover this need with the development of a security incident response center, that is why since the case of study CIBERSECURITY of Colombia Ltda. has considered to be meeting this need with the development of a security incident response center (CSIRT), this is an organization that counts experts who are responsible for coordinating and supporting response to a computer security event or incident with systematic methods to minimize risks or mitigate the impact of an ongoing incident. In the development of this project, documentary design will be carried out for the implementation of the CSIRT for the case study of the company CIBERSECURITY of Colombia LTDA, this, from an applied research that allows to show the activities of the CSIRT for the company, with the description of the different fields of application, the definition of the roles of the staff that will integrate the team with their respective functions , the design of the catalogue of services to be provided, the operations manual and finally the organic structure that the CSIRT will have.

KEYWORDS: CISRT, vulnerability, threat, risk, SGSI, database, incident.

INTRODUCCIÓN

El crecimiento tecnológico y la continua dependencia social y económica de los procesos sobre las TIC, trae consigo el incremento de delitos informáticos, lo cual ha generado desde simples molestias para las organizaciones hasta pérdidas económicas de gran envergadura, es por ello que quienes cuenten con una infraestructura TI y activos de información sin importar su clasificación y con mayor razón si la información es confidencial o critica, deben estar conscientes de los riesgos a los que están expuestos; de ahí la importancia que tiene un CSIRT el cual por sus siglas en ingles hace referencia a centro de respuesta a incidentes de seguridad informática

Por lo anterior la empresa caso de estudio Cibersecurity de Colombia LTDA, se ha propuesto hacer la documentación administrativa como paso fundamental antes del desarrollo y puesta en marcha del CSIRT, a fin de implementar una organización que cuente con un equipo calificado para prevenir incidentes o mitigar el impacto que estos puedan generar en los activos de información de los clientes; este proyecto aplicado identifica la importancia que tiene para la sociedad colombiana y para su economía salvaguardar los sistemas y la información, esto a partir de un análisis de la ciberseguridad en Colombia en los cinco últimos años, permitiendo con ello determinar un sector o ámbito en donde el CSIRT se desenvuelva.

Teniendo en cuenta los ataques o incidentes que actualmente más se presentan y el nivel de riesgos que estos conllevan, se hace posible jerarquizarlos y ofrecer una serie de tareas para resolverlos, lo cual constituirá el catálogo de servicios del CSIRT, permitiendo así que las empresas contratantes elijan y sean asesorados por profesionales en el tema de seguridad informática, solventando los daños causados de un evento en ocurrencia o cuando el cliente desee implementar medidas para que los riesgos no ocurran, caso contrario que causen los menores daños posibles sobre la infraestructura TI y los activos de información con los que cuenta el cliente. Un equipo de profesionales adecuado permitirá que una organización en fase de documentación tenga el éxito esperado en su fase de implementación, por ello el proyecto aborda el tema organizativo del CSIRT, mostrando el nivel jerárquico de las dependencias, los cargos que se deben crear y las funciones y responsabilidades que permitirán generar una operatividad de buen nivel para la prestación de servicios del CSIRT a sus clientes.

Para finalizar y como es sabido, toda empresa debe diseñar un manual de políticas de seguridad de la información que maneja en sus procesos, en este proyecto se redactan una serie de medidas que el CSIRT deberá tomar con el fin de garantizar el buen manejo y la seguridad de su información y la de sus clientes, con lo que podrá tener un orden estructurado en todo su archivo histórico y además de ello ofrecer garantías a sus clientes en cuanto a confidencialidad.

1. PLANTEAMIENTO DEL PROBLEMA

El cibercrimen entendido como el acceso no autorizado a sistemas de información y datos de terceros con el fin de vulnerar la confidencialidad, la integridad y la disponibilidad de la información, ha ido en constante aumento a la par del crecimiento tecnológico de las sociedades; una de las causas posibles es el paso de negocios físicos a virtuales y el manejo de dinero desde bancas virtuales, lo que implica un manejo más abierto de los datos. Un ejemplo de la tendencia creciente del cibercrimen a nivel global, según Castaño[1], se puede observar en los más de 2 billones de ataques entre 2018 y 2019, siendo Latinoamérica la que presenta el mayor porcentaje de crecimiento en ataques, pues para 2016 tenía un 28% y para 2018 presentó un aumento de 53% de fraude o crimen económico.

Por otro lado en Colombia los delitos han ido mutando con el tiempo, pasando del escenario físico al virtual; según datos estadísticos del centro cibernético policial[2], el delito cibernético creció 28,3 % en el año 2017 con respecto al año anterior; las principales amenazas cibernéticas de las que han sido víctimas las personas y las empresas han causado impactos negativos que van desde crecimiento de la autolesión o suicidios en la población juvenil, hasta pérdidas económicas individuales y empresariales; de acuerdo el centro cibernético policial, algunas amenazas que se han identificado son:

- Ciber inducción al daño físico: aquí se puede nombrar un caso reconocido el de la famosa ballena azul con sus “retos suicidas”, el cual inducia a la autolesión a través de retos y coacciones a los participantes, quienes en mayor porcentaje eran niños y adolescentes en este tipo amenaza se tiene 508 alertas generadas en Colombia para el año 2017.

- Suplantación de *sim card*: El atacante se presenta como el propietario de la sim para hacer una reposición; ya teniendo en su poder la *sim card* podrá lograr sincronizar redes sociales, correos y cuentas bancarias asociadas al número lo que le permitirá al atacante cometer ilícitos que van desde el saqueo virtual de cuentas hasta la suplantación de identidad ante otras personas y terceros; se han reportado pérdidas cercanas a $7.690.000.000.

- *Vishing*: A través de llamadas los delincuentes obtienen datos bancarios como números de cuentas, claves y datos que generan vulnerabilidades en tarjetas de

[1] CASTAÑO GUTIERREZ, Jorge. Circular externa 007 de 2018. [ONLINE]. Bogotá: Superintendencia Financiera de Colombia, 2018. [Citada: 21 septiembre 2019]. Disponible en: https://fasecolda.com/cms/wp-content/uploads/2019/08/ce007-2018.pdf

[2] COLOMBIA, POLICIA NACIONAL. Balance del cibercrimen en Colombia []ONLINE]. Bogotá: Policía Nacional, 2017. [Citada: 30 septiembre 2019. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

crédito las cuales pueden ser usadas para compras online y otro tipo de estafas como la duplicidad del documento, en 2017 este delito produjo perdidas que ascienden a $2.132.000.000.

- Ciber pirámides: con el auge de las criptomonedas los criminales han aprovechado para estafar a sus usuarios con la creación de pirámides sin ninguna base que respalde las ganancias exorbitantes; en muchos casos se trata simplemente de páginas *fake*, en otros tantos se puede establecer que verdaderamente se generó inversión, pero sin conocimientos sobre el tema se pudieron producir pérdidas que llevaron a la desaparición de la pirámide.

- *Ransomware:* divulgación y penetración de *programa maligno* que habitualmente se ha apoderado de los dispositivos y de la información del usuario y que por medio de correos fraudulentos exigen dineros a cambio de descifrar o retornar la información, para este caso en 2017 se tuvo una cifra de 619520 usuarios impactados.

- Suplantación de correo corporativo: los criminales tratan de engañar a sus víctimas mediante la creación de correos que son casi idénticos a los correos emisores de bancos o entidades oficiales con el fin de lograr transferencias de dinero importantes a cuentas no verificadas, se estima que por cada caso presentado hay una pérdida de 380 millones de pesos.

- El *carding:* mediante la suplantación, la clonación y el cambio de tarjetas, los delincuentes han logrado su objetivo que es desviar dinero ya sea a cuentas propias o generar gastos mediante la compra de productos online que finalmente pueden vender para recuperar el dinero, esta amenaza a producido 60 mil millones de pesos en pérdidas por año en Colombia.

- Estafas por internet: se presentan ventas en las cuales el producto nunca es entregado, uso de llamadas telefónicas, SMS o WhatsApp fraudulentos y las conocidas cartas nigerianas que ofrecen recompensas a través de correo electrónico; actualmente se tienen casos en los que ofrecen curas milagrosas para el COVID-19 a lo que la gente accede a dar dinero por la desesperación de una pandemia.

El cibercrimen tiene un efecto domino sobre los entes atacados ya que puede generar como consecuencia mayor gasto en tecnología para mitigar los riesgos; para entidades financieras y que manejan acciones, estas pueden bajar debido a su reputación; en el sector empresarial en general los empleados pueden tener percepciones de inseguridad sumado a que las relaciones empresariales pueden

vulnerarse o romperse[3]. Ante estas amenazas latentes las empresas se ven obligadas a tener planes de contingencia y manejo de incidencias, ya que es inminente que en algún momento puedan presentarse las consecuencias del manejo inadecuado de la seguridad de la información.

FORMULACION DEL PROBLEMA

Por lo anteriormente descrito se hace necesario plantear la pregunta ¿Cómo se puede implementar un CSIRT que manejé los incidentes cibernéticos y gestión de vulnerabilidades del sector empresarial en Colombia?

[3] CARDONA, Lyda Durley., & URIBE, Andrés. Sistema de gestión de incidentes de seguridad informática para corbeta. [ONLINE]. Medellín: Universidad De San Buenaventura Seccional Medellín, 2015 [Citada: 30 septiembre 2019]. Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/3932/3/Sistema_Gestion_Incidentes_Seguridad_Mona_2015.pdf

2. JUSTIFICACION

Un incidente de Seguridad Informática puede definirse como un suceso que atenta en contra de los pilares básicos de la seguridad informática (la confidencialidad, integridad y disponibilidad), lo que impide la operación normal de los sistemas, las redes y las políticas que protegen los activos de información y la infraestructura tecnológica, según el MINTIC[4] en este sentido este tipo de incidentes viene aumentando sus cifras en Colombia, ya que las personas y empresas han evidenciado un crecimiento en la dependencia hacia el manejo de datos de forma tecnológica, factor que ha favorecido el aumento de cifras del cibercrimen en los últimos años, es por eso que se hace necesario la implementación de un centro de respuesta a incidentes cibernéticos (CSIRT), que tenga la capacidad de apoyar y dar soporte en la prevención, manejo y respuesta a los incidentes de seguridad informática de una forma metódica y privada para las compañías y personas, para así lograr minimizar su ocurrencia y proteger la información que cada cliente determine como valiosa.

Por otra parte, Díaz, Firvida y Lozano[5] proponen que la creación de un CSIRT permitirá el trabajo de expertos responsables del diseño y perfeccionamiento de medidas que logren prevenir y reaccionar ante incidencias de seguridad en los sistemas de información de cada cliente, con lo cual se podrá analizar, establecer y contribuir a mejorar el estado de seguridad de la Infraestructura en el ámbito de tecnología y de los sistemas Informáticos de las compañías, así como prevenir y atenuar incidentes de seguridad graves.

En cuanto a los costos, ORGANIZACION DE LOS ESTADOS AMERICANOS[6], afirma que se debe considerar que, con el funcionamiento de un CSIRT, las empresas podrán tener una respuesta efectiva para limitar el daño potencial y minimizar los costos de una eventual recuperación, esto ocurre gracias a una respuesta focalizada y centralizada frente a los incidentes a partir de la coordinación de un equipo táctico y operativo. Teniendo en cuenta lo anterior, el caso de estudio

[4] COLOMBIA, MINTIC. Guía para la Gestión y Clasificación de incidentes de seguridad de la información. [ONLINE]. Bogotá: Ministerio de las tecnologías de la información y comunicación, 2014. [Citada: 29 septiembre 2019]. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[5] DIAZ, Jesús, FIRVIDA, Daniel y LOZANO, Marco. Identificación y reporte de incidentes de seguridad para operadores estratégicos. [ONLINE]. Madrid: Intecocert, 2013. [Citada:29 septiembre 2019]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/int_cnpic_identificacion_reporte_incidentes.pdf

[6] ORGANIZACION DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. [ONLINE]. Washington: Secretaría General de la Organización de los Estados Americanos (OEA). 2016. [Citada: 4 octubre 2019]. Disponible en https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

CIBERSECURITY de Colombia LTDA, es una empresa que se ha propuesto cubrir esta necesidad en Colombia, prestando el servicio de manejo de incidentes de seguridad, que permita a sus clientes tener bases sólidas y evidencias para realizar procedimientos legales además de los beneficios ya mencionados por parte del CSIRT.

Para lograr la implementación efectiva del CSIRT para el caso de estudio de la empresa CIBERSECURITY de Colombia se hace necesario diseñar una previa documentación de los procesos y procedimientos que permitirán desarrollar las actividades propias del CSIRT, con lo que se logrará que el caso de estudio CIBERSECURITY de Colombia sea pionero y líder en el servicio a prestar teniendo como base estándares de seguridad y buenas prácticas, que permitan a sus clientes minimizar visiblemente las afectaciones de seguridad que se puedan presentar, mediante la reacción inmediata ante ataques que permitan tener como prioridad el restablecimiento del servicio informático y tomando estos como lecciones que suministren experiencia para prever ataques futuros de la misma índole.

Como aporte a la ciencia de la tecnología, la implementación de un CSIRT en las empresas colombianas permitirá a nivel interno que la compañía sume experiencia y busque controles inmediatos y a futuro, que permitirán la documentación de vulnerabilidades y amenazas latentes en la sociedad que ayuden a una comunidad que integran varios CSIRT y están en constante comunicación y crecimiento como lo denota Montoya[7].

El proyecto permitirá un enriquecimiento de conocimientos profesionales, asimilados a partir de la consulta de fuentes de información desde los conceptos más básicos hasta el logro del objetivo general, con lo que se puede beneficiar tanto el desarrollador del proyecto, como también la comunidad educativa ya que los CSIRT es un tema que en Colombia aún tiene un gran potencial de aplicación y que requiere más profundización de estudio.

[7] MONTOYA, German. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. [ONLINE]. Bogotá: Asobancaria. [Citada: 30 septiembre 2019]. Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Documentar el diseño de la implementación del CSIRT para el caso de estudio de la empresa CIBERSECURITY de Colombia Ltda.

3.2 OBJETIVOS ESPECIFICOS

- Analizar la situación actual de la ciberseguridad en Colombia y crear una taxonomía de ataques para el ámbito de actuación del CSIRT.
- Definir el catálogo de servicios del CISRT como herramienta de presentación de la empresa hacia sus clientes.
- Especificar perfiles del equipo de trabajo y la estructura orgánica que conformará el CSIRT.
- Diseñar políticas y procedimientos operacionales del CSIRT.

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL Y TEORICO

La información en la sociedad actual se ha transformado en un bien de consumo, es por ello que nace la necesidad de gestionarla, garantizando la integridad de los datos; por lo que la información ahora es el activo más importante a tratar y salvaguardar en cada organización, el análisis de riesgos informáticos en una empresa es de vital importancia, hay que iniciar afirmando que la información es el núcleo central de cualquier organización y sobre ella recaen procesos que tienen como finalidad el cumplimiento de los objetivos de cada empresa; aunque se considera imposible garantizar un nivel de protección total, esto debido a que se deben tener en cuenta diversos factores como la educación del usuario final, factores ambientales externos no premeditados, incidentes, además y como más importante la creciente ola tecnológica con lo que los datos también crecen y proporcionalmente crecerán también los riesgos y amenazas.

Teniendo en cuenta la publicación de Ramírez[8], los elementos, los activos de información, las vulnerabilidades y las amenazas, de manera conjunta determinan los riesgos, los cuales pueden ser físicos o lógicos; con ello se logra determinar la importancia de la información como un todo fundamental que permite garantizar el buen funcionamiento de cada empresa.

En su artículo Ureña[9] afirma que las consecuencias se deben tener en cuenta para la evaluación de riesgos, principalmente sobre la confidencialidad, la integridad y la disponibilidad de la información como los pilares que garantizan la seguridad informática; además de otro factor que es la probabilidad la cual muestra la posibilidad de que un riesgo ocurra.

La confidencialidad de los datos significa que solo los usuarios autorizados puedan ver dichos datos. El fin de la confidencialidad es permitir que los usuarios autorizados si puedan leer información; con esto la importancia para la empresa es

[8] RAMIREZ CASTRO, Alexandra. Riesgo tecnológico y su impacto para las organizaciones parte i. [ONLINE]. México: Universidad nacional autónoma de México. 2016. [Citada: 30 septiembre 2019]. Disponible en: https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i

[9] UREÑA CENTENO, Francisco. Ciberataques la mayor amenaza actual, [ONLINE]. Madrid: Instituto español de estudios estratégicos. 2015. [Citada: 20 octubre 2019]. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

que ningún usuario no autorizado husmee, vea, edite o suprima información que no le compete o es de carácter privado[10].

La integridad garantiza que los usuarios accedan a la información, pero no la modifique si no cuentan con la autorización necesaria. Por ello en este sentido lo que se debe salvaguardar es la totalidad y la exactitud de los datos. Para las organizaciones es de vital importancia que los datos sean íntegros, una factura, un pagaré, documentos legales deben permanecer íntegros ante cualquier eventualidad.

En un documento público de la Supersalud se evidencia que la disponibilidad de la información se refiere principalmente al acceso a los datos, este debe ser continuo, sin cortes ni interrupciones que comprometan la integridad y tampoco la confidencialidad de los datos[11]. Para las organizaciones de hoy en día este es un pilar de funcionamientos masivo ya que generalmente se requiere acceso total a la información prácticamente 24/7.

4.1.1 Modelos para el manejo de riesgos. En el ámbito de seguridad informática es posible implementar algunos modelos que permitan el manejo de los riesgos informáticos, con ello se puede reducir el impacto que estos producen sobre los activos de información que por consiguiente pone en peligro la estabilidad de una organización; entre estos modelos es posible destacar los que se numeran a continuación.

4.1.1.1 COBIT[12]. Es un modelo aceptado internacionalmente que tiene como fin controlar las herramientas tecnológicas de la información y los riesgos a las que están expuestas; este modelo proporciona herramientas que permiten la conexión entre los controles, los aspectos técnicos y los riesgos, este modelo es gran referente como marco de buenas prácticas aplicables a gobierno TI, siendo así un marco de trabajo de alto nivel que puede integrar otros modelos como lo son ITIL e ISO proporcionando una flexibilidad en su aplicación y enfocándose en el control más que en la ejecución.

[10] LAFRANCO, Einar y PEREZ, Ernesto. CSIRTs. [ONLINE]. Madrid: CERT UNLP. [Citada: 02 octubre 2019]. Disponible en: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

[11] COLOMBIA, Supersalud. Gestión de servicios tecnológicos. [ONLINE]. Bogotá: Supersalud. [Citada: 2 octubre 2019]. Disponible en: https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSPD02.docx

[12] IT GOVERNANCE INSTITUTE. COBIT Marco Referencial. [ONLINE]. Lincoln: Comité Directivo COBIT. 2017. [Citada: 11 septiembre2 2019]. Disponible en: http://files.uladech.edu.pe/docente/02659781/CAT/S07/02_03MarcoReferencial.pdf

4.1.1.2 ITIL (Biblioteca de Infraestructura de Tecnologías de Información). Mundialmente ITIL es un enfoque altamente aceptado de gerencia de servicios de TI, con un gran número de profesionales certificados ya que proporciona un modelo que tiene como resultado la unión de las mejores prácticas del sector público y privado, además, este modelo se encarga de los procesos que se ejecutan dentro de las organizaciones para la administración y operación de la infraestructura de las tecnologías de información, con el fin de proveer los servicios a los clientes teniendo en cuenta los costos acordes a las estrategias del negocio; las principales características de este enfoque es que es un *framework* no propietario, es independiente de proveedores y tecnología, provee terminología estándar además de lineamientos para planteamiento y definición de roles en los procesos.

4.1.1.3 ISO 27001[13]**.** Define requisitos de un SGSI (Sistema de gestión de la seguridad de la información), estableciendo, implantando, documentando y evaluando políticas que permitan la protección de los activos; se basa en un enfoque por procesos con el principio de una mejora continua, por lo cual es altamente compatible y se puede integrar con otros sistemas de gestión existentes en una organización; el eje central de este estándar es la protección de los pilares de la seguridad informática (la confidencialidad, integridad y disponibilidad de la información). Esto lo realiza a través de la investigación referente a los problemas potenciales que pueden afectar la información (evaluación de riesgos), luego propone definir qué hacer para evitar que los problemas lleguen a producirse (mitigación o tratamiento del riesgo).

4.1.2 CSIRT. Según la documentación de FIRST[14] y teniendo como base los riesgos a los que se enfrenta la información se debe abordar el cómo plantear medidas para evitar que las afectaciones sean graves y que sean recuperables en el caso de que se presenten; para ello se analizará y se pondrá a consideración el termino CSIRT. Para el año 1988 se presentó el primer incidente cibernético denominado “Morris” que tenía como intención buscar contraseñas de los ordenadores, como medida se creó CERT en la Universidad Carnegie Mellón, en Pittsburgh, Pensilvania (EE. UU), a partir de aquí los equipos para manejos de incidentes fueron creciendo, pero se diferenciaban su propósito, su financiación, su idioma y sus zonas horarias; esto cambió al aparecer un nuevo gusano llamado “*wank*” que para contraatacarlo generó que se juntaran y coordinaran esfuerzos desde los diferentes equipos de manejo de incidentes lo que creó y fortaleció la comunidad; América Latina logró tener su primer CSIRT en México, su nombre fue

[13] ESCUELA EUROPEA DE LA EXCELENCIA. El Anexo A y los controles de seguridad en ISO 27001. [ONLINE]. Madrid: Escuela Europea de la excelencia. 2019. [Citada: 03 octubre 2019] Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/05/el-anexo-a-y-los-controles-de-seguridad-en-iso-27001/

[14] FIRST. Primera Historia. [ONLINE]. First. 2015. [Citada:16 septiembre 2019]. Disponible en: https://www.first.org/about/history

MX-CERT y fue propuesto por el Instituto Tecnológico y Estudios Superiores de Monterrey (ITESM), llegó a ser miembro del grupo FIRST; actualmente Colombia tiene varios CSIRT registrados a FIRST mencionados en la Figura 1:

Figura 1. CSIRT Colombia en el grupo FIRST

Team	Official Team Name	Country
BS-CSIRT	Cyber Security Operation Center B-SECURE	CO
C-DOC	Cyber Defense Operation Center	CO
CGCSD	Cybersecurity Government Center and Digital Security the Evolution Technologies Group CGCSD	CO
CSIRT Asobancaria	CSIRT Financiero Asobancaria	CO
CSIRT OLIMPIA	COMPUTER SECURITY INCIDENT RESPONSE TEAM OF OLIMPIA DIGITAL	CO
CSIRT-CCIT	Computer Security Incident Response Team of the Colombian Informatics and Telecommunications Chamber	CO
CSIRT-ETB	Computer Security Incident Response Team - Empresa de Telecomunicaciones de Bogotá S.A. ESP	CO
CSIRT-MOC Newnet	Computer Security Incident Response Team of NewNet	CO
CSIRTPONAL	Response Team Computer Security Incident of the Colombian National Police	CO
CSVD-A3Sec	CSVD-A3Sec	CO
DigiCSIRT	DigiSOC Computer Security Incident Response Team	CO
ETEK-CSIRT	Computer Security incident response team of ETEK International	CO
GammaCSOC-CSIRT	Gamma Ingenieros CSOC - CSIRT	CO
ITSSOC-CSIRT	IT SECURITY SERVICES S.A.S SOC CSIRT	CO
ShieldNow	ShieldNow	CO
SOC Team Claro Colombia	Security Operations Center Team Claro Colombia	CO
SOC-CCOC	Security Operations Center - Cyber Operations Command Joint	CO

Fuente: First.org[15], Equipos CSIRT.

Hoy en día un CSIRT es definido como un equipo o unidad de una organización la cual integra personal altamente calificado en seguridad informática, su objetivo radica principalmente en la prevención y en la respuesta inmediata u oportuna ante los incidentes que comprometan los activos de información o la infraestructura tecnológica, además, refuerza la gestión de la seguridad informática de sus usuarios atendidos, a través de la comunicación y coordinación de su trabajo con una red de CSIRT a nivel local y mundial con empresas dedicadas a la protección de seguridad informática[16].

[15] FIRST. Equipos CSIRT. [ONLINE]. First, 2019. [Citada: 17 septiembre 2019]. Disponible en: https://www.first.org/members/teams/?#

[16] UNITED STATS, DEPARTMENT OF DEFENSE. Department Of Defense Trusted Computer System Evaluation Criteria. [ONLINE]. New York: Department Of Defense. 2015. [Citada: 24 septiembre 2019]

4.1.3 Servicios de un CSIRT[17]. Son considerados como servicios reactivos y proactivos; los reactivos requieren de una reacción por petición u ocurrencia, pueden ser análisis de vulnerabilidades, detección de malware, gestión de código malicioso, y toda la gestión ante un incidente informático que va desde el análisis, el tratamiento, el apoyo y la investigación del incidente; mientras que los servicios proactivos proponen anticipar ataques ayudando a proteger y asegurar los sistemas con lo que se trata de disminuir los riesgos a futuro.

4.1.4 Ámbitos de un CSIRT[18]. Una de las formas de clasificar un CSIRT es por medio de su ámbito de actuación, lo que permite hacer una agrupación sectorizada de la comunidad o del tipo de organizaciones a quienes presta sus servicios, a continuación, se proporciona un listado de algunos CSIRT clasificados según su que actualmente se encuentran en constante operación, ver tabla 1.

Tabla 1. Ámbitos de los CSIRT

Ámbitos de CSIRT	Detalle
CSIRT comerciales	Venden el servicio de atención de incidentes a clientes que no quieren o no tienen los recursos para montar un CSIRT propio.
CSIRT de infraestructuras críticas	Prestan servicios a sectores públicos o privados de los cuales dependen los procesos más importantes para el desarrollo y fines de uno o varios sectores de la nación.
CSIRT gubernamentales	Brindan seguridad a la información de los entes gubernamentales
CSIRT nacionales	Asume el papel de coordinador nacional de incidentes informáticos
CSIRT del sector militar	Prestan servicios a los entes e instituciones militares de un país.
CSIRT de proveedores	Son destinados a prestar servicio sobre incidentes a productos específicos
CSIRT del sector PYME	Se centran en ayudar a las PYME y a ciudadanos
CSIRT académico	Atienden universidades, colegios, comunidades académicas

Fuente: elaboración propia.

[17] GORGONA, Luis. Primera respuesta: antes de que llegue la policía. [ONLINE] México: OAS, 2018 [Citada: 3 octubre 2019]. Disponible en: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

[18] ENISA. Cómo crear un CSIRT paso a paso. [ONLINE]. Enisa. [Citada: 4 octubre 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

4.2 MARCO TECNOLOGICO

Para el tratamiento de incidentes, un CSIRT necesita algunas herramientas tecnológicas básicas que permitan ejecutar el objetivo principal de la organización el cual es garantizar que no se presenten incidentes de seguridad y si estos se llegaran a presentar se logren mitigar los daños al máximo, por lo que es de gran importancia contar con instrumentos como los que se numeran a continuación

4.2.1 RTIR. En su página oficial[19] muestra a RTIR como una herramienta que ayuda a equipos de respuesta a incidentes proporcionando colas y flujos de trabajo, correlacionando datos clave del manejo de incidentes que permiten encontrar patrones y vincular múltiples informes de incidentes con un incidente de causa raíz. Este software permite a un usuario crear una incidencia, con lo que un equipo de soporte hace la respectiva revisión para aprobación, rechazo y trabajos adecuados sobre el incidente, finalmente se hace un cierre del caso haciendo un informe detallado de los hechos; cabe destacar que RTIR tiene un licenciamiento *open source* y su uso es gratuito por lo que cada organización puede adaptarlo a sus propias necesidades constituyéndose como herramienta importante al momento de manejar incidentes.

4.2.2 Herramientas CRM. *Customer Relationship Management* o por su nombre traducido gestión de relaciones con clientes, permite el manejo estratégico de clientes, logrando un manejo eficiente de estos dentro de la organización, este software tiene como objetivo principal ganar, analizar, atraer y retener clientes[20]; además con ello se puede mejorar la comunicación dentro de la organización y hacer que el personal sea más productivo y organizado en sus labores.

4.2.3 Herramientas para verificación de la información. Permiten hacer búsquedas selectivas y actualizadas de información relacionada a un objetivo general; para el caso del manejo de incidentes es correcto usar algunas de estas herramientas como son *website checker* la cual tiene una licencia de uso comercial y permite hacer un constante monitoreo para detectar en tiempo real los cambios realizados sobre una página web; otra herramienta de este tipo es *whatch that page* la cual tiene una versión gratuita con algunas limitantes en su funcionalidad y una versión comercial con más funciones habilitadas, esta permite enviar correos electrónicos cuando se

[19] RTIR. *Best Practical*. [ONLINE] *Best Practical*. [Citada 12 septiembre 2019] Disponible en: https://bestpractical.com/rtir

[20] MONTOYA AGUDELO, Cesar y BOYERO SAAVEDRA, Martin. El CRM como herramienta para el servicio al cliente en la organización. [ONLINE]. Medellín: Revista Científica "Visión de Futuro". 2012. [Citada: 23 septiembre 2019]. Disponible en: https://www.redalyc.org/pdf/3579/357935480005.pdf

produzcan cambios en una página web determinada.

4.2.4 Herramientas de encriptación. Estas herramientas permiten encapsular la información con lo que cualquier dato será cifrado e ilegible ante cualquier visualización, esto gracias a algoritmos que logran desordenar sus componentes, por lo que solo con las claves correctas y el algoritmo preciso los datos podrán ser legibles, dentro de estas herramientas están *GNUPG* la cual permite cifrar datos y comunicaciones con la administración de claves versátil, es de código abierto por lo que las organizaciones podrán editar y adaptar a sus necesidades.

4.2.5 Herramientas de obtención de datos volátiles de memoria. En toda investigación se debe hacer la recolección de datos volátiles, esto con el fin de garantizar un proceso investigativo integro preservando la evidencia catalogada como volátil y adicionando a ello *logs* que permitan responder preguntas del caso de forma rápida y eficaz sin realizar *Backups* sobre las unidades expuestas, reduciendo así los riesgos de perdida de datos en un incidente.

- Lime para UNIX / LINUX: Se usa desde un dispositivo USB conectado en los sistemas u ordenadores afectados.

- *Volatilly:* al igual que el anterior se usa desde un dispositivo USB sobre el sistema afectado.

- En Windows hay herramientas como *FTK imager, DumpIT o MemoryDD* los cuales realizan un volcado de la memoria del sistema.

4.2.6 Kali linux[21]. Es un proyecto de código abierto que es mantenido y financiado por *Offensive Security*, un proveedor de servicios de prueba de penetración y capacitación de seguridad de la información de clase mundial. Este sistema operativo tiene gran número de herramientas para realizar auditorías informáticas con lo que se puede lograr detección de vulnerabilidades y poder gestionar los riesgos de los sistemas informáticos.

[21] KALI LUNUX. Kali Linux By Offensive Security. [ONLINE] 2019. [Citada: 23 septiembre 2019] Disponible en: https://www.kali.org/

4.3 MARCO LEGAL

Legalmente la ciberseguridad en Colombia está fundamentada en varios documentos y artículos generados desde el gobierno central y sus ministerios reconociendo tratados internacionales con Interpol y Europol por lo que es conveniente citar a continuación los referentes en cuanto a la seguridad de la información y la ciberseguridad en Colombia:

4.3.1 Conpes 3701 de 2011. Este documento establece una política de ciberseguridad en el país, estableciendo una línea que permite dar respuesta a situaciones de riesgo de seguridad informática a cargo de la policía y las fuerzas militares de la nación, el conpes 3701 de 2011 está basado en tres acciones principales que se citan a continuación[22]:

- Adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten.

- Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en DEFENSA CIBERNETICA y CIBERSEGURIDAD.

- Fortalecer la legislación en estas materias, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales.

4.3.2 Ley 527 de 1999[23]. Es un marco legal para generar contratos y negocios por medios electrónicos, este documento se compone de dos capítulos, el primero detalla el valor jurídico y probatorio de los mensajes electrónicos y el segundo capítulo permite observar información acerca de regulación de entes encargados de generar firmas digitales.

[22] COLOMBIA, PLANEACION NACIONAL. Documento conpes 3701. [ONLINE]. Bogotá: Departamento Nacional de Planeación, 2011. [Citada: 24 septiembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[23] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527 de 1999. [ONLINE]. Bogotá: República de Colombia, 1999. [Citada: 27 septiembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

4.3.3 Ley 594 de 2000[24]. Esta ley dentro de sus contenidos establece y regula los principios archivísticos desde el panorama de la seguridad de la información, el tratamiento de los datos y la conservación de estos, regulando así las buenas prácticas dentro del archivo público que pueden ser llevadas al archivo privado también.

4.3.4 Ley 679 de 2001[25]. Esta ley le hace frente a lo concerniente con la pornografía infantil, genera responsabilidades a los ISP sobre el contenido que los usuarios podrán mover o manejar en el ciberespacio, en él se establecen lineamientos claros acerca de las prohibiciones y deberes tanto de los usuarios del servicio de internet como los proveedores.

4.3.5 Ley 962 de 2005[26]. Este marco normativo establece normas en las que se simplifica y racionaliza los tramites que se deben llevar a cabo ante entidades públicas por lo que se debe instaurar atributos sobre la seguridad de la información electrónica que manejan estas entidades del sector público o que prestan servicios públicos.[27]

4.3.6 1150 de 2007[28]. Brinda normatividad acerca de la contratación en línea y la seguridad electrónica a aplicar sobre esta; además vela por la eficiencia y la transparencia sobre el cumplimiento de la ley 80 de 1993 la cual brinda lineamientos acerca de la contratación pública para lo cual se desarrolla el sistema electrónico para la contratación pública, o mejor conocido por sus siglas SECOP.

---

[24] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 594 de 2000. [ONLINE]. Bogotá: Congreso de la República, 2000. [Citada: 27 septiembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-15049_documento.pdf

[25] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 679 de 2001. [ONLINE]. Bogotá: Congreso de la República, 2001 [Citada: 27 septiembre 2019]. Disponible en: http://www.oas.org/juridico/spanish/cyb_col_ley_679_2001.pdf

[26] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 962 de 2005. [ONLINE]. Bogotá: Congreso de la República. 2005. [Citada: 27 septiembre 2019]. Disponible en: http://www.aguasdebuga.net/intranet/sites/default/files/Ley%20962%20de%202005-

[27] COLOMBIA, PLANEACION NACIONAL. Documento conpes 3701. [ONLINE]. Bogotá: Departamento Nacional de Planeación, 2011. [Citada: 24 septiembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[28] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1150 de 2007. [ONLINE]. Bogotá: Congreso de la República. [Citada: 27 septiembre 2019]. Disponible en: https://www.mintransporte.gov.co/descargar.php?idFile=711

4.3.7 Ley 1273 de 2009[29]. Define a la información como bien jurídico tutelado y muestra los diferentes delitos Informáticos y las penas a las que se ven expuestos sus infractores, teniendo como principal referente el código penal a quienes usen los sistemas de información y los medios electrónicos o telemáticos para desarrollar conductas determinadas para este articulo como criminales.

4.3.8 Ley 1341 de 2009[30]. También conocida como ley de tecnologías de la información y las comunicaciones (TIC), define conceptos y principios sobre la sociedad de las tecnologías de la Información y la aplicación de seguridad, resaltando que las TIC son pilares fundamentales de una sociedad evolutiva por lo que se debe proveer de protección al usuario y la formación de talento para el fortalecimiento de la infraestructura.

4.3.9 Ley 1437 de 2011[31]. Garantiza los derechos y libertades de las personas, además muestra los criterios y políticas de seguridad sobre plataformas tecnológicas, las cuales se aplican a toda entidad u organismo del sector público, quienes deben utilizar medios electrónicos para hacer valer los derechos de las personas a través de actuaciones y procedimientos administrativos.

4.3.10 Ley 1480 de 2011[32]. Esta ley permite proteger al consumidor que realiza sus transacciones y movimientos bancarios o de divisas por medios electrónicos, mediante el establecimiento de criterios que garantizan la seguridad del usuario, de la plataforma que presta el servicio (pasarelas de pago) y de la entidad u organización que recibirá los dineros producto de dicha transacción.

[29] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273 de 2009. [ONLINE]. Bogotá: Congreso de la República, 2008 [Citada: 27 septiembre 2019]. Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

[30] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1341 de 2009. [ONLINE]. Bogotá: Congreso de la República, 2009 [Citada: 27 septiembre 2019]. Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

[31] COLOMBIA, CONGRESO DE LA REPÚBLICA Ley 1437 de 2011. [ONLINE]. Bogotá: Congreso de la República, 2011 [Citada: 27 septiembre 2019]. Disponible en: https://camaratulua.org/wp-content/uploads/2016/02/CoDIGO_DE_PROC._ADMINISTRATIVO.pdf

[32] COLOMBIA, CONGRESO DE LA REPÚBLICA Ley 1480 de 2011. [ONLINE]. Bogotá: Congreso de la República, 2011 [Citada: 27 septiembre 2019]. Disponible en: https://www.wipo.int/edocs/lexdocs/laws/es/co/co103es.pdf

4.3.11 Decreto Ley 019 de 2012[33]. Este decreto logra estandarizar los tramites a través de medios electrónicos y establece criterios de seguridad sobre estos procesos, siendo su principal objetivo el eliminar trámites innecesarios en el sector público garantizando el cumplimiento de sus deberes y procurando la aceptación de los derechos de los ciudadanos a través de la transparencia y la eficiencia en los procesos.

4.3.12 Ley 1581 de 2012[34]. Mediante esta ley el gobierno central dicta y establece disposiciones generales acerca de la protección de datos personales de cada ciudadano en cuanto a la información que repose en bases de datos, para la cual el usuario y/o ciudadano tiene derecho a solicitar actualización, información o eliminación total o parcial si él así se requiere.

4.3.13 Ley 1712 de 2014[35]. Gracias a esta ley se promueve el principio de transparencia, en ella se dictan disposiciones generales del derecho que tienen los ciudadanos al acceso a la información pública, así como también las excepciones normativas establecidas por la ley o por la constitución política que intervienen en la publicación de información.

4.3.14 Resolución 8934 de 2014[36]. Esta resolución establece directrices concernientes a gestión documental y a la organización de archivos que deben cumplir las organizaciones vigiladas por la superintendencia de industria y comercio, en ella se parametriza la producción, recepción, distribución, organización, conservación, recuperación y consulta de la información teniendo en cuenta el medio en que se encuentra.

[33] COLOMBIA, PRESIDENCIA DE LA REPÚBLICA. Decreto Ley 019 de 2012. [ONLINE]. Bogotá: Presidencia de la República. [Citada: 27 septiembre 2019]. Disponible en: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/Decreto-Ley-019-de-2012-Antitramites.PDF

[34] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012. [ONLINE]. Bogotá: Congreso de la República, 2012 [Citada: 27 septiembre 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[35] COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1712 de 2014. [ONLINE]. Bogotá: Congreso de la República. [Citada: 27 septiembre 2019]. Disponible en: http://www.anticorrupcion.gov.co/SiteAssets/Paginas/Publicaciones/ley-1712.pdf

[36] COLOMBIA, SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 8934 de 2014. [ONLINE]. Bogotá: Superintendencia de industria y comercio, 2014. [Citada 28 abril 2020]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?id=4041484

4.4 MARCO ESPACIAL

El estudio se basa en el alto índice de la criminalidad cibernética y de los incidentes cibernéticos presentados en los últimos años, por lo cual nace la necesidad de la implementación de un CSIRT como mecanismo de defensa ante los delitos informáticos y riesgos de orden tecnológico hacia los activos de información, por ello la documentación tiene un orden espacial sobre las organizaciones colombianas que deseen una compañía que haga la identificación, análisis, respuesta y control de los incidentes que se puedan presentar. La empresa caso de estudio Cibersecurity de Colombia desempeñara las labores de CSIRT desde Bogotá – Colombia y tendrá su mercado o aplicación principal en organizaciones nacionales que no tengan el interés por implementar un CSIRT o no cuenten con los recursos suficientes para ponerlo en marcha.

4.5 MARCO METODOLOGICO

El modelo de investigación a usar para este proyecto es cualitativo teniendo en cuenta que la información que se va a estudiar no pretende presentar el conocimiento desde la exactitud numérica sino desde la comprensión y profundización del tema de estudio; el tipo de investigación a utilizar se denomina investigación aplicada la cual tiene por objetivo la resolución de una situación o problema específico, basado en la búsqueda y consolidación de conocimiento para la aplicación práctica del caso de estudio CIBERSECURITY de Colombia LTDA.

Las técnicas a utilizar dentro del desarrollo del presente proyecto son la consulta bibliográfica y documental[37], la cual garantiza los fundamentos teóricos del proyecto, se tendrá un proceso sistemático y secuencial de recolección de información, luego se implementara una selección, clasificación, evaluación y análisis de contenido del material recolectado (conocimientos empíricos, material impreso, medios gráficos, evidencias físicas y/o virtuales) que sirva de fuente teórica, conceptual y metodológica para el proyecto, que permita de esta manera realizar la documentación de la implementación de un CSIRT para la empresa caso de estudio Cibersecurity de Colombia LTDA. Además de ello se hará uso de la técnica de indagación e interpretación de datos utilizando la encuesta a administradores IT como herramienta para determinar los incidentes de seguridad de la información que más se presentan en las organizaciones en las que desarrollan sus labores.

[37] VARGAS CORDERO, Zoila Rosa. La investigación aplicada: una forma de conocer las realidades con evidencia científica. [ONLINE]. San Pedro: Universidad de Costa Rica, 2009. [Citada: 27 septiembre 2019]. Disponible en: https://www.redalyc.org/pdf/440/44015082010.pdf

El proyecto analizará el ámbito de aplicación del CSIRT que para este caso son los clientes del caso de estudio CIBERSECURITY de Colombia quienes al depender de entes tecnológicos para la prestación de sus servicios y por ello están expuestos a ataques y explotación de vulnerabilidades que puedan generar afectaciones en el funcionamiento normal de sus sistemas.

El documento se desarrollará en 4 fases las cuales darán cumplimiento a los objetivos específicos planteados para el proyecto, dentro de dichas fases se realizará tareas investigativas y se documentara todo lo concerniente al CSIRT de la empresa caso de estudio CIBERSECURITY de Colombia LTDA, por lo que se distribuirán de la siguiente forma:

4.5.1 Fase 1: Estudios preliminares**.** Para iniciar se hace un análisis de la actualidad de la ciberseguridad en Colombia y una identificación de los incidentes cibernéticos de mayor ocurrencia basados en estadísticas y boletines brindados por paginas oficiales de entidades dedicadas al control de este tipo de sucesos, con esto y un estudio de factibilidad se puede determinar los puntos de actuación del CSIRT y la taxonomía de ataques que se manejaran.

4.5.2 Fase 2: Estructuración de los servicios del CSIRT. Se diseña un catálogo de servicios, donde se describe detalladamente los servicios reactivos, proactivos y de valor agregado que prestará el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA logrando así que estos se adapten a la necesidad y exigencias del cliente.

4.5.3 Fase 3: Estructura orgánica del CSIRT**.** Dentro de la documentación de este proyecto se encuentra un manual de funciones donde se define de manera detallada los perfiles del personal que integrará el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, lo que permitirá la caracterización y asignación de las actividades de cada profesional o colaborador.

4.5.4 Fase 4: Políticas operacionales del CSIRT. Con el diseño de manuales operativos que apoyaran las tareas y operaciones del CSIRT se garantiza el manejo de un paso a paso en cada actividad a desarrollar en el CSIRT; con lo que es posible hacer la estructura orgánica, la cual dará una claridad jerárquica a partir de funciones y tareas del cómo se gestionará el CSIRT de manera interna para lograr los objetivos en la prestación de servicios a sus clientes.

5. FASE 1: ESTUDIOS PRELIMINARES.

5.1 PANORAMA ACTUAL DE LA CIBERSEGURIDAD EN COLOMBIA

Con la constante dependencia de la tecnología en los diferentes procesos tanto en enfoque público como en organizaciones privadas se ha hecho necesaria contar con diferentes soportes que puedan garantizar la seguridad sobre las TIC en el territorio nacional; en la constitución política de Colombia[38] se encuentran algunos fundamentos enfocados en la ciberseguridad y tratamiento de la información los cuales se resumen a continuación.

5.1.1 Artículo 2. Establece que la finalidad esencial del estado está dirigida sobre la comunidad, sirviéndola y promoviendo la prosperidad general, garantizando los principios, derechos y deberes que se han consagrado en la constitución política de Colombia al igual que el estado debe garantizar la participación en decisiones que afecten la economía, la política, la vida administrativa y el factor cultural en la nación.

5.1.2 Capítulo 1 del título II artículo 15. Registra el derecho a un buen nombre además de la intimidad de cada persona y de su familia, siendo el Estado quien deba respetar y hacerlos respetar. Además de ello dicta generalidades para que los ciudadanos tengan derecho a solicitar edición, adición o eliminación de sus datos personales de bases de datos de organizaciones públicas y privadas.

5.1.3 Artículo 20. Este artículo de la constitución política dicta medidas que permiten garantizar la libertad de expresión y la difusión del pensamiento de los ciudadanos, a su vez el derecho a enviar y recibir información veraz promueve la no censura y el esparcimiento de información con fines sociales para la nación.

5.1.4 Artículo 101. Este articulo considera como una parte de la nación o del estado el espectro electromagnético y el espacio donde este actúa, además de archipiélagos, islas, islotes y límites establecidos por el congreso y aprobados por la presidencia de la republica ante entes de fiscalización internacional.

[38] REPÚBLICA DE COLOMBIA. Constitución Política de Colombia. [ONLINE] Bogotá: Asamblea constituyente República de Colombia. [Citada: 27 septiembre 2019]. Disponible en: http://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf

5.1.5 Artículo 217. El desarrollo de este articulo refiere que teniendo en cuenta lo dictado en el artículo 101 que considera el espectro electromagnético y su espacio como parte del territorio de la nación, las Fuerzas Militares tienen como fin defender esta soberanía y todo lo que haga parte de la nación según el orden constitucional.

5.1.6 Ley 1273 de 2009. Esta ley genera mecanismos penales que permiten proteger la información y de los datos además de preservar los sistemas de información y comunicación: también fue modificado en 2011, con la ley 1453. Con lo que se puede inferir que Colombia tiene una legislación con fundamentos bien cimentados para el manejo de delitos informáticos, teniendo en cuenta que las fuerzas del orden y la rama judicial son los encargados del manejo e investigación de los delitos cibernéticos presentados en la nación.

5.1.7 Ley 1581 de 2012. La cual plantea lineamientos enfocados en la protección y tratamiento de datos, siendo La Superintendencia de Industria y Comercio la encargada de todo el manejo y protección de datos; adicional a lo anteriormente mencionado hay varios instrumentos que dictan normas relacionadas con la ciberseguridad en temas referentes al comercio en línea, la pornografía y la explotación sexual de menores de edad en medios electrónicos, los trámites y procedimientos en línea y los derechos de autor; Además en Colombia se ha ido reglamentando diferentes mecanismos de autenticación, así como el habeas data, la firma electrónica, las instituciones de certificación abierta y el registro nacional de bases de datos.

5.1.8 Actos administrativos y decretos. Algunos que se pueden considerar de relevancia en el entorno digital son la circular externa 052 de 2007 la cual brinda lineamientos de seguridad referentes al manejo de información en canales de distribución de productos y servicios financieros; la resolución 3066 y 3067 de 2011 que establece derechos de los usuarios de servicios de comunicaciones, el decreto 1704 de 2012 que brinda potestad a un juez para ordenar la interceptación de comunicaciones para apoyar procesos investigativos, además del decreto 2573 de 2014 que aporta los requerimientos generales para la implementación del gobierno en línea; en cuanto a políticas encaminadas a la ciberseguridad nacional se pueden nombrar:

5.1.9 Conpes 3701 de 2011[39]. Busca plantear lineamientos claros que permitan desarrollar políticas de seguridad y la defensa cibernética, está encaminada a desplegar estrategias nacionales que eviten el aumento de amenazas a la

[39] REPUBLICA COLOMBIANA. Documento conpes 3701. Bogotá: Departamento Nacional de Planeación. Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

infraestructura TI o a los activos de información que afectan la nación, los indicadores de cumplimiento según el DNP en 2015 muestran un cumplimiento del 79% sobre los objetivos y actividades de este documento CONPES.

Al validar los resultados principales se concluye que ha brindado a la institucionalidad mayores herramientas para el manejo de la temática de ciberseguridad con la creación del COLCERT, CCOC, CCP, CSIRT PONAL, un ente encargado de la protección de los datos en la Superintendencia de Industria y Comercio, una Subdirección en el ministerio de tecnologías encargada de la seguridad y privacidad de las TIC; además la ciberseguridad es definida como la capacidad de reacción del estado que permite minimizar al máximo la magnitud de los riesgos cibernéticos a los que están expuestos los ciudadanos y pueda afectar la soberanía del estado, se crearon las unidades cibernéticas de las fuerzas militares, se creó la CNDIE (comisión nacional digital y de información estatal), cuyo objetivo es coordinar y orientar la ejecución de las funciones y los servicios públicos concernientes con el tratamiento de información del ámbito público del estado colombiano; además de ello se pudo hacer que la información sea un bien jurídico juramentado.

En 2013 Colombia se unió a la Convención de Europa sobre criminalidad cibernética, y se pudo establecer el convenio con el Foro Económico Mundial, que permite la identificación y manejo de los riesgos de los sistemáticos informáticos globales; se logró el trabajo conjunto con varios (CSIRT) de la región haciendo que Colombia conforme la red de alerta que brinda formación técnica sobre políticas nacionales acerca de seguridad informática.

El CCP de la policía cooperación agencias internacionales como la INTERPPOL, el FBI, la DEA, el EC3, la AMERIPOL, KOICA), NCA, la división de delitos informáticos de la INTERPOL (GLDTA) y el ATA. Todo ello para ser apoyo y tener apoyo en el combate del cibercrimen; Colombia cuenta con 8 CSIRT en el FIRST[14] lo cual promueve una cultura del combate en contra del cibercrimen en el país

En el año 2014 el presidente Santos, autorizo formar una comisión encargada de las políticas de ciberseguridad de la nación, esta fue encabezada por los ministros de Defensa, de Justicia y además del ministro de Tecnologías de la Información y las Comunicaciones (TIC), acompañados desde el ámbito internacional; trabajaron entre los años 2014 y 2015 de la mano de miembros del CCOC, del COLCERT ,del CCP, de las Fuerzas Militares con sus unidades cibernéticas, como también del sector público y privado, la OEA, del Consejo de Europa y de la INTERPOL; gracias a todo el análisis fundamentado se logró la transición de diseñar estrategias de ciberseguridad y defensa cibernética, hacia el diseño de la gestión de riesgos de seguridad digital.

5.1.10 Conpes 3854 de 2016[40]. Este documento se enfoca para que la sociedad colombiana, los entes gubernamentales y las organizaciones privadas sean conscientes de los riesgos que tienen en el entorno cibernético y con ello implementen políticas que permitan prevenir y reaccionar con lo que se logre mitigar el impacto que produzcan los delitos y ataques cibernéticos.

Esta política propone realizar campañas educativas y de concientización como punto de identificación de riesgos cibernéticos a los que están expuestos los colombianos con el uso del internet de las TIC, a partir de la auto prevención y el autocuidado ante delitos y los ataques cibernéticos, para lograr la implementación de estas políticas se tienen en cuenta los siguientes ejes:

- La gestión de riesgos será la base para lograr la seguridad digital.

- Generar confianza en el uso de las TIC que permitan el desarrollo de actividades socioeconómicas a partir de la gestión y tratamiento de los riesgos.

- La gestión y tratamiento de los riesgos permitirá el fortalecimiento de la seguridad del estado y de los individuos.

- La gestión y tratamiento de los riesgos permitirá el Fortalecimiento de la seguridad y defensa de la soberanía del estado desde el entorno digital.

- Implementación de la colaboración en temas de ciberseguridad desde organizaciones nacionales e internacionales

A pesar de las políticas, legislaciones y entes encargados de la ciberseguridad no se ha podido evitar que Colombia sea uno de los países más atacados por el cibercrimen en Latinoamérica, así lo demuestra el siguiente grafico de detecciones de código malicioso de FILECODER en Latinoamérica en el año 2018, siendo Colombia el país en Latinoamérica que más ataques recibió, ver Figura 2.

[40] COLOMBIA, PLANEACION NACIONAL, Op. Cit., p. 32

Figura 2. Ataques cibernéticos en Latinoamérica año 2018

Fuente: Galán[41], Colombia, el país de Latinoamérica más afectado por el *Ransomware*

5.2 ESTUDIO DE FACTIBILIDAD

5.2.1 Demanda y consumidor. Según la firma SOPHOS, Colombia es el país que más ataques cibernéticos ha recibido a través de sitios web maliciosos con corte al año 2018, con una muestra de 200 encuestados el 49% recibió este tipo de ataques, según el informe 'El rompecabezas imposible de la ciberseguridad' esto deja claro que se hace necesario entes encargados de la ciberseguridad, los consumidores principales serán organizaciones con infraestructura tecnológica e información que pueden presentar riesgos y deseen proteger sus activos ante estas amenazas.

5.2.2 Estudio de mercado. Este estudio permite obtener información con lo cual la organización genera estrategias para mejorar la competitividad de Cibersecurity de Colombia LTDA frente a los servicios prestados por empresas u otras organizaciones similares; por lo que se debe tener en cuenta la información que se enumera a continuación.

[41] GALAN, Ricardo. Colombia, el país de Latinoamérica más afectado por el *Ransomware* [ONLINE]. Bogotá: FILECODER, 2019. [Citada: 3 octubre 2019]. Disponible en: https://libretadeapuntes.com/2019/01/colombia-el-pais-de-latinoamerica-mas-afectado-por-el-ransomware/

5.2.2.1 Competencia en el mercado. Según el Foro de Equipos de Respuesta a Incidentes de Seguridad (FIRST) Colombia cuenta con 17 equipos de respuesta a incidentes de seguridad entre sus miembros; nombrados en la Figura 1. Además, también es posible nombrar al CSIRT DIGIWARE y al de ASOBANCARIA que no son miembros de FIRST.

5.2.2.2 Proveedores. Entendiendo el termino proveedores como personas o empresas que abastecen al CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA de herramientas y servicios para que logre el desarrollo de sus actividades a partir de la transformación o su uso, se citan a continuación en el cuadro 1.

Cuadro 1. Proveedores

Uso	Herramienta	Licencia	Proveedor
Encriptación de correo electrónico	GNUPG	Herramienta de uso gratuito.	https://gnupg.org/
	PGP	Uso comercial, se debe adquirir licencia.	Symantec
Tratamiento de incidentes	RTIR	Herramienta de uso gratuito y open *source*.	BEST PRACTICAL
CRM	SUGARCRM	Herramienta licenciada.	https://www.sugarcrm.com/
Verificación de la información	WEBSITE WATCHER	Herramienta licenciada.	AIGNESBERGER Software GMBH
Auditoria y análisis forense	Kali *linux*	Herramienta de uso gratuito.	https://www.kali.org
Equipos tecnológicos	HARDWARE	Licencias de acuerdo con el uso que se dará.	CASTOR DATA SAS
Fuente: El Autor			

5.2.3 Estrategia comercial. A continuación, se analizan un conjunto de prácticas y acciones que permitirán sacar a flote y posicionar en el mercado los servicios prestados por el CSIRT de la empresa caso de estudio Cibersecurity de Colombia.

5.2.3.1 Plaza. El alcance que tendrá el CSIRT de la empresa caso de estudio Cibersecurity de Colombia serán principalmente todas las organizaciones que manejan infraestructura TI y activos de información que pueden presentar riesgos o incidentes de seguridad informática y deseen un CSIRT que pueda gestionarlos garantizando el menor daño posible.

5.2.3.2 Promoción. El equipo de marketing será el encargado de los canales de promoción de la organización los cuales serán vía electrónica, por medio de correos presentando un completo portafolio de servicios, por medio de un portal web que genere confianza tanto en clientes prevalentes como en posibles nuevos clientes, redes sociales, publicidad digital y en medios de comunicación masivos.

5.2.3.3 Producto. El servicio del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA se hace indispensable para empresas que manejan activos de información e infraestructura tecnológica en un mundo cambiante, lo que genera a diario nuevos riesgos que podrían producir incidentes de seguridad informática, por ello las organizaciones podrán acceder a los servicios, sin tener que implementar su propio CSIRT lo que produciría una reducción considerable de costos.

5.2.3.4 Demanda estimada. Después de la implementación del CSIRT, según el estudio de demanda estimada es que tendrá el manejo de incidentes de 20 empresas, organizaciones o clientes durante el primer año, estimando un crecimiento mínimo del 10% por año, durante los próximos 3 años y del 30% anual en los siguientes 5 años.

5.2.4 Estudio legal. Se deben seguir los requisitos que exige la cámara de comercio, necesarios para la creación de una empresa según la ley colombiana se deben crear estatutos del CSIRT, realizar la actualización del RUT y del representante legal, tramitar una autorización de la DIAN para la facturación física y electrónica, verificar la inscripción contable ante cámara de comercio y hacer los trámites pertinentes para la creación de cuentas bancaria a nombre de la empresa.

5.2.5 Estudio de impacto social. El CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA puede generar una reducción de los delitos informáticos sobre la infraestructura tecnológica y activos de información de las empresas u organizaciones contratantes, permitiendo así el fortalecimiento de la confianza en la institucionalidad, el manejo de datos electrónicos y la credibilidad entre usuarios y organizaciones gracias al manejo seguro de información.

5.2.6 Evaluación financiera. La evaluación financiera mostrada en la tabla 2, evidencia un flujo de caja de 70 millones para el año uno y de 84.700.000 para el año tres con el crecimiento constante del 10% sobre los ingresos teniendo en cuenta que se obtendrá 1 millón de ingresos mensuales por cada empresa a la que se maneje los incidentes informáticos, lo que anualmente serian 12 millones anuales;

lo anterior evidencia una factibilidad aceptable teniendo en cuenta el flujo de ganancia y la suma al capital para el fortalecimiento de la empresa.

Tabla 2. Evaluación Financiera

Descripción	Año 1	Año 2	Año 3
Ingresos	240.000.000	264.000.000	290.400.000
Egresos	170.000.000	187.000.000	205.700.000
Depreciación	10.000.000	11.000.000	12.100.000
Flujo de caja	70.000.000	77.000.000	84.700.000

Fuente: elaboración propia.

Se concluye que la implementación de un CSIRT en el ámbito comercial es viable ya que la mayoría de los administradores TI de las organizaciones encuestadas refieren haber sufrido incidentes informáticos en el transcurso de los dos últimos años y estarían dispuestos a requerir un servicio de manejo de incidentes informáticos de manera contratada.

5.3 TAXONOMIA DE ATAQUES

Para realizar la taxonomía de ataques que manejara el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA se define el cuadro 2 en el que se realiza una clasificación y jerarquización de los incidentes y una breve descripción de ellos, teniendo en cuenta la información brindada por INCIBE[42].

[42] INCIBE. Taxonomía de ataques. [ONLINE]. Madrid: INCIBE-CERT, 2019 [Citada: 17 octubre 2019]. Disponible en: https://www.incibe-cert.es/taxonomia

Cuadro 2 .Taxonomía de ataques

Clasificación de ataques o incidentes	Incidente o ataque	Descripción
Contenido abusivo	*Spam*	Correo electrónico no requerido, tienen como finalidad hacer publicidad, causar molestias, llenar buzón de entradas.
	Copyright	Ataques a la propiedad intelectual de los autores
	Explotación sexual infantil/Racismo /Incitación a violencia	Pornografía infantil, distinción de razas o superioridad innecesaria, incitación, generación o provocación de odio o violencia.
Código malicioso	Virus	Código diseñado para explotar vulnerabilidades con la identificación y mal uso de puertos abiertos, modificación, eliminación, daño o robo de información, alteración de sistemas informáticos
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Recopilación de información	Escaneo	Ataque que permite la obtención de información de puertos, abiertos, de nombres de equipos informáticos, DNS
	Sniffing	Análisis del tráfico de red en el que pueden capturar información sensible
	Ingeniería Social	Uso de técnicas y herramientas que permiten la obtención o recopilación de información a partir de la interacción del eslabón más débil de la seguridad informática (el usuario - persona).
Intentos de intrusión	Explotación de vulnerabilidades	Intentos por comprometer un servicio o Sistema informático a partir de la explotación de vulnerabilidades ya identificadas.
	Intentos de *login*	Uso de técnicas y herramientas para descifrar claves de usuario, por medio de fuerza bruta, diccionarios y *cracking*.
	Nuevos ataques	Intentos por explotar vulnerabilidades aun no identificadas.
Intrusiones	Cuenta con privilegios altos afectada	Accesos que pueden ser generados remotamente, localmente, por *bootnet* o por vulnerabilidades conocidas.
	Cuenta sin privilegios afectada	

Cuadro 2. (Continuación)

Clasificación de ataques o incidentes	Incidente o ataque	Descripción
	Aplicaciones comprometidas	
	Bot	
Disponibilidad	Denegación de servicios (DoS)	La disponibilidad de un Sistema o de la información puede verse afectada por factores como la puesta en marcha de ataques *DoS* que son el envío masivo de peticiones *ICMP*, ataques *DDoS* que deniegan los servicios mediante *bots*, sabotaje por parte de personas que tienen acceso a la infraestructura TI y a los activos de información o por imprevistos como desastres naturales, cortes eléctricos, entre otros.
	Denegación de servicio distribuido (DDoS)	
	Sabotaje	
	Interrupción no intencionada	
Seguridad de la información	Acceso no autorizado a la información	La información puede ver comprometida su seguridad de forma local o remota, por descuidos, explotación de vulnerabilidades, puertos abiertos, *spoofing*, errores humanos y malas configuraciones.
	Modificación o edición no autorizada de la información	
Fraude	Uso no autorizado de recursos	Uso de los recursos organizacionales para fines no autorizados, se puede nombrar el uso de internet para descarga de películas o el uso de correo electrónico corporativo para fines personales
	Suplantación	Un atacante asume la identidad de alguien legitimo para beneficiarse de ello.
	Phishing	Pesca de datos mediante el uso de ingeniería social
Otros	Los ataques que no están en otras clasificaciones se pueden incluir aquí	Revisar continuamente este tipo de clasificación cuando tenga un numero alto de miembros
Fuente: elaboración propia.		

5.3.1 Riesgos y respuesta del CSIRT. Se realiza a continuación una valoración de los riesgos que puede atender el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, lo cual permitirá priorizar la atención y definir el plan mitigación del impacto que se pudiese generar en los incidentes informáticos.

5.3.1.1 Métricas. A continuación, se define las métricas usadas para generar el mapa de riesgo; en la tabla 3 se observa el impacto que puede tener un incidente en la estructura tecnológica y activos de información.

Tabla 3. Métrica para estimación del impacto

Valor	Descripción
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente: Elaboración propia.

El riesgo puede ser estimado como catastrófico, moderado o leve, con ello se define las consecuencias potenciales del incidente informático y las vulnerabilidades que se deben cubrir, ver tabla 4.

Tabla 4. Métrica para estimación del riesgo

Valor	Descripción
Catastrófico (7-9)	El riesgo representa pérdidas importantes que detengan en su totalidad procesos relevantes
Moderado (4-6)	El riesgo puede representar perdidas que generen daños en procesos importantes
Leve (1-3)	El riesgo no representa pérdidas significativas

Fuente: Elaboración propia

De acuerdo con la valoración definida por el CSIRT para la evaluación de un incidente, también se parametriza la métrica y la priorización con la que los incidentes serán atendidos, ver tabla 5.

Tabla 5. Métrica respuesta del CSIRT

Valor	Descripción
Baja	Prioridad de atención de incidente baja
Media	Atención de incidentes posterior a las prioridades altas
Alta	Atención inmediata de incidentes

Fuente: Elaboración propia.

5.3.1.2 Mapa de riesgos y respuesta del CSIRT. A continuación, se presenta la estimación del impacto y de la probabilidad de los incidentes que atenderá el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, con la que se calcula el nivel del riesgo y la capacidad que tiene el CSIRT para dar respuesta y solución al incidente o ataque. Ver cuadro 3

Cuadro 3. Mapa de riesgos y respuesta del CSIRT

Incidente o ataque	Id riesgo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Impacto		Probabilidad		Riesgo		Capacidad de respuesta CSIRT
Spam	R1	B	B	B	B	A	1	B	3	A	3	Leve	Baja
Copyright	R2	A	M	A	M	B	2	M	2	M	4	Moderado	Media
Explotación sexual infantil/Racismo / Incitación a violencia	R3	B	B	A	A	B	2	M	3	A	6	Moderado	Media
Virus	R4	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Worm	R5	A	M	A	A	A	3	A	3	A	9	Catastrófico	Alta
Trojan	R6	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Spyware	R7	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Dialler	R8	M	M	A	M	A	3	A	2	M	6	Moderado	Media

Cuadro 3. (Continuación)

Incidente o ataque	Id riesgo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Impacto		Probabilidad		Riesgo		Capacidad de respuesta CSIRT
Rootkit	R9	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Escaneo	R10	A	A	A	A	A	3	A	2	M	6	Moderado	Media
Sniffing	R11	A	M	A	M	A	3	A	3	A	9	Catastrófico	Alta
Ingeniería Social	R12	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Explotación de vulnerabilidades	R13	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Intentos de *login*	R14	M	M	M	M	M	2	M	3	A	6	Moderado	Media
Nuevos ataques	R15	B	B	B	B	B	1	B	2	M	2	Leve	Baja
Cuenta con privilegios altos afectada	R16	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Cuenta sin privilegios afectada	R17	M	M	M	M	M	2	M	3	A	6	Moderado	Media
Aplicaciones comprometidas	R18	M	M	A	A	M	2	M	3	A	6	Moderado	Media
Bot	R19	M	M	M	B	M	2	M	3	A	6	Moderado	Media
Denegación de servicios (DoS)	R20	M	M	M	M	A	3	A	3	A	9	Catastrófico	Alta
Denegación de servicio distribuido (DDoS)	R21	M	M	M	M	B	3	A	3	A	9	Catastrófico	Alta
Sabotaje	R22	M	M	M	M	M	2	M	2	M	4	Moderado	Media
Interrupción no intencionada	R23	B	A	B	A	A	2	M	2	M	4	Moderado	Media
Acceso no autorizado a la información	R24	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta

Cuadro 3. (Continuación)

Incidente o ataque	Id riesgo	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Impacto		Probabilidad		Riesgo		Capacidad de respuesta CSIRT
Modificación o edición no autorizada de la información	R25	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Uso no autorizado de recursos	R26	B	M	B	A	A	2	M	3	A	6	Moderado	Media
Suplantación	R27	A	A	A	A	A	3	A	3	A	9	Catastrófico	Alta
Phishing	R28	A	M	A	A	A	3	A	3	A	9	Catastrófico	Alta
Fuente: Elaboración propia.													

5.3.1.3 Formato de registro de incidentes. A continuación, se presenta un formato de registro de incidentes para ser diligenciado cuando estos se presenten en las organizaciones, este alimentará una base de datos del CSIRT para con ello estar preparado para casos que se presenten de la misma índole teniendo la respuesta o salvaguarda aplicada. Ver cuadro 4.

Cuadro 4. Formato de registro de incidentes informáticos

Registro de incidentes								
Organización	Tipo de incidente	Fecha de incidente	Hora de reporte	Salvaguardas	Fecha de solución	Hora de solución	Responsable	Observaciones
Fuente: Elaboración propia								

6. FASE 2: ESTRUCTURACÍON DE LOS SERVICIOS DEL CSIRT

Los servicios que prestara el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA se dividen en tres tipos, los cuales son los servicios reactivos, los proactivos y los que generan un valor agregado los cuales se definen y desglosan a continuación con el objetivo de generar el portafolio de servicios del CSIRT.

6.1 SERVICIOS REACTIVOS

Los servicios reactivos también se definen como de reacción, cuando un incidente ya se ha presentado, el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA presenta una serie de tareas y protocolos enfocados a mitigar los efectos adversos que se puedan producir a partir del incidente y poner a disposición en el menor tiempo posible los activos de información y la infraestructura TI a servicio del cliente nuevamente.

6.1.1 Gestión de Vulnerabilidades. Este es un proceso continuo en el que se debe tener en cuenta los aspectos numerados a continuación.

6.1.1.1 Identificación de vulnerabilidades. El personal experto del CSIRT de la empresa caso de estudio Cibersecurity de Colombia, identificara fallas mediante documentación y estadísticas que arroje el análisis, las pruebas de penetración y *testing* que permitan evidenciar las fallas de seguridad y vulnerabilidades que pueden tener los portales web, sistemas operativos o sistemas de información.

6.1.1.2 Pruebas de calidad de software. Este tipo de pruebas permite realizar una verificación a través de listas de chequeo y aplicación de metodologías de buenas prácticas sobre los sistemas de información con la finalidad de que estén libres de fallas que denoten agujeros o portales en la seguridad de la información que podrían ser usados por los atacantes, para ello se genera un plan para la corrección o para el reporte al proveedor del software.

6.1.1.3 Reportes y recomendaciones. El paso siguiente después de realizar la identificación y evaluación de las vulnerabilidades, amenazas y riesgos es continuar con un análisis que facilite la detección de falsos incidentes y a la vez la generación de recomendaciones para la correcta configuración tanto de software como políticas sobre los activos de información que permitan hacerle frente a los

factores que representan un riesgo

6.1.2 Gestión de códigos maliciosos. Teniendo en cuenta el código malicioso como un script que permite la vulneración de los sistemas informáticos, el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, tendrá la capacidad de gestionar este tipo de amenazas a partir de los siguientes servicios prestados.

6.1.2.1 Análisis de código malicioso. En la prestación de este servicio se realizan estudios que permitan identificar fallos para posteriormente buscar la raíz del problema haciendo el bloqueo de códigos, herramientas, archivos o programas que pueden representar una amenaza por ser usados para transgredir y afectar los sistemas de información y la infraestructura TI de las organizaciones.

6.1.2.2 Soporte a usuarios. Todo requerimiento que surja por petición de los clientes del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA será atendido por el personal experto e idóneo con la aplicación de estrictas normas y manuales de procedimiento y de buenas prácticas lo que garantizara la eficacia y la eficiencia en los procesos de las organizaciones contratantes.

6.1.3 Gestión y tratamiento de Incidentes de Seguridad de la Información. Un sistema nunca está completamente seguro y en cualquier momento se presentar un incidente por lo que el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA garantizara a sus clientes los siguientes aspectos.

6.1.3.1 Identificación de incidentes. Para llevar a cabo la identificación de incidentes se genera un proceso de reconocimiento de los daños causados y el impacto que generó un incidente de seguridad sobre los activos de información y sobre la infraestructura TI, con lo que se hace posible determinar recomendaciones para su tratamiento de forma tal que se supere el impase en el menor tiempo posible.

6.1.3.2 Tratamiento de incidentes. Se realiza una documentación de los incidentes presentados a fin de generar estrategias que permitan dar respuesta inmediata, utilizando metodologías adecuadas a fin de tener una idea de lo sucedido y generar bases de conocimiento utilizables en otros procesos del propio CSIRT o de la red de apoyo.

6.1.3.3 Soporte a la respuesta a incidentes. Con la red de apoyo con otros CSIRT tanto como en Colombia como en el mundo se puede generar un soporte de alta calidad basado en la experiencia y en la documentación que servirá a otros organismos de respuesta a incidentes que permitirá la recuperación de ataques e incidentes informáticos ya presentados y resueltos por alguno de los miembros de dicha red de apoyo.

6.1.3.4 Reporte de incidentes. A partir del análisis del incidente identificado se determina si este viola los códigos de conducta y las leyes que cubren la ciberseguridad en Colombia con lo que se procederá a informar a las autoridades competentes acerca de los actos delictivos con las respectivas evidencias que sustenten el caso para iniciar procesos judiciales en contra de los actores.

6.1.3.5 Levantamiento de estadísticas. Con los casos atendidos constantemente se actualiza las bases de datos que generan las estadísticas de incidentes por organización, por tipo de organización, por tipo de incidente y por región con lo que se generan informes que alimentan estadísticas nacionales y de los grupos de CSIRT a los que la empresa caso de estudio pertenece.

6.1.3.6 Alertas de acción. Las alertas de acción permiten que el momento cuando un incidente que atenta contra la seguridad de la información de una organización está en curso, los administradores TI de dicha organización recibirán correos o mensajes en los que se detalla todo el proceso que se lleva a cabo para solucionar el problema en tiempo real.

6.2 SERVICIOS PROACTIVOS

Los servicios proactivos permiten que el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA se adelante a los sucesos que pudiesen ocurrir sobre la infraestructura TI y los activos de información de las empresas u organizaciones contratantes, esto con metodologías y herramientas que identifiquen posibles riesgos y el control que se debe aplicar para evitar que se presente.

6.2.1 Sistema de alertas tempranas. El sistema de alertas tempranas SAT del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, permite que los administradores TI de las organizaciones que en algún momento han contratado los servicios, reciban notificaciones acerca de vulnerabilidades, ataques, herramientas y virus, con lo que se mantiene una base de conocimiento actualizada.

6.2.2 Monitoreo de portales web. Con el uso de herramientas especializadas el monitoreo de portales web de los clientes, permite identificar los ataques e incidentes sobre las páginas web en tiempo real, haciendo un envío masivo de mensajes de alerta tanto a los administradores de los portales como a los expertos del equipo de respuesta con lo cual generara un control a fin de evitar los riesgos antes de que se puedan presentar.

6.2.3 Boletines de seguridad informática.
El equipo de respuesta a incidentes genera boletines de seguridad informática los cuales contienen información de gran utilidad que permite a los administradores TI de las organizaciones contratantes realizar planes de ajuste y control que logren mejorar la seguridad de la infraestructura tecnológica y los activos de información de las empresas.

6.2.4 Desarrollo de herramientas. El CSIRT de la empresa caso de estudio Cibersecurity de Colombia, está en la capacidad de generar desarrollo de herramientas, aplicación de métodos y de buenas prácticas que permitan la identificación y evaluación de riesgos e incidentes con lo que se pasara a la minimización del impacto de estos sobre los activos de información e infraestructura TI.

6.2.5 . Prospectiva tecnológica. El personal experto del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA está en capacidad de brindar asesoría y hacer diseño de una arquitectura tecnológica recomendada que haga posible la implementación de software, hardware y políticas de seguridad encaminadas a garantizar la seguridad de los activos de información y de la infraestructura TI.

6.3 SERVICIOS DE VALOR AGREGADO

6.3.1 Formación. El CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, mediante su personal podrá dar capacitaciones formativas a funcionarios y servidores de las organizaciones contratantes en materia de seguridad informática, manejo de herramientas, diseño e implementación de políticas de seguridad y prevención de riesgos, con lo que se reduciría sustancialmente los incidentes informáticos.

6.3.2 Concientización. Dentro de las organizaciones contratantes se hacen campañas de difusión y boletines acerca de buenas prácticas que deben tener los funcionarios y servidores de las empresas como el eslabón más débil dentro de la

cadena de posibles focos de ataque, con lo que se podrá mejorar la seguridad informática a partir de pautas y buenos manejos de los usuarios.

6.3.3 Asesoría legal. Las empresas contratantes y cualquier persona pueden solicitar el acompañamiento en materia de seguridad de la información en el aspecto legal, el equipo de expertos hará un trabajo exhaustivo para asistir ante las autoridades competentes con las evidencias y material probatorio necesario a fin de emprender acciones legales eficientes y de gran solvencia.

6.3.4 Gestión de riesgos. Se identifican, analizan, evalúan y valoran los riesgos con el fin de mitigar su impacto generando sistemas de gestión de la seguridad informática basados en metodologías, normas y estándares de buenas prácticas que garanticen a profundidad que un riesgo sea controlado de la mejor manera y con el menor daño posible sobre los activos de las organizaciones.

6.3.5 Consultoría. Se ofrece asesoría profesional en todo el campo de la seguridad informática enfocada en organizaciones, este campo cubre auditorias, *pentesting*, explotación de vulnerabilidades para próximas correcciones, todo con el fin de mejorar el desempeño de procesos de las organizaciones que permitan tener un mejor flujo de la información.

6.3.6 Coordinar la recuperación de desastres. En el mundo de la seguridad informática hay eventos que se pueden evitar, pero también hay muchos otros de los que no se sabe que sucederán, por lo que el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA cuenta con personal que puede actuar de forma eficaz ante desastres y con ello restablecer los procesos de infraestructuras críticas en tiempos pertinentes y con el menor impacto posible.

7. FASE 3: ORGANIZACIÓN DEL CSIRT

7.1 PERFIL DEL EQUIPO A CONFORMAR EL CSIRT

Ocasionalmente una persona puede ejecutar labores de varios perfiles dentro del equipo, pero es recomendable que cada cargo tenga sus roles definidos, de acuerdo con el manual de buenas prácticas de la OEA[43] para implementación de un CSIRT los perfiles que se deben tener en cuenta se enumeran a continuación.

7.1.1 Dirección general. La dirección general es la dependencia de más alto nivel dentro de la organización; para el caso del CSIRT de la empresa caso de estudio Cibersecurity LTDA, su objetivo principal es el trazado de metas y estrategias que permitan cumplir los objetivos de la entidad, dentro de esta dependencia se tiene el cargo de director, definido en el cuadro 5.

Cuadro 5. Perfil director

Cargo	Director	**Vacantes**	1
Descripción del cargo	Sera el responsable de dirigir a nivel ejecutivo la orientación estratégica del equipo, generará cooperación con otras organizaciones y será el enlace general ante otros CSIRT.		
Funciones y responsabilidades			
• Sera la persona con más jerarquía dentro de la organización, tiene la mayor responsabilidad ya que sobre el recae la toma de decisiones que podrá llevar al éxito o fracaso del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA. • Definir los requerimientos del CSIRT y de los proyectos que este emprenda a partir de una planificación inicial en la cual precise el alcance, las estrategias, métodos, objetivos y herramientas para la prestación del servicio. • Fijación de objetivos y trazado de estrategias técnicas y metodológicas para alcanzarlos. • Liderar los procesos que permitan el desempeño optimo del personal para el cumplimiento óptimo de los objetivos del CSIRT • Velar por el cumplimiento de las actividades de la organización estando así al tanto de cada funcionario y las tareas que desempeña. • Detectar riesgos para la organización e implementar planes de mejora y subsanación de errores y/o vulnerabilidades en cualquier eje de la organización.			

[43] ORGANIZACION DE LOS ESTADOS AMERICANOS. Op. Cit., p. 48.

Cuadro 5. (Continuación)

Funciones y responsabilidades
• Articulación interinstitucional con otros CSIRT y organizaciones de las cuales dependa la prestación del servicio. • Proyección y ejecución de destino para los recursos financieros de la entidad organización. • Enlace con las compañías a quienes se prestará el servicio y con los medios de comunicación, figurando como el líder de la compañía. • Sera el portavoz dentro de la empresa caso de estudio Cibersecurity de Colombia LTDA.
Requisitos
• Pregrado en áreas de la TI. • Especialista en seguridad informática. • Postgrado en gerencia de proyectos. • Experiencia de 10 años o superior en seguridad informática. • Experiencia de 3 años o superior en gerencia de proyectos TI. **Adicionales no obligatorios.** • Certificaciones CISSP, CISM, CISA o similar.
Fuente: Elaboración propia.

7.1.2 Auditoria. Esta dependencia jerárquicamente puede evaluar todos los cargos y funciones dentro de la organización, vela por la eficiencia y eficacia de los procesos establecidos dentro de las actividades de cada perfil; en el cuadro 6 se resume el cago de auditor interno que va dentro de esta dependencia.

Cuadro 6. Perfil Auditor interno

Cargo	Auditor interno.	**Vacantes**	1
Descripción del cargo	Evaluar la eficacia de la gestión de los procesos que se presentan dentro de la organización, para establecer políticas de mejora.		
Funciones y responsabilidades			
• Identificación de puntos débiles en procesos que necesariamente se deben mejorar. • Jerarquizar procesos en los que es urgente la instalación de políticas de mejora. • Generar e implementar políticas que velen por la generación de procesos limpios. • Evaluación de las políticas implantadas para corrección de errores o generación de otras políticas adicionales.			

Cuadro 6. (Continuación)

Funciones y responsabilidades
• Conocimiento aplicación y mejora de procesos bajo la norma ISO 27001
Requisitos
• Pregrado en las áreas TI, contabilidad o administración de empresas. • Certificaciones *Certified Information Systems* Auditor, o CISA. • Experiencia mínima de 3 años como auditor TI o auditor líder ISO 27001.
Fuente: Elaboración propia.

7.1.3 Dependencia Jurídica. En esta dependencia se efectúan todos los trámites legales del CSIRT, a continuación, en el cuadro 7 se define el cargo de asesor jurídico.

Cuadro 7. Perfil Asesor Jurídico

Cargo	Asesor jurídico	**Vacantes**	1
Descripción del cargo	Asesorar a la organización y a las entidades contratantes del CSIRT en temas jurídicos y penales ante las autoridades correspondientes.		
Funciones y responsabilidades			
• Acompañamiento en temas legales para el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA. • Acompañamiento y asesoría legal en temas jurídicos a clientes que así lo requieran antes las entidades correspondientes.			
Requisitos			
Obligatorio • Profesional en Derecho. • Especialista en derecho de las tecnologías de la información. • 3 años de experiencia en asesoría jurídica de las TI.			
Fuente: elaboración propia			

7.1.4 Secretaria General. Esta dependencia es creada para el manejo de las labores administrativas del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, dentro de ella se encuentra los subgrupos finanzas, recursos humanos y administración los cuales se describen a continuación.

7.1.4.1 Finanzas. Este grupo de trabajo es el encargado de velar por que los recursos e inventarios de la organización se encuentren al día de acuerdo con sus

criterios contables, en cuadros 8 y 9 se describen los cargos creados para dar cumplimiento a estas labores dentro del CSIRT de la empresa caso de estudio Cibersecurity de Colombia Ltda.

Cuadro 8. Perfil contador público

Cargo	Contador público.	**Vacantes**	1
Descripción del cargo	Dirigir las actividades contables, presupuestales y financieras de la organización.		
Funciones y responsabilidades			
• Colaborar con la dirección para ejecutar los objetivos y propósitos de la empresa. • Diseñar e implementar mecanismos para la evaluación de gestión financiera en la organización. • Implantar y administrar sistemas de información contable y financiera. • Diseñar, analizar, documentar y exponer informes de gestión del área contable y financiera de la organización. • Comunicación y representación ante entes de control financiero de la nación. • Realizar tareas asignadas por la dirección.			
Requisitos			
• Formación profesional en contaduría pública. • Experiencia 1 año en organizaciones con manejo de TI.			
Fuente: elaboración propia			

Cuadro 9. Perfil auxiliar contable

Cargo	Auxiliar contable	**Vacantes**	1
Descripción del cargo	Soporte al contador público, debe manejar la fase presupuestal a partir de ingresos y de egresos de la organización.		
Funciones y responsabilidades			
• Registro y documentación de los libros contables de la empresa. • Gestión de soportes de egresos de la organización. • Arqueo de cuentas. • Elaboración de informes presupuestales. • Liquidación de nómina.			
Requisitos			
• Técnico o tecnólogo en contabilidad y finanzas. • 1 año de experiencia laboral. • Manejo de software contable.			
Fuente: elaboración propia.			

7.1.4.2 Recursos Humanos. El área de recursos humanos se encarga de comunicaciones internas, trámites administrativos y todo lo concerniente al personal del CSIRT, para este caso se designa un cargo de Líder de recursos humanos como se muestra en el cuadro 10.

Cuadro 10. Perfil líder de recursos humanos

Cargo	Líder de recursos humanos	**Vacantes**	1
Descripción del cargo	Gestión de todo lo pertinente al personal que labora en la empresa.		
Funciones y responsabilidades			
• Redactar las ofertas de empleo a petición de la dirección general. • Buscar candidatos idóneos. • Reclutamiento del personal idóneo a cada cargo. • Control de horario y turnos de los empleados. • Gestión de vacaciones • Manejo de seguridad social y salud. • Proponer y desarrollar programación para el bienestar institucional.			
Requisitos			
• Profesional en administración de Empresas, Ingeniería Industrial y/o carreras afines. • Experiencia profesional de 2 años en manejo de personal, selección, reclutamiento, contratación, inducción, reinducción, desarrollo de planes y manejo de descargos.			
Fuente: elaboración propia.			

7.1.4.3 Secretaria administrativa. Sera quien haga el puente entre los clientes y el personal operativo o administrativo del CSIRT, en el cuadro 11 se define este perfil.

Cuadro 11. Perfil secretaria administrativa

Cargo	Secretaria	**Vacantes**	1
Descripción del cargo	Asistir funciones y peticiones de la dirección general.		
Funciones y responsabilidades			
• Recepción y gestión documental. • Atención al público vía telefónica y presencial. • Manejo de agenda de la organización.			
Requisitos			
Técnica o tecnóloga en secretariado, experiencia en atención al cliente, manejo de herramientas informáticas.			
Fuente: elaboración propia.			

7.1.5 Dirección de operaciones. Esta dependencia va encaminada a la coordinación, la investigación y la ejecución de acciones que generen el mayor valor agregado a los servicios prestados por el CSIRT mediante la planificación, organización, dirección y control para la gestión de incidentes presentados en los activos de información de los clientes; para ello se genera el cargo de director de operaciones el cual se describe en el cuadro 12.

Cuadro 12. Perfil director de operaciones

Cargo	Director de operaciones	**Vacantes**	1
Descripción del cargo	Coordinar la gestión de incidentes y el grupo de apoyo con el fin de cumplir los objetivos de la empresa con sus clientes.		
Funciones y responsabilidades			
• Coordinar las actividades y funciones del grupo de gestión de incidentes. • Asignación de personal idóneo a un incidente. • Monitoreo de incidentes y auditoria del manejo de incidentes. • Coordinar el grupo de apoyo. • Toma de decisiones frente a un incidente respecto a su documentación. • Revisión autorización e implementación de sistemas de gestión de riesgos informáticos.			
Requisitos			
• Título universitario en áreas de TI • Especialista en seguridad informática • Experiencia 5 años en proyectos encaminados a la seguridad de la información o manejo de incidentes informáticos • Experiencia en coordinación de personal.			
Fuente: elaboración propia.			

7.1.5.1 Gestión de incidentes. En este grupo de trabajo se opera sobre los incidentes informáticos que presentan los clientes del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, el objetivo principal de es reestablecer el funcionamiento normal de la infraestructura tecnológica y minimizar los impactos negativos que se hayan generado. Para ello se crean los cargos de analista de incidentes cuyo perfil se observa en el cuadro 13 y el perfil de especialista en manejo de incidentes que se puede observar en el cuadro 14.

Cuadro 13. Perfil analista de incidentes

Cargo	Analista de incidentes	**Vacantes**	1
Descripción del cargo	Analizar todos los incidentes que presenten los clientes al CSIRT y hacer la clasificación de acuerdo con la taxonomía de ataques, distribuyendo las tareas dependiendo el nivel de impacto, conocimiento y aplicación de los especialistas en manejo de incidentes.		
Funciones y responsabilidades			
• Análisis de sistemas y redes en que se presenten los incidentes, para a partir de ello designar el especialista que se hará cargo del incidente. • Si un incidente es de bajo grado y el analista tiene la capacidad de resolverlo, es su deber hacerlo e informar para la respectiva documentación y publicación. • Clasificación de incidentes de acuerdo con la taxonomía de ataques. • Priorización de incidentes. • Demás funciones que la dirección de operaciones asigne. • Comunicación continua con el personal de monitoreo para estar al tanto de posibles nuevos casos de incidentes en las infraestructuras manejadas.			
Requisitos			
• Técnico, tecnólogo o profesional en las áreas TI • Experiencia 2 años en mesa de ayuda, soporte o atención a incidentes TI. • Especialista en seguridad informática.			
Fuente: elaboración propia.			

Cuadro 14. Perfil especialista en manejo de incidentes

Cargo	Especialista en manejo de incidentes	**Vacantes**	3
Descripción del cargo	Resolver incidentes informáticos asignados a su cargo.		
Funciones y responsabilidades			
• Resolución de incidentes informáticos en el menor tiempo posible. • Análisis de comportamientos de la infraestructura TI de los incidentes asignados.			

Cuadro 14. (Continuación)

Funciones y responsabilidades
• Análisis y evaluación de logs. • Definir causas de incidentes. • Manejo de matrices para fácil detección de incidentes similares. • Manejo de bitácoras y formatos que permitan tener control en el avance de resolución de incidentes. • Entrega de formatos a personal de documentación para que se realice la publicación e informe del incidente presentado. • Análisis forense del caso • Coordinación con personal de apoyo en caso de ser necesario manejo de hardware.
Requisitos
• Profesional en áreas de TI. • Especialista en seguridad informática. • Estudios o experiencia en informática forense. • Conocimiento en infraestructura y redes. • 5 años en manejo de incidencias informáticas • Conocimiento en Hacking ético.
Fuente: Elaboración propia.

7.1.5.2 Apoyo. El personal de este grupo de trabajo se encarga de labores documentales y labores sobre el hardware encargadas por el equipo de gestión de incidentes; para ello se definen los siguientes perfiles.

- Técnico sistemas. Sera la persona encargada de las labores técnicas tanto sobre el *hardware* como sobre el *software* de la infraestructura tecnológica de los clientes del CSIRT, estará a disposición del personal de gestión de incidentes. Ver cuadro 15.

Cuadro 15. Perfil técnico en sistemas

Cargo	Técnico en sistemas	**Vacantes**	2
Descripción del cargo	Persona encargada de hacer mantenimientos preventivos y correctivos sobre infraestructura tecnológica que este en riesgo o haya presentado incidentes informáticos.		
Funciones y responsabilidades			
• Estar a disposición del grupo de gestión de incidentes para resolver cualquier requerimiento presentado y que necesite su intervención sobre la infraestructura tecnológica del cliente. • Coordinar con el personal de sistemas de los clientes la mejor ruta para reestablecer la infraestructura tecnológica en el menor tiempo posible. • Realizar instalaciones o reinstalaciones de sistemas operativos. • Realizar revisiones sobre redes. • Instalar o reinstalar software • Mantenimientos preventivos o correctivos sobre hardware.			
Requisitos			
• Tecnólogo en áreas TI. • Experiencia en soporte técnico. • Experiencia en documentación de procesos. • Manejo de herramientas informáticas. • Manejo de hardware. • Conocimiento en electrónica básica. • Conocimiento en redes, modelo OSI y protocolo TCP/IP.			
Fuente: elaboración propia			

- Perfil de documentación y redacción, se relaciona a continuación en el cuadro 16.

Cuadro 16. Perfil documentador

Cargo	Documentador	**Vacantes**	1
Descripción del cargo	Recepción de bitácoras, formatos de registro de incidentes e informes por parte del personal de gestión de incidentes para realizar la documentación pertinente.		
Funciones y responsabilidades			
• Recepción de bitácoras, registro de incidentes e informes. • Documentar detalladamente el incidente presentado y la forma en que se solucionó. • Publicación del incidente en el medio que se dispone por parte del CSIRT y realizar envío a la red interinstitucional de CSIRT a la que CIBERSECURITY de Colombia pertenece. • Presentar la documentación al departamento de comunicaciones para que se realice el informe en palabras no técnicas al cliente.			
Requisitos			
• Tecnólogo en áreas TI. • Experiencia en soporte técnico. • Experiencia en documentación de procesos. • Manejo de herramientas informáticas.			
Fuente: elaboración propia			

- Investigación y desarrollo ver cuadro 17.

Cuadro 17. Perfil apoyo I & D

Cargo	Apoyo I & D	**Vacantes**	2
Descripción del cargo	Generar documentación, manuales, software y demás que permitan tanto a la organización como a sus clientes maximizar la seguridad de la infraestructura TI.		
Funciones y responsabilidades			
• Análisis de registros, estadísticas y estudios que muestren puntos clave donde generar conciencia en clientes. • Generar manuales y documentación que permita evitar incidentes informáticos para envío constante a clientes. • Planteamiento y desarrollo de software para la organización y para quien contrate los servicios que permitan incrementar la seguridad de la información. • Dictar cursos, talleres y charlas técnicas a clientes que lo soliciten.			

Cuadro 17. (Continuación)

Requisitos
• Título universitario en TI. • Conocimiento de desarrollo de sistemas en 2 lenguajes de programación. • Experiencia en desarrollo y posicionamiento de software • Experiencia en documentación de manuales y exposición pública.
Fuente: Elaboración propia.

- Gestión de riesgos, ver cuadro 18.

Cuadro 18. Analista SGSI

Cargo	Analista SGSI	**Vacantes**	2
Descripción del cargo	Desarrollar Sistemas de gestión de la seguridad de la información para clientes que así lo soliciten.		
Funciones y responsabilidades			
• Realizar inventario de activos de información en la infraestructura TI del cliente. • Análisis de amenazas y vulnerabilidades sobre la infraestructura TI del cliente. • Valorar riesgos encontrados y definición de metodologías. • Gestión y tratamiento de los riesgos a partir de la búsqueda e implementación de controles. • Implementación de SGSI. • Evaluación del SGSI. • Guiar al cliente para la certificación bajo la norma 27001.			
Requisitos			
• Formación profesional en áreas TI. • Especialista en seguridad informática. • Contar con por lo menos una certificación CISSP, CEH, CPTE, CISM, CCNA o CCNP. • Experiencia de más de 1 año en implementación de SGSI bajo la norma ISO 27001.			
Fuente: elaboración propia			

7.1.6 Dirección estratégica. Esta es la encargada de atraer clientes nuevos y conservar los actuales con el uso de herramientas y técnicas que permitan explotar al máximo el marketing y la visual externa de la empresa. Ver cuadro 19 en el que

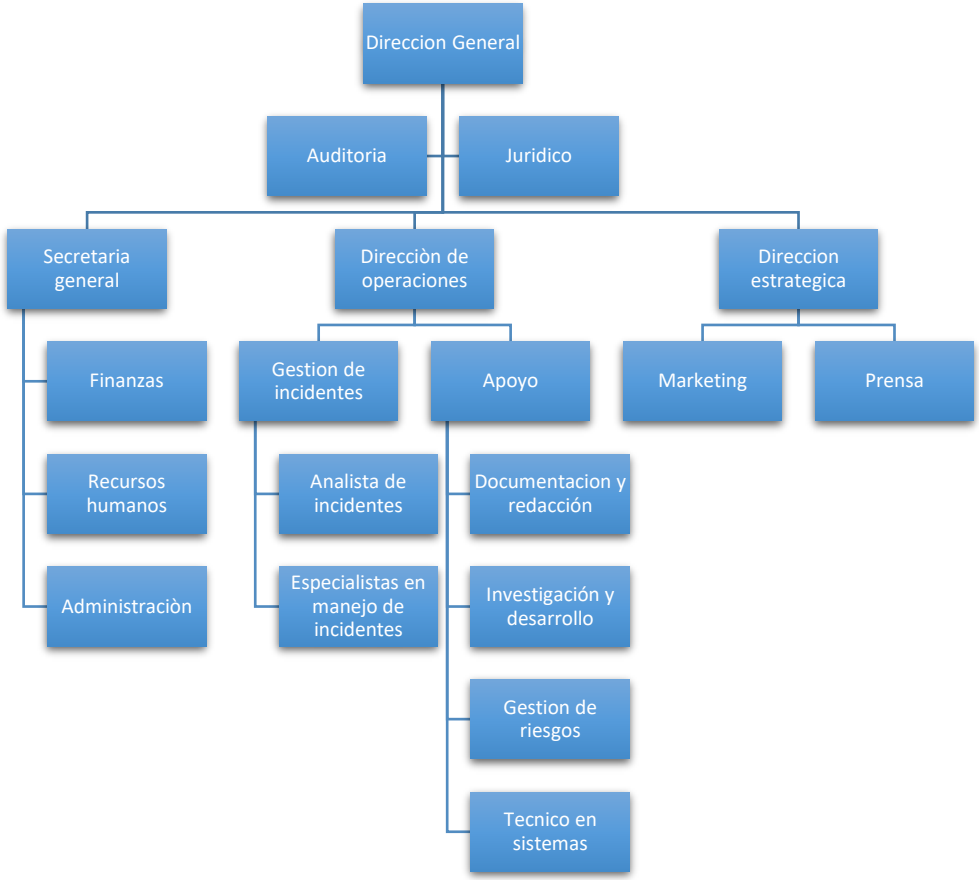
se detalla el perfil de marketing y prensa para esta dirección.

Cuadro 19. Perfil marketing y prensa

Cargo	Marketing y prensa	**Vacantes**	1
Descripción del cargo	Será quien ofrezca los servicios del CSIRT por medio de diferentes canales además de encargarse del manejo de comunicados de prensa		
Funciones y responsabilidades			
• Gestionar la relación con clientes bajo una plataforma CRM que permita administrar la información, generar el contacto de los clientes y potenciales clientes de manera efectiva con el CSIRT e integrar procesos de marketing y ventas. • Ofrecer servicios del CSIRT por diferentes canales. • Procurar el crecimiento económico a través del incremento de clientes del CSIRT. • Generar comunicados de prensa a través de los canales para ello dispuestos y a petición de la dirección del CSIRT. • Entablar comunicación con el cliente explicándole de manera no técnica la resolución del incidente.			
Requisitos			
• Licenciatura, grado en periodismo o titulaciones afines. • Tecnólogo en áreas TI. • Experiencia en redacción de contenidos de 1 año. • Experiencia en relaciones públicas.			
Fuente: elaboración propia.			

7.2 ESTRUCTURA ORGANICA DEL CSIRT

Figura 3. Organigrama CSIRT CIBERSECURITY Ltda.



Fuente: Elaboración propia

8. FASE 4: POLITICAS OPERACIONALES DEL CSIRT

8.1 POLÍTICA DE CLASIFICACIÓN DE INFORMACIÓN

Esta política está basada en el documento que propone INCIBE[44] y define la clasificación que hará el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA para la información, teniendo como base fundamental que este es el activo más importante para proteger tanto para clientes como para la información de la misma organización. Se define la parametrización del alcance de esta política el compilado de todos los datos e información disponible en cualquier medio posible ya sea físico o digital y que pase por un proceso concerniente a las funciones dentro de la organización o repose en el archivo histórico del CSIRT.

El objetivo de esta política es definir el tipo de información que se manejara entorno al CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, que permitan garantizar mediante su clasificación los criterios de confidencialidad, integridad y disponibilidad como ejes fundamentales de la seguridad de los activos de información manejados por el CSIR

La información es el activo más importante que se debe proteger dentro de la seguridad informática por ello es de obligatorio cumplimiento gestionar inventarios de todos los activos de información de la organización, tanto de los que actualmente se tienen inventario como los que se hace recepción a diario en la generación de documentación del soporte de incidentes del CSIRT. Por lo anterior se debe tener en cuenta las siguientes especificaciones.

8.1.1 Criterios de clasificación. Se debe clasificar claramente la información inventariada según los criterios de seguridad que se definen por la organización como confidencial, interna o publica los cuales se definen y analizan en la tabla 6 y tabla 7, estos criterios van ligados estrechamente a las políticas de seguridad que se plantea para la información.

[44] INCIBE. Clasificación de la información – Políticas de seguridad para la Pyme. [ONLINE]. Madrid: Instituto nacional de ciberseguridad. [Citada: 02 abril 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

Tabla 6. Clasificación de la información según su confidencialidad

Clasificación	Descripción
Confidencial	Solo el personal autorizado por la dirección tendrá acceso a este tipo de información.
Interna	Solo tendrá acceso a este tipo de información el personal perteneciente al CSIRT
Publica	Información que se emite de manera pública y podrá ser visualizada por entes externos al CSIRT.

Fuente: elaboración propia

Tabla 7. Clasificación de la información por funcionalidad

Clasificación	Descripción
Cliente – Proveedor	Información que tiene envuelve datos básicos de clientes y de proveedores del CSIRT.
Contable	Información acerca de ingresos y egresos de la organización.
Recursos Humanos	Información acerca del personal que dispone el CSIRT

Fuente: elaboración propia

8.1.2 Etiquetado de información. Se realizará un etiquetado a la información de acuerdo con el tipo de información adoptada por el CSIRT; los criterios que se establecen para el etiquetado se realizaran teniendo en cuenta la tabla de clasificación de la información según su confidencialidad, siendo así se rotulará la información o activos de información como confidencial, interna o pública en cintillas o papel legible.

8.1.3 Tratamiento de seguridad. La organización debe realizar tratamientos de seguridad a la información disponible; entre los procesos de este paso se puede destacar los accesos limitados a la información, el cifrado o encriptado de la información relevante o confidencial, la generación periódica de *Backups* y el establecimiento de acuerdos de confidencialidad con el personal de la organización.

8.1.4 Auditoria de procesos. La organización debe realizar por medio del personal experto y bajo la supervisión de personal de auditoría interna procesos periódicos de evaluación acerca de la clasificación y tratamiento de la información, lo que permitirá detectar errores y corregirlos a tiempo con lo que se asegura, compila y

mantiene la información disponible en el CSIRT.

8.2 PROTECCIÓN DE DATOS

El diseño e implementación de esta política de seguridad pretende dar unos lineamientos claros que deben tenerse en cuenta para la protección de los datos que se manejan dentro del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA teniendo en cuenta el manejo de la ley 1781 de 2012 y los lineamientos de seguridad que brinda la ANT[45].; el objetivo principal de esta proceso es implementar políticas que permitan proteger los datos que se manejan dentro del CSIRT aplicando medidas de seguridad sobre todas las bases de datos con las que cuente la empresa en cualquier medio de almacenamiento disponible y de transporte, lo que permitirá garantizar la confidencialidad y la seguridad de los mismos. Por lo anteriormente mencionado se debe tener en cuenta los siguientes criterios.

8.2.1 Identificación del responsable del manejo de los datos. La organización responsable del manejo de los datos es el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA con sede en la ciudad de Bogotá Colombia y que presta sus servicios especializados en manejo de incidentes de seguridad informática a compañías y organizaciones nacionales que así lo requieran.

8.2.2 Compromisos. El CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA como una organización transparente y que vela por la ética profesional de sus empleados y de las personas que hagan manejo de datos sensibles tanto de sus clientes como propia se compromete a cumplir los siguientes parámetros:

- Usar los datos de sus proveedores, clientes y personal solo para fines misionales, es decir para labores de la empresa (compras, ventas, contactos, etc.) si se hace necesario se debe rectificar, actualizar o suprimir total o parcialmente los datos a petición de su propietario.

- Informar acerca del uso y tratamiento de datos personales y solicitar la autorización correspondiente a su propietario, de no obtener dicha autorización queda totalmente prohíbo el uso o manejo de dicha información para todo fin.

[45] AGENCIA NACIONAL DE TIERRAS, COLOMBIA. Lineamientos de seguridad de la información, tratamiento y protección de datos personales. [ONLINE]. Bogotá: ANT, 2017. [Citada: 02 abril 2020]. Disponible en http://www.agenciadetierras.gov.co/wp-content/uploads/2018/04/INTI-Politica-008-lineamientos-de-seguridad-de-la-informacion-tratamiento-y-proteccion-de-datos-personales.pdf

- Dar acceso a los datos tratados en el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, a su propietario con el fin de realizar validaciones o correcciones si el mismo así lo requiere previa solicitud escrita y aprobada por la gerencia.

8.2.3 Datos de menores de edad. Se hará respetar los derechos fundamentales de los menores de edad y solo bajo casos especiales se hará tratamiento de datos relacionados con menores de edad siempre en concordancia con la ley y bajo estricto acompañamiento de las autoridades competentes, además de sus representantes o tutores según sea el caso.

8.2.4 Datos sensibles. El CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, tendrá un compilado donde se manejarán datos sensibles clasificados como confidenciales de acuerdo con el carácter de los servicios del CSIRT, por lo que se compromete a hacer un tratamiento en concordancia a los servicios prestados, velando siempre por la seguridad de aquellos datos.

8.2.5 Almacenamiento de datos personales. La información personal de clientes, prestadores de servicios, personal, proveedores y demás datos sensibles deben estar almacenados en bases de datos que permitan garantizar la máxima protección y seguridad ante cualquier riesgo de edición, adición, secuestro o eliminación total o parcial de la información, velando por los principios de confidencialidad, integridad y acceso restringido.

8.2.6 Modificación a política de protección de datos. Cualquier modificación que el CSIRT realice sobre la política de protección de datos debe ser informada de manera oportuna y a detalle presentando las razones pertinentes solicitando un acuerdo de aceptación de cambios a quienes estén incluidos dentro de las bases de datos que maneja el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA.

8.2.7 Revelación de la información. Al aceptar las políticas de tratamiento de datos, las personas u organizaciones cuya información reposa en las bases de datos del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, están en acuerdo en que sus datos sean revelados bajo solicitud de entidades judiciales y pueden ser auditadas por entidades de control siempre cuidando el principio de confidencialidad.

8.3 RETENCIÓN DE INFORMACIÓN

En esta política se define el tiempo que el CSIRT de la empresa caso de estudio Cibersecurity de Colombia Ltda. debe conservar la información o registros de información, todo esto regidos bajo la resolución 8934 de 2014[46] donde se establece "las directrices en materia de gestión documental y organización de archivos que deben cumplir los vigilados por la Superintendencia de Industria y Comercio". Por lo anterior se define que el objetivo de esta política es establecer el tiempo y la forma de retención de la información dentro del CSIRT.

El CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA debe implementar dentro de su sistema de gestión de seguridad de la información los siguientes requerimientos[47] que permitirán gestionar una línea de vida de la información y los datos que se tengan en el CSIRT:

- Contratar o alinear este trabajo con personal con estudios superiores en archivística y que tenga conocimientos para diseñar una tabla de retención documental TRD acorde a los requerimientos de la organización teniendo en cuenta la clasificación de la información y la importancia que esta tenga tanto para la empresa como para los contratantes si fuese el caso.

- Agrupar los documentos en series, subseries y unidades documentales, teniendo en cuenta que las tablas de retención documental se deben aplicar a documentos producidos dentro de la organización como a documentación enviada por terceros.

- Dentro de las tablas de retención documental se debe determinar el tipo de soporte del documento (papel, magnético, electrónico), una vez estén elaboradas se las debe hacer públicas y se debe aclarar al personal la fecha en que inician a regir.

8.4 DESTRUCCIÓN DE INFORMACIÓN

Para esta política de seguridad a implementar se debe decir que esta instancia es clave en toda organización, para ello se establecen protocolos que permitan hacer la destrucción de información de forma segura sin que esto afecte la seguridad de

[46] COLOMBIA, SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 8934 de 2014. [ONLINE]. Bogotá: Superintendencia de industria y comercio, 2014. [Citada 28 abril 2020]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?id=4041484

[47] ARCHIVO GENERAL DE LA NACION. COLOMBIA. Tablas de retención y transferencias documentales. [ONLINE]. Bogotá: Archivo general de la nación. [Citada 29 abril 2019]. Disponible en: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/Minimanual_TRD.pdf

la información ni los intereses de la organización; es por ello que se puede inferir que el objetivo de esta política en cuanto al CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA es definir el método a seguir para la destrucción segura de la información con la que cuenta el CSIRT. Teniendo en cuenta lo mencionado se debe implementar los siguientes criterios:

- Se debe realizar un comité de archivos donde se definirá que documentación pasará a ser candidata a destrucción, este proceso recae sobre la persona o dependencia que actualmente tenga la custodia del documento en cuestión.

- Los documentos que se marquen como eliminables dentro de las tablas de retención documental (TRD) deben ser eliminados en un lapso no mayor a 3 días laborales, o según como se haya fijado en las propias tablas de retención documental en que se registró el documento.

- Aunque se puede destruir información, la serie documental siempre permanecerá en las tablas de retención documental, se debe levantar en ese momento un acta en la cual se detalle a fondo el motivo de la eliminación y el tiempo que tuvo de retención.

- Si la información es física y en papel, esta se debe pasar por el cortapapel y los restos de la destrucción se debe contratar una empresa de terceros que haga manejo de residuos sólidos y que garantice la incineración de estos para evitar fuga de información.

- Si la información es lógica se debe magnetizar elevadamente los dispositivos de almacenamiento para garantizar un daño para luego triturar los dispositivos de almacenamiento, para ello se debe contratar una empresa que garantice este proceso de forma segura.

8.5 DIVULGACIÓN DE INFORMACIÓN

Aquí se detalla el cómo y el cuándo se compartirá o distribuirá la información interna o externamente, para lo cual se define como objetivo de esta política especificar una metodología que permita establecer el momento en que el CSIRT comparta o distribuya información. Por ello es de importancia las siguientes políticas:

- El CSIRT de la empresa caso de estudio Cibersecurity de Colombia debe realizar estudios que promuevan la seguridad y confiabilidad sobre cada uno de los candidatos a ser integrante de la entidad, con lo que se busca que estas personas tengan una integridad profesional, moral y ética, con lo que se previene así filtración de información al exterior.

- Los integrantes del CSIRT está en la obligación de reportar y denunciar ante las autoridades pertinentes y ante sus superiores cualquier caso de divulgación de información.

- La ley 1273 del 2009, en el artículo 269F, muestra que la pena para quien divulgue información sin consentimiento de los interesados es de 48 a 96 meses de prisión y una multa de 100 a 1000 SMLV.

- El CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA podrá divulgar información sin relevancia de los casos, con fines netamente académicos, que permitan fortalecer la seguridad de la información de terceros que así lo necesiten.

- La divulgación de información de carácter sensible si se requiere debe ser con previa autorización de las personas o entidades involucradas bajo un acuerdo de confidencialidad y eliminando datos que puedan generar huecos de seguridad.

8.6 ACCESO A LA INFORMACIÓN

Esta política tiene como objetivo principal establecer quién podrá acceder a la información del CSIRT de la empresa caso de estudio Cibersecurity LTDA, en ella se incluyen todas las dependencias del CSIRT además de terceros a quienes se determine brindar acceso a la información por solicitud de la gerencia o de autoridades judiciales. Se deben tener en cuenta las siguientes especificaciones:

- De acuerdo con las funciones de cada perfil y su dependencia se realizará la asignación de un rol con sus respectivos privilegios lo cual permitirá que los funcionarios ingresen única y exclusivamente a la información determinada para sus funciones y su cargo.

- Los cambios de etapas productivas de los empleados pueden involucrar los ceses temporales, parciales o totales de las actividades, lo cual requiere una permanente auditoria para realizar un bloqueo o eliminación del perfil dentro de los sistemas de información del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA.

- Se debe realizar auditorías internas a equipos de la organización, lo que permitirá establecer hora, fechas, tiempo de utilización y aplicativos usados, con lo que se genera más manejo y solvencia a la hora de proteger la información ante ataques internos.

- La información física debe encontrarse en lugares seguros que cuenten con seguridad biométrica o con circuitos cerrados de televisión para que solo personal autorizado tenga acceso a la documentación de acuerdo con su criticidad y su clasificación establecida.

- La información electrónica de gran relevancia debe encontrarse encriptada aplicando algoritmos que en la actualidad sean seguros, tal es el caso del encriptado AES-256, las claves y el software usado para tal fin solo deben conocerlos sus propietarios y el personal autorizado.

- Se debe implementar políticas de claves seguras para el acceso a la infraestructura TI, además del cambio periódico obligatorio de las mismas lo cual previene de ataques conocidos principalmente sobre claves débiles y ataques de ingeniería social sobre usuarios.

- Para el acceso a la información por parte de terceros solo será permitido bajo autorización escrita de la gerencia o bajo pedido previamente justificado de las autoridades competentes con una orden judicial igualmente avalada por la gerencia del CSIRT.

8.7 USO APROPIADO DE LOS SISTEMAS DEL CSIRT

Esta política define como se debe gestionar el uso razonable de los sistemas y recursos que sean usados por el personal de las diferentes dependencias del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, velando siempre por el uso para fines netamente relacionados a la actividad del CSIRT. En concordancia con ello es importante aclarar que:

- La función para la que sea contratado el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA debe estar bajo los parámetros de legalidad regido por las leyes colombianas sin que ello conlleve a acciones ilegitimas al personal de la organización.

- El director de cada dependencia del CSIRT debe velar por el buen actuar de sus dependientes, velando por la legalidad, la ética, la moralidad y el buen vivir para con la sociedad de los empleados para con la sociedad protegiendo siempre el buen nombre del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA.

- Todo sistema de información o aplicativo que sea propiedad explicita de la organización, incluyendo documentos electrónicos o físicos solo deberán usarse para las tareas que el personal sea asignado dentro de sus labores se incluye toda

información cargada en servidores, comunicada y/o emitida en los sistemas de información organizacionales.

- Toda herramienta propiedad de la organización debe ser usada única y exclusivamente para labores del CSIRT, se prohíbe rotundamente el uso para fines personales, además de ello es estrictamente prohibido manejar archivos de índole personal sobre los hosts de la empresa.

- Los programas y aplicativos manejados en la organización deben disponer de una licencia para los casos necesarios, o archivos los que se demuestre que son de uso libre, para su utilización e instalación en los computadores de trabajo, host de uso personal y servidores, además de ello se deben cumplir al máximo la reglamentación que protege el uso de software.

8.8 DEFINICIÓN DE INCIDENTES DE SEGURIDAD Y POLÍTICA DE EVENTOS

Dentro de esta política se describe los criterios que determinan como se define y clasifica un incidente de seguridad o evento dentro del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, esto depende además de otros factores de la jerarquización de cada uno según el tipo y la gravedad.

Se establece dentro de esta política los tipos de incidentes o eventos a manejar por parte del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, se clasificarán de acuerdo con los siguientes parámetros normalizados en el presente proyecto.

- Código malicioso
- Contenido abusivo
- Recopilación de información
- Intentos de intrusión
- Intrusiones
- Disponibilidad
- Seguridad de la información
- Fraude
- Otros

Para una información más detallada del listado anterior se puede observar el cuadro 2 donde se realiza la clasificación o taxonomía de los incidentes; por otra parte, en el cuadro 3 se observa un mapa de riesgos que permite identificar la gravedad si el incidente se llega a presentar.

A continuación, en la tabla 8 muestra es un resumen del mapa de riesgos en el que solo se enfoca el incidente y la gravedad provocada por el mismo.

Tabla 8. Incidente y gravedad

Incidente o ataque	Gravedad
Spam	Leve
Copyright	Moderado
Explotación sexual infantil/Racismo / Incitación a violencia	Moderado
Virus	Catastrófico
Worm	Catastrófico
Trojan	Catastrófico
Spyware	Catastrófico
Dialler	Moderado
Rootkit	Catastrófico
Escaneo	Moderado
Sniffing	Catastrófico
Ingeniería Social	Catastrófico
Explotación de vulnerabilidades	Catastrófico
Intentos de *login*	Moderado
Nuevos ataques	Leve
Cuenta con privilegios altos afectada	Catastrófico
Cuenta sin privilegios afectada	Moderado
Aplicaciones comprometidas	Moderado
Bot	Moderado
Denegación de servicios (DoS)	Catastrófico
Denegación de servicio distribuido (*DDoS*)	Catastrófico
Sabotaje	Moderado
Interrupción no intencionada	Moderado
Acceso no autorizado a la información	Catastrófico
Modificación o edición no autorizada de la información	Catastrófico
Uso no autorizado de recursos	Moderado
Suplantación	Catastrófico
Phishing	Catastrófico

Fuente: Elaboración propia

8.9 GESTIÓN DE INCIDENTES

En esta política corresponde a la capacidad de respuesta a cada incidente y los procedimientos a aplicar, es importante aclarar que el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA no se hace responsable de la prevención de los incidentes, sino que hace parte fundamental del aseguramiento de las plataformas, sistemas de información y activos de información de las empresas.

Según el mapa de riesgos del cuadro 3 es posible resumir la capacidad de respuesta del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, como baja, media y alta, asignada cada una a un incidente o ataque dependiendo de su criticidad, se definen por ello en la tabla 9.

Tabla 9. Capacidad de respuesta del CSIRT

Incidente o ataque	Capacidad de respuesta CSIRT
Spam	Baja
Copyright	Media
Explotación sexual infantil/Racismo / Incitación a violencia	Media
Virus	Alta
Worm	Alta
Trojan	Alta
Spyware	Alta
Dialler	Media
Rootkit	Alta
Escaneo	Media
Sniffing	Alta
Ingeniería Social	Alta
Explotación de vulnerabilidades	Alta
Intentos de *login*	Media
Nuevos ataques	Baja
Cuenta con privilegios altos afectada	Alta
Cuenta sin privilegios afectada	Media
Aplicaciones comprometidas	Media
Bot	Media
Denegación de servicios (DoS)	Alta

Tabla 9. (Continuación)

Incidente o ataque	Capacidad de respuesta CSIRT
Denegación de servicio distribuido (DDoS)	Alta
Sabotaje	Media
Interrupción no intencionada	Media
Acceso no autorizado a la información	Alta
Modificación o edición no autorizada de la información	Alta
Uso no autorizado de recursos	Media
Suplantación	Alta
Phishing	Alta

Fuente: Elaboración propia

La forma de actuar frente a un incidente se puede definir en un paso a paso que el equipo del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA seguirá de manera permanente siempre buscando mitigar o evitar al máximo los riesgos que se pueden ocasionar.

- El equipo de respuesta a incidentes debe analizar los posibles riesgos que se pudieran presentar sobre los activos de información de la organización contratante, si el incidente ya ocurrió se debe generar un análisis e identificación a partir de la recolección de material probatorio y evidencia que permitan verificar el tipo de ataque o incidente presentado.

- Crear bitácoras documentadas de todos los procedimientos que se realicen a lo largo del proceso, con el fin de realizar un expediente a detalle del incidente y si este se vuelve a presentar se seguirán los mismos pasos que ya han funcionado antes, definiendo dentro de ellas las causas, riesgos y culpables del origen del incidente.

- Tomar medidas correctivas en pro de reactivar la infraestructura tecnológica y evitar al máximo los daños, ya que al cliente lo que realmente le importa es que los servicios se normalicen en el menor tiempo posible, por lo que este paso es el más importante de la gestión del incidente.

- Generar observaciones, articular e implantar medidas que permitan que el incidente no se repita dentro de la misma organización, ello se lograra con la generación de políticas de seguridad que deberán ser anexadas al SGSI de la empresa contratante.

- Documentar los procedimientos tomados con dicho incidente para que sirvan en actividades futuras dentro del CSIRT y en su red de apoyo que permitan realizar el Intercambio de conocimientos dentro de la red de apoyo del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA.

8.10 COOPERACIÓN

En esta política se define como se realiza la cooperación entre el CSIRT de la empresa caso de estudio Cibersecurity de Colombia Y otros CSIRT lo que permitirá el intercambio de información y experiencia acerca de incidentes para con ello combatir delitos informáticos a través de la práctica propia y de otros

La cooperación permite que varios grupos de reacción ante incidentes como lo son CSIRT, CERT, áreas TI y grupos de investigación informática, formen una red de apoyo y comunicación que permita el intercambio de experiencias y conocimientos obtenidos a partir de la resolución de incidentes, tanto a nivel organizacional como a nivel global; por ello se crean redes de apoyo y respuesta mucho más amplias y completas, con lo que se logra brindar soluciones eficaces a organizaciones en todo el mundo.

Se debe gestionar la cooperación interinstitucional, con autoridades como la Policía y la Fiscalía, brindando y recibiendo conceptos que aporte al esclarecimiento de investigaciones cibernéticas. (CSIRT Policía – Grupo de Reacción Informática de la Fiscalía); para realizar el intercambio de solución de incidentes se debe pedir autorización exclusiva a la organización involucrada y evitar exponer datos que creen brechas o huecos de seguridad en los sistemas de información.

9. RESULTADOS

Después del desarrollo de los objetivos específicos se tiene como resultado que actualmente Colombia tiene un marco normativo bastante amplio para contrarrestar los delitos informáticos, pero normalmente por desconocimiento de las personas u organizaciones que manejan los incidentes, normalmente los administradores TI o administradores de redes y sistemas informáticos no generan material probatorio de los incidentes presentados por lo que no tienen bases suficientes para hacer una denuncia solida ante las autoridades .

De acuerdo al estudio de factibilidad se tiene como resultado que la mayoría de empresas u organizaciones donde laboran las personas que hicieron colaboración con la encuesta, el 66,7% presentó incidentes informáticos, para los incidentes más presentados entre 21 encuestados se tiene que el 64,3% corresponde a virus y el 49,2 % corresponde a ingeniería social, para la pregunta final acerca de si estaría dispuesto a contratar los servicios de un equipo que maneje los servicios informáticos se tiene como si la respuesta más votada, con el 90,5%; esto lleva a la deducción de que en Colombia hay un gran mercado para un CSIRT, por lo que el ámbito de aplicación para el caso de estudio de CIBERSECURITY de Colombia es CSIRT comercial, ya que es una opción viable para grandes y pequeñas empresas que no tienen los recursos para montar su propio equipo de respuesta o simplemente quieren ahorrar recursos.

Dentro de la taxonomía se hace una priorización para dar respuesta a los incidentes de información teniendo unas métricas que son respuesta alta, media y baja, siendo la métrica alta la atención inmediata y la baja la que se aplica a incidentes que no producen daños catastróficos sobre la infraestructura tecnológica.

Sobre los servicios a prestar por parte del CSIRT se hace referencia a los reactivos, los proactivos y los de valor agregado que suministran a los clientes una forma segura de proteger sus activos de información antes de que se presente un incidente o también la corrección de un incidente ya ocurrido.

Con la correcta formación de un equipo interdisciplinar se logrará conformar un CSIRT que pueda prestar a cabalidad y con prontitud todos los requerimientos realizados por sus clientes; dentro de la organización se deben establecer políticas que permitan el manejo seguro de la información propia como la de sus clientes por lo que se establece que de no ser cumplidas puede haber pérdidas totales, parciales, fugas, eliminación y alteración de datos significativos que podrían incurrir en delitos informáticos y hasta en sanciones judiciales.

10. CONCLUSIONES

- Como base fundamental la alta demanda tecnológica se debe decir que un CSIRT es primordial en las organizaciones ya que con él, es posible mitigar en gran parte el impacto de los riesgos ocasionados por un incidente informático y también evitarlo antes de que se presente, es por ello que este proyecto detalla el contexto donde puede tener aplicabilidad el CSIRT, al igual que evidencia los aportes que ofrece su desarrollo a partir de la necesidad de la creación de la documentación del CSIRT antes de su implementación técnica.

- El primer objetivo específico de este proyecto se representó en el capítulo 5, denominado Fase1: estudios preliminares, de aquí es posible concluir que Colombia tiene un marco normativo que cobija la seguridad de los activos de información y la infraestructura tecnológica, sin embargo estos deben estar en constante actualización ya que como se refleja en el análisis realizado por *FILECODER*, Colombia con el 30% es uno de los países latinoamericanos que más ataques informáticos ha recibido en los últimos años; también se genera un análisis de mercado como parte esencial de un plan comercial, el cual es de suma importancia y que en Colombia actualmente tendría una buena acogida una empresa que maneje CSIRT, con la aplicación de encuestas a profesionales TI se logra definir los ataques más presentados sobre los activos de información con lo cual se define la taxonomía de ataques informáticos que permite realizar un mapa de riesgos en el que se evidencia la gravedad del impacto que generaría la presencia de un ataque de estos siendo clasificado como catastrófico a los cuales el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA debe brindar una atención de respuesta de nivel alto.

- Para el segundo objetivo específico del proyecto se desarrolló en el capítulo 6 definido como estructuración de los servicios del CSIRT, básicamente la prestación del servicio se divide en servicios reactivos, los cuales entran en actuación cuando los incidentes ya se han presentado o están en curso, para ello se gestiona las incidencias con un paso a paso desde su identificación, pasando por la mitigación y generando la alerta de acción para prevenir a los demás CSIRT; por otro lado se encuentran los servicios proactivos, los cuales están llamados a prevenir que los incidentes se presenten y finalmente se encuentran los servicios de valor agregado del CSIRT entre los que se destacan la formación, concientización y consultoría, como conclusión a este punto se resalta que para el funcionamiento eficaz del CSIRT es necesario que como mínimo se presten los servicios proactivos y reactivos, ya que el uno complementa al otro permitiendo tanto la reacción como las actividades de prevención de incidentes.

- El tercer objetivo específico se desarrolla en el capítulo 7 y en él se define la organización del CSIRT, para ello se hizo el análisis a partir de empresas de este ámbito ya formadas y se perfila a las personas formando un equipo de trabajo con solides y una estructura orgánica que permita flexibilidad ante el crecimiento continuo del servicio, todo esto cumpliendo estándares de calidad y aportando a la seguridad y al desarrollo tecnológico de la región colombiana en donde se ubicará. Las personas del equipo deberán ser las idóneas para que puedan cumplir la misión, visión y objetivos del CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, el personal a contratar debe sumar unos requisitos y características encaminados a la seguridad informática siendo el director general, la cabeza visible de la organización y sobre quien recae toda la responsabilidad del manejo tanto administrativo como operacional, es por ello que este principalmente debe tener una serie de conocimientos y experiencias que puedan llevar al éxito el emprendimiento.

- El objetivo específico 4 se desarrolla en el capítulo 8 definido como políticas operacionales del CSIRT, en el cual se pauta una a una las políticas a implementar en el desarrollo del proyecto, es importante mencionar que la seguridad de la información de los clientes, depende exclusivamente del manejo que le dé el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, por ello los empleados del CSIRT deberán cumplir a cabalidad una serie de compromisos y deberes que permitan salvaguardar tanto la información de los clientes como los activos de información del CSIRT.

11. RECOMENDACIONES

Como recomendación general se puede decir que se debe promover los servicios que presta un CSIRT como estrategia fundamental para garantizar la seguridad de la información, por ello las estrategias comerciales para el caso de estudio deben basarse en la necesidad de las organizaciones o entidades por proteger el bien más importante que tienen que son los activos de información.

Es importante que la promoción del servicio no solo sea a demanda, sino que se busque espacios de difusión como ferias empresariales, entre otras donde se dé a conocer el portafolio de servicios del CSIRT y la importancia de este para aquellas organizaciones que aún no conocen o no han implementado este mecanismo de defensa.

El CSIRT debe tener unas políticas internas de manejo de la información con las que da seguridad y fiabilidad a sus clientes acerca de su información, con lo que además de ello promueve buenas prácticas y credibilidad en el mercado por parte de sus clientes lo que eventualmente le ocasionara más demanda del servicio prestado.

El CSIRT debe generar alianzas estratégicas que permitan desarrollar planes de trabajo conjunto entre CSIRT lo que conllevara a un aprendizaje continuo y unas bases de datos de incidentes actualizadas fortaleciendo los conocimientos del CSIRT y el posicionamiento estratégico de la marca y de la localidad.

BIBLIOGRAFÍA

AGENCIA NACIONAL DE TIERRAS, COLOMBIA. Lineamientos de seguridad de la información, tratamiento y protección de datos personales. [ONLINE]. Bogota: ANT, 2017. [Citada: 02 abril 2020]. Disponible en http://www.agenciadetierras.gov.co/wp-content/uploads/201.

COLOMBIA, SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Resolución 8934 de 2014. [ONLINE]. Bogotá: Superintendencia de industria y comercio, 2014. [Citada 28 abril 2020]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?id=4041484.

ARCHIVO GENERAL DE LA NACION. COLOMBIA. Tablas de retención y transferencias documentales. [ONLINE]. Bogotá: Archivo general de la nación. [Citada 29 abril 2019]. Disponible en: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consul.

CARDONA, Lyda Durley., & URIBE, Andrés. Sistema de gestión de incidentes de seguridad informática para corbeta. [ONLINE]. Medellin: Universidad De San Buenaventura Seccional Medellín, 2015 [Citada: 30 septiembre 2019]. Disponible en:http://bibliotecadigit.

CASTAÑO GUTIERREZ, Jorge. Circular externa 007 de 2018. [ONLINE]. Bogotá: Superintendencia Financiera de Colombia, 2018. [Citada: 21 septiembre 2019]. Disponible en: https://fasecolda.com/cms/wp-content/uploads/2019/08/ce007-2018.pdf.

COLOMBIA, CONGRESO DE LA REPÚBLICA Ley 1437 de 2011. [ONLINE]. Bogotá: Congreso de la República, 2011 [Citada: 27 septiembre 2019]. Disponible en: https://camaratulua.org/wp-content/uploads/2016/02/CoDIGO_DE_PROC._ADMINISTRATIVO.pdf. [En línea]

COLOMBIA, CONGRESO DE LA REPÚBLICA Ley 1480 de 2011. [ONLINE]. Bogotá: Congreso de la República, 2011 [Citada: 27 septiembre 2019]. Disponible en: https://www.wipo.int/edocs/lexdocs/laws/es/co/co103es.pdf .

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1150 de 2007. [ONLINE]. Bogotá: Congreso de la República. [Citada: 27 septiembre 2019]. Disponible en: https://www.mintransporte.gov.co/descargar.php?idFile=711.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1273 de 2008. [ONLINE]. Bogotá: Congreso de la República, 2008 [Citada: 27 septiembre 2019]. Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1341 de 2009. [ONLINE]. Bogotá: Congreso de la República, 2009 [Citada: 27 septiembre 2019]. Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 1712 de 2014. [ONLINE]. Bogotá: Congreso de la República. [Citada: 27 septiembre 2019]. Disponible en: http://www.anticorrupcion.gov.co/SiteAssets/Paginas/Publicaciones/ley-1712.pdf.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527 de 1999. [ONLINE]. Bogotá: República de Colombia, 1999. [Citada: 27 septiembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 594 de 2000. [ONLINE]. Bogotá: Congreso de la República, 2000. [Citada: 27 septiembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-15049_documento.pdf.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 679 de 2001.[ONLINE]. Bogotá: Congreso de la República, 2001 [Citada: 27 septiembre 2019]. Disponible en: http://www.oas.org/juridico/spanish/cyb_col_ley_679_2001.pdf.

COLOMBIA, CONGRESO DE LA REPÚBLICA. Ley 962 de 2005. [ONLINE]. Bogotá: Congreso de la República. 2005. [Citada: 27 septiembre 2019]. Disponible en: http://www.aguasdebuga.net/intranet/sites/default/files/Ley%20962%20de%202005-.

COLOMBIA, MINTIC. Guía para la Gestión y Clasificación de incidentes de seguridad de la información. [ONLINE]. Bogotá: Ministerio de las tecnologías de la informacion y comunicación, 2014. [Citada: 29 septiembre 2019]. Disponible en https://www.mintic.gov.

COLOMBIA, PLANEACION NACIONAL. Documento conpes 3701. [ONLINE]. Bogotá: Departamento Nacional de Planeación, 2011. [Citada: 24 septiembre 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

COLOMBIA, POLICIA NACIONAL. Balance del cibercrimen en Colombia []ONLINE]. Bogotá: Policía Nacional, 2017. [Citada: 30 septiembre 2019. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf.

COLOMBIA, PRESIDENCIA DE LA REPÚBLICA. Decreto Ley 019 de 2012. [ONLINE]. Bogotá: Presidencia de la República. [Citada: 27 septiembre 2019]. Disponible en: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/Decreto-Ley-019-de-2012-A.

COLOMBIA, Supersalud. Gestión de servicios tecnológicos. [ONLINE]. Bogotá: Supersalud. [Citada: 2 octubre 2019]. Disponible en: https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSPD02.docx.

DIAZ, Jesús, FIRVIDA, Daniel y LOZANO, Marco. Identificación y reporte de incidentes de seguridad para operadores estratégicos. [ONLINE]. Madrid: Intecocert, 2013. [Citada:29 septiembre 2019]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/i.

ENISA. Cómo crear un CSIRT paso a paso. [ONLINE]. Enisa. [Citada: 4 Octubre 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport.

ESCUELA EUROPEA DE LA EXCELENCIA. El Anexo A y los controles de seguridad en ISO 27001. [ONLINE]. Madrid: Escuela Europea de la excelencia.

2019. [Citada: 03 octubre 2019] Obtenido de https://www.escuelaeuropeaexcelencia.com/2019/05/el-anexo-a-y-los-contr.

FIRST. Equipos CSIRT. [ONLINE]. First, 2019. [Citada: 17 septiembre 2019]. Disponible en: https://www.first.org/members/teams/?#.
FIRST. Primera Historia. [ONLINE]. First. 2015. [Citada:16 septiembre 2019]. Disponible en: https://www.first.org/about/history.

GALAN, Ricardo. Colombia, el país de Latinoamérica más afectado por el ransomware.

GORGONA, Luis. Primera respuesta: antes de que llegue la policía. [ONLINE] Mexico: OAS, 2018 [Citada: 3 octubre 2019]. Disponible en: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf.

INCIBE. Clasificacion de la informacion – Politicas de seguridad para la Pyme. [ONLINE]. Madrid: Instituto nacional de ciberseguridad. [Citada: 02 abril 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clas.

INCIBE. Taxonomia de ataques. [ONLINE]. Madrid: INCIBE-CERT, 2019 [Citada: 17 Octubre 2019]. Disponible en: https://www.incibe-cert.es/taxonomia .

IT GOVERNANCE INSTITUTE. COBIT Marco Referencial. [ONLINE]. Lincoln: Comité Directivo COBIT. 2017. [Citada: 11 septiembre2 2019]. Disponible en: http://files.uladech.edu.pe/docente/02659781/CAT/S07/02_03MarcoReferencial.pdf.

KALI LUNUX. Kali Linux By Offensive Security. [ONLINE] 2019. [Citada: 23 septiembre 2019] Disponible en: https://www.kali.org/.

LAFRANCO, Einar y PEREZ, Ernesto. CSIRTs. [ONLINE]. Madrid: CERT UNLP. [Citada: 02 octubre 2019]. Disponible en: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf .

MONTOYA AGUDELO, Cesar y BOYERO SAAVEDRA, Martin. El CRM como herramienta para el servicio al cliente en la organización. [ONLINE]. Medellin: Revista Científica "Visión de Futuro". 2012. [Citada: 23 septiembre 2019]. Disponible en: https://www.redalyc.org.

MONTOYA, German. La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. [ONLINE]. Bogotá: Asobancaria. [Citada: 30 septiembre 2019]. Disponible en: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf.

ORGANIZACION DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. [ONLINE]. Washington: Secretaría General de la Organización de los Estados Americanos (OEA). 2016. [Citada: 4 octubre 2019]. Disponible en https://www.sites.oas.or.

RAMIREZ CASTRO, Alexandra. Riesgo tecnológico y su impacto para las organizaciones parte i. [ONLINE]. México: Universidad nacional autónoma de México. 2016. [Citada: 30 septiembre 2019]. Disponible en: https://revista.seguridad.unam.mx/numero-14/riesgo-te.

REPUBLICA COLOMBIANA. (). Documento conpes 3701. Bogotá: Departamento Nacional de Planeación. Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

REPÚBLICA DE COLOMBIA. Constitución Política de Colombia. [ONLINE] Bogotá: Asamblea constituyente República de Colombia. [Citada: 27 septiembre 2019]. Disponible en:http://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf .

RTIR. Best Practical. [ONLINE] Best Practical. [Citada 12 septiembre 2019] Disponible en: https://bestpractical.com/rtir.

UNITED STATS, DEPARTMENT OF DEFENSE. Department Of Defense Trusted Computer System Evaluation Criteria. [ONLINE]. New York: Department Of Defense. 2015. [Citada: 24 septiembre 2019] Disponible en: https://csrc.nist.gov/csrc/media/publications/conference-.

UREÑA CENTENO, Francisco. Ciberataques la mayor amenaza actual, [ONLINE]. Madrid: Instituto español de estudios estratégicos. 2015. [Citada: 20 octubre 2019]. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCibera.

VARGAS CORDERO, Zoila Rosa. La investigación aplicada: una forma de conocer las realidades con evidencia científica. [ONLINE]. San Pedro: Universidad de Costa Rica, 2009. [Citada: 27 septiembre 2019]. Disponible en: https://www.redalyc.org/pdf/440/440150.

ANEXOS

Anexo A. Formato de encuesta digital a administradores TI

CIBERSEGURIDAD

Página 1

La organizacion donde labora ha tenido incidentes informáticos en el transcurso del ultimo año *

- ◯ sí
- ◯ no

Si su respuesta a la anterior pregunta fue, SI , identifique el tipo de incidentes.

- ☐ Acceso no autorizado a la información
- ☐ Aplicaciones comprometidas
- ☐ Bot
- ☐ Copyright
- ☐ Cuenta con privilegios altos afectada
- ☐ Cuenta sin privilegios afectada
- ☐ Denegación de servicio distribuido (DDoS)
- ☐ Denegación de servicios (DoS)
- ☐ Dialler
- ☐ Escaneo
- ☐ Explotación de vulnerabilidades
- ☐ Explotación sexual infantil/Racismo / Incitación a violencia
- ☐ Ingeniería Social
- ☐ Intentos de logueo
- ☐ Interrupción no intencionada
- ☐ Modificación o edición no autorizada de la información
- ☐ Nuevos ataques
- ☐ Phishing
- ☐ Rootkit
- ☐ Sabotaje
- ☐ Sniffing
- ☐ Spam
- ☐ Spyware
- ☐ Suplantación
- ☐ Trojan
- ☐ Uso no autorizado de recursos
- ☐ Virus
- ☐ Worm

Si se presentara un incidente informático tiene las herramientas necesarias para solucionarlo?

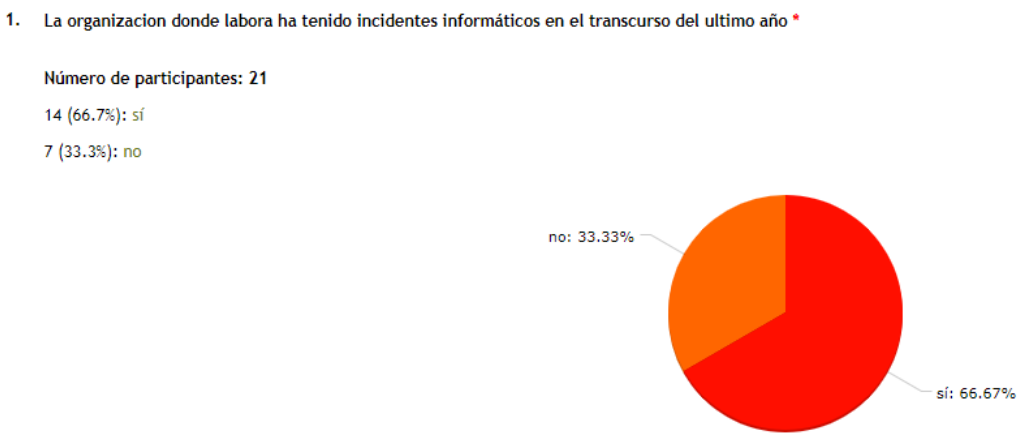
- ◯ sí
- ◯ no

Estaría dispuesto a contratar un equipo que prevenga y de respuesta los incedentes de seguridad informaticos de su entidad?

- ◯ sí
- ◯ no

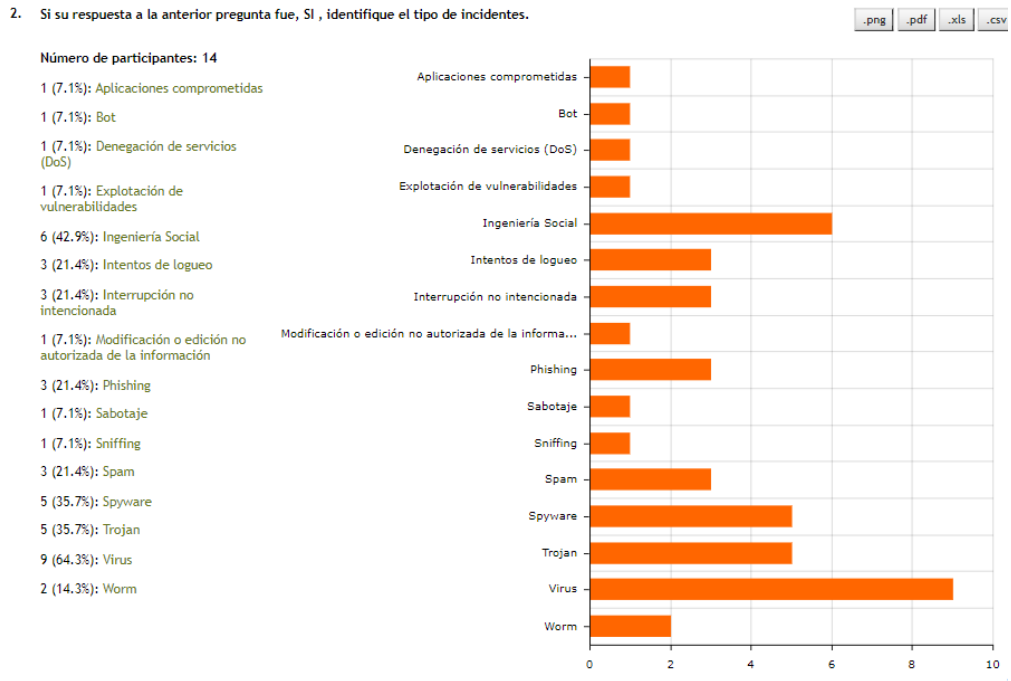
Anexo A. Resultados encuesta ciberseguridad dirigida a administradores TI.

Figura 4. Resultados pregunta 1 - Encuesta CIBERSEGURIDAD



Fuente: elaboración propia.

Figura 5. Resultados pregunta 2 - Encuesta CIBERSEGURIDAD.

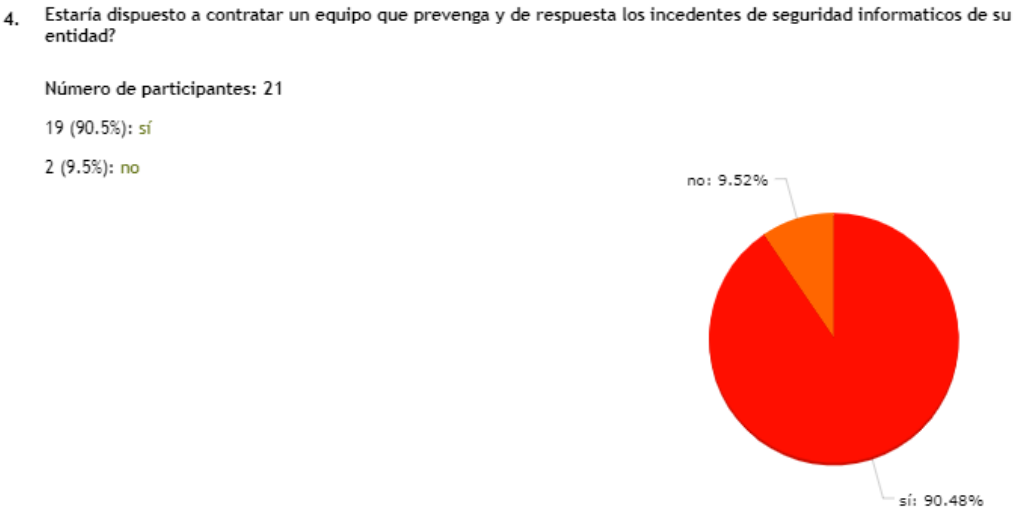


Fuente: elaboración propia.

Figura 6. Resultados pregunta 3 - Encuesta CIBERSEGURIDAD.

Fuente: elaboración propia.

Figura 7. Resultados pregunta 4 - Encuesta CIBERSEGURIDAD



Fuente: elaboración propia.

Anexo B. Enlace video proyecto seguridad informática I.
https://www.youtube.com/watch?v=fPfz99M8a00

Anexo C.. Enlace video proyecto seguridad informática II.
https://www.youtube.com/watch?v=3Iy1uOBFHQY

Anexo D . Resumen analítico especializado – RAE

RESUMEN ANALITICO ESPECIALIZADO – RAE UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD	
Tema	Diseño documental de un CSIRT
Titulo	Diseño documental para la implementación del CSIRT para el caso de estudio de la empresa Cibersecurity de Colombia LTDA
Autor	ROSERO NARVAEZ, William Andrés
Asesor	M.sc. John F. Quintero T.
Año	2021

Fuentes bibliográficas

COLOMBIA, MINTIC. Guía para la Gestión y Clasificación de incidentes de seguridad de la información. [ONLINE]. Bogotá: Ministerio de las tecnologías de la información y comunicación, 2014. [Citada: 29 septiembre 2019]. Disponible en https://www.mintic.gov.

DIAZ, Jesús, FIRVIDA, Daniel y LOZANO, Marco. Identificación y reporte de incidentes de seguridad para operadores estratégicos. [ONLINE]. Madrid: Intecocert, 2013. [Citada:29 septiembre 2019]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/i.

ENISA. Cómo crear un CSIRT paso a paso. [ONLINE]. Enisa. [Citada: 4 octubre 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport.

INCIBE. Clasificación de la información Políticas de seguridad para la Pyme. [ONLINE]. Madrid: Instituto nacional de ciberseguridad. [Citada: 02 abril 2020]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clas.

INCIBE. Taxonomía de ataques. [ONLINE]. Madrid: INCIBE-CERT, 2019 [Citada: 17 octubre 2019]. Disponible en: https://www.incibe-cert.es/taxonomia.

Resumen

El cibercrimen en Colombia tiene un alto índice y afecta a la ciudadanía, empresas e incluso organizaciones gubernamentales, muchas de estas no tienen un plan de contingencia ante estos hechos, a veces por desconocimiento o incluso por falta de recursos, es por ello que desde el caso de estudio Cybersecurity de Colombia LTDA, se ha planteado cubrir esta necesidad a partir del desarrollo de un centro de respuesta a incidentes de seguridad informática (CSIRT), esta es una organización que cuenta expertos que se encargan de la coordinación y el apoyo para la respuesta ante un evento o incidente de seguridad informática con métodos y herramientas que permitan reducir al máximo los riesgos o mitigar el impacto de un incidente en curso.

La consulta bibliográfica acerca de la ciberseguridad en Colombia permite mostrar las actividades propias que tendrá CSIRT, generando con esto un catálogo de los servicios que el CSIRT prestará a sus clientes, especificando su campo de aplicación según la jerarquización de ataques que el CSIRT cubrirá, lo que dará pie al organigrama y el diseño de roles y perfiles que cada profesional vinculado debe tener. Finalmente se generan las políticas de seguridad de la información, por medio de las cuales el CSIRT deberá garantizar la confidencialidad, integridad y disponibilidad de la información propia y de terceros que tenga bajo su custodia

Palabras clave	CSIRT, Seguridad, información, Incidente, SGSI

Contenidos

• Planteamiento del problema
• Objetivos
• Marco referencial
• Fase 1: estudios preliminares
• Fase 2: estructuración de los servicios del CSIRT
• Fase 3: organización del CSIRT
• Fase 4: políticas operacionales del CSIRT
• Resultados
• Conclusiones
• Recomendaciones

Objetivo general

Documentar el diseño de la implementación del CSIRT para el caso de estudio de la empresa CIBERSECURITY de Colombia Ltda.

Objetivos específicos

• Analizar la situación actual de la ciberseguridad en Colombia y crear una taxonomía de ataques para el ámbito de actuación del CSIRT.
• Definir el catálogo de servicios del CISRT como herramienta de presentación de la empresa hacia sus clientes.
• Especificar perfiles del equipo de trabajo y la estructura orgánica que conformará el CSIRT.
• Diseñar políticas y procedimientos operacionales del CSIRT.

Metodología

En el proyecto se aplica el modelo de investigación cualitativo y el tipo de investigación aplicada, las técnicas utilizadas en el proyecto son la consulta bibliográfica y documental, la que garantiza los fundamentos teóricos del proyecto, generando un proceso sistemático y secuencial de recolección de información, luego se implementa una selección, clasificación, evaluación y análisis de contenido del material recolectado que sirva como fuente teórica, conceptual y metodológica para el proyecto, que permita de esta manera realizar la

documentación de la implementación de un CSIRT para la empresa caso de estudio Cibersecurity de Colombia LTDA.

Además de ello se hará uso de la técnica de indagación e interpretación de datos utilizando la encuesta a administradores IT como posibles clientes del mercado; el documento se desarrolla en 4 fases las cuales dan cumplimiento a los objetivos específicos planteados para el proyecto, dentro de dichas fases se realizará tareas investigativas y se documentara todo lo concerniente al CSIRT de la empresa caso de estudio CIBERSECURITY de Colombia LTDA, por lo que se distribuirán de la siguiente forma:

Fase 1: Estudios preliminares.
Fase 2: Estructuración de los servicios del CSIRT.
Fase 3: Estructura orgánica del CSIRT.
Fase 4: Políticas operacionales del CSIRT.

Referentes teóricos y conceptuales

En la reseña y consulta sobre diferentes fuentes bibliográficas y normas los cuales sirvieron como apoyo teórico y para definir conceptos, están entre las más importantes:

• ISO 27001.
• COBIT.
• ITIL.
• Lineamientos de seguridad de la información, tratamiento y protección de datos personales de la ANT.
• FIRST.
• INCIBE.
• Guía para la Gestión y Clasificación de incidentes de seguridad de la información del MINTIC.
• ENISA. Cómo crear un CSIRT paso a paso.

Resultados

Actualmente Colombia tiene un marco normativo bastante amplio para contrarrestar los delitos informáticos, pero quienes manejan los incidentes, tienen un gran desconocimiento y no generan material probatorio de los incidentes presentados por lo que no tienen bases suficientes para hacer una denuncia solida ante las autoridades.

El estudio de factibilidad permite deducir que en Colombia hay un gran mercado para un CSIRT, por lo que el ámbito de aplicación para el caso de estudio de CIBERSECURITY de Colombia es CSIRT comercial, ya que es una opción viable para grandes y pequeñas empresas que no tienen los recursos para montar su propio equipo de respuesta o simplemente quieren ahorrar recursos.

Dentro de la taxonomía se hace una priorización para dar respuesta a los incidentes de información teniendo unas métricas que son respuesta alta, media y baja, siendo la métrica alta la atención inmediata y la baja la que se aplica a incidentes que no producen daños catastróficos sobre la infraestructura tecnológica; con esto se genera el portafolio de los servicios a prestar por parte del CSIRT haciendo referencia a servicios reactivos, proactivos y los de valor agregado para cubrir las necesidades de los usuarios finales.

En de la organización se establecen unas políticas organizacionales que permiten el manejo seguro de la información propia como la de sus clientes por lo que se establece que de no ser cumplidas puede haber pérdidas totales, parciales, fugas, eliminación y alteración de datos significativos que podrían incurrir en delitos informáticos y hasta en sanciones judiciales.

Conclusiones

Colombia tiene un marco normativo amplio pero que muchas veces no se logra aplicar por falta de conocimiento del personal TI, por lo que tampoco se puede realimentar para próximos ataques; el mapa de riesgos definido desde la taxonomía evidencia la gravedad del impacto que generaría la presencia de un ataque de estos siendo clasificado como catastrófico a los cuales el CSIRT debe brindar una atención de respuesta de nivel alto.

Hoy en día no es suficiente con la seguridad básica como los firewalls, antivirus, VPN, antimalware; también se debe complementar con los servicios que ofrece un CSIRT que puede ofrecer una base de conocimientos de incidentes actuales; no se puede garantizar una seguridad total sobre la infraestructura tecnológica ya que esto está en constante cambio y por ello los procesos y bases de conocimiento también deben actualizarse constantemente.

El CSIRT debe contar con un equipo de trabajo con solides y una estructura orgánica que permita flexibilidad ante el crecimiento continuo del servicio todo esto cumpliendo estándares de calidad y aportando a la seguridad y al desarrollo tecnológico de la región colombiana en donde se ubicara.

En cuanto a políticas para implementar en el desarrollo del CSIRT, es importante mencionar que la seguridad de la información de los clientes depende exclusivamente del manejo que le dé el CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA, por ello los empleados del CSIRT deberán cumplir a cabalidad una serie de compromisos y deberes que permitan salvaguardar tanto la información de los clientes como los activos de información del CSIRT.