ESTUDIO DOCUMENTAL, PARA LA CREACIÓN DEL CENTRO DE RESPUESTA A INCIDENTES CSIRT PARA CASO DE ESTUDIO “ESCENARIO ADMINISTRATIVO” CIBERSECURITY DE COLOMBIA LTDA.

LIBARDO BARBOSA VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2021

ESTUDIO DOCUMENTAL, PARA LA CREACIÓN DEL CENTRO DE RESPUESTA A INCIDENTES CSIRT PARA CASO DE ESTUDIO “ESCENARIO ADMINISTRATIVO” *CIBERSECURITY* DE COLOMBIA LTDA.

LIBARDO BARBOSA VARGAS

Proyecto Aplicado como requisito para optar al título de:
Especialista en Seguridad Informática

Esp. Ing. Edgar Mauricio López Rojas
Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C., enero 30 de 2021

A mi madre Luz Mila María Vargas Mejía, mi esposa Yulieth Valencia y mi hija Julieta Barbosa, las cuales han sido el motor de mis esfuerzos y dedicación día a día para lograr los objetivos trazados en mi vida, el cual estoy cumpliendo en este momento.

Libardo

AGRADECIMIENTOS

Libardo expresa su agradecimiento a:

A Dios, que es nuestro padre y creador de vida, quien me ha dado la fortaleza y capacidad, inteligencia y perseverancia, para poder luchar y lograr título tan importante. Por siempre guiarme en los pasos y proyectos que me he propuesto.

La Universidad Nacional Abierta y a Distancia, Sede José Acevedo y Gómez, así como a todos y cada uno de los tutores que han sido fundamentales al compartirme sus conocimientos educativos y experiencias en la materia de Ciberseguridad, en especial a los Ingenieros Edgar Mauricio López Rojas, Ingeniera Katherine Márceles y el Ingeniero Fernando Zambrano Hernández.

CONTENIDO

pág.

1 INTRODUCCIÓN 23

2 DEFINICIÓN DEL PROBLEMA 28

2.1 ANTECEDENTES 30
2.1.1 Necesidad de la Seguridad. 30
2.1.2 Los CSIRT en América Latina. 32
2.1.2.1 Brasil CERT.br. 33
2.1.2.2 Ecuador ecuCERT. 33
2.1.2.3 Perú PECERT. 33
2.1.2.4 Chile CSIRT. 33
2.1.2.5 Uruguay CERTUY. 33
2.1.2.6 Venezuela venCER. 33
2.1.2.7 Argentina CSIRT. 34
2.1.2.8 Colombia colCER. 34
2.1.2.9 CSIRT - B-SECURE. 35
2.1.2.10 CSIRT C-DOC. 35
2.1.2.11 CSIRT Olimpia. 36
2.1.2.12 CSIRT-CCIT. 36
2.1.2.13 CSIRT-ETB. 36
2.1.2.14 CSIRT PONAL. 37
2.1.2.15 CSIRT Digi. 37
2.1.2.16 CSIRT ETEK. 37
2.1.2.17 CSIRT ITSSOC. 38
2.1.2.18 CSIRT ShieldNow. 38
2.1.2.19 SOC Claro Colombia. 38
2.1.2.20 SOC-CCOC. 39
2.2 PLANTEAMIENTO DEL PROBLEMA 40
2.3 FORMULACIÓN DEL PROBLEMA 45
2.4 ALCANCE Y LIMITACIONES 45
2.4.1 Alcance. 45
2.4.2 Limitaciones. 45

3 JUSTIFICACIÓN 46

4 OBJETIVOS 51

4.1 OBJETIVO GENERAL 51
4.2 OBJETIVOS ESPECÍFICOS 51

5 MARCO DE REFERENCIA 52

5.1 MARCO TEÓRICO 52
5.1.1 Seguridad informática e Internet. 52
5.1.2 Seguridad de la Información. 53

5.1.3 Amenazas de la seguridad informática. 55
5.2 MARCO CONCEPTUAL 55
5.2.1 Definición de CSIRT. 55
5.2.1.1 Infraestructura física. 56
5.2.2 Tipos de CSIRT. 59
5.2.2.1 CSIRT del sector Académico. 59
5.2.2.2 CSIRT Comercial. 60
5.2.2.3 CSIRT del sector Público. 60
5.2.2.4 CSIRT interno. 60
5.2.2.5 CSIRT del sector Militar. 60
5.2.2.6 CSIRT Nacional. 61
5.2.2.7 CSIRT del sector de las (PYMES). 61
5.2.2.8 CSIRT del sector Financiero. 62
5.2.3 Ventajas de tener un CSIRT. 62
5.3 MARCO HISTÓRICO 62
5.3.1 Familia de normas ISO. 62
5.3.1.1 ISO 27000. 63
5.3.1.2 ISO 27001. 63
5.3.1.3 ISO 27002. 64
5.3.1.4 ISO 27003. 64
5.3.1.5 ISO 27004. 64
5.3.1.6 ISO 27005. 65
5.3.1.7 ISO 27006. 65
5.3.1.8 ISO 27007. 65
5.3.1.9 ISO 27008. 66
5.3.1.10 ISO 27009. 66
5.3.1.11 ISO 27010. 66
5.3.1.12 ISO 27035. 67
5.3.1.13 ISO 22301. 67
5.3.1.14 ISO 31000. 67
5.4 MARCO ESTADO ACTUAL 70
5.4.1 Estado actual de la seguridad cibernética en el país. 71
5.4.1.1 Política y Estrategia de Seguridad Cibernética. 71
5.4.1.2 Cultura Cibernética y Sociedad. 74
5.4.1.3 Capacitación y Habilidades de Seguridad Cibernética. 76
5.4.1.4 Marcos Legales y Regulatorios. 77
5.4.1.5 Estándares, Organizaciones y Tecnologías. 79
5.5 MARCO TECNOLÓGICO 82
5.5.1 Avances Tecnológicos. 82
5.5.2 Importancia de la tecnología. 83
5.5.3 Infraestructura tecnológica. 83
5.5.3.1 Software para ciberseguridad. 83
5.5.3.2 Hardware para ciberseguridad. 84
5.6 MARCO CONTEXTUAL 86
5.6.1 Propiedades de los Csirt Internacionales. 86

5.6.2 Modelos de los CERT y CSIRT. 88
5.6.3 Modelo Incrustado. 88
5.6.4 Modelo Organización Independiente. 89
5.6.5 Modelo campus. 90
5.6.6 Modelo voluntario. 90
5.6.7 Modelo Coordinador. 91
5.6.8 Modelo Distribuido. 92
5.6.9 Modelo Centralizado. 93
5.7 MARCO LEGAL 94
5.7.1 Ley 527 de 1999. 94
5.7.2 Ley 599 del 2000. 94
5.7.3 Ley Estatutaria 1266 de 2008. 95
5.7.4 Ley 1273 de 2009. 95
5.7.5 Ley 1341 de 2009. 95
5.7.6 Ley Estatutaria 1581 de 2012. 95
5.7.7 Ley 1712 de 2014. 95
5.7.8 Decreto presidencial 1081 del 2015. 95
5.7.9 Directiva NIS (UE) 2016/1148. 95
5.7.10 Reglamento (UE) 2019/881. 95
6 DISEÑO METODOLÓGICO 96
6.1 ESTUDIO METODOLÓGICO 96
6.2 ENFOQUE METODOLÓGICO 96
6.3 POBLACIÓN Y MUESTRA 96
6.3.1 Fuentes de información. 97
6.3.2 Recolección de información. 97
6.4 FASES DE TRABAJO 97
6.4.1 Fase 1. 98
6.4.2 Fase 2. 98
6.4.3 Fase 3. 98
6.4.4 Fase 4. 98
7 SERVICIOS QUE PRESTAR Y NECESIDADES DEL CSIRT 99
7.1 DESARROLLO DEL PLAN COMERCIAL. 99
7.1.1 Servicios reactivos. 100
7.1.2 Servicios Proactivos. 101
7.1.3 Servicios de Informática forense. 101
7.2 PLAN ESTRATÉGICO 103
7.2.1 Socios Estratégicos para el CSIRT. 103
7.2.2 Cooperación Internacional. 104
7.3 NECESIDADES 105
7.3.1 Necesidades de infraestructura física. 105
7.3.2 Necesidades de capacitación. 105
7.3.3 Necesidad de vigilancia. 106
7.3.4 Necesidades de talento humano. 106
7.3.5 Necesidades de subcontratación. 106

7.3.6 Necesidades del grupo de clientes atendido.....106
7.3.7 Necesidad de la estructura del equipo de trabajo. 106
7.3.8 Necesidad de hardware y software. 107
7.3.9 Necesidad de procesos y procedimientos.....107
7.3.10 Necesidades adicionales de otras áreas.....107
7.3.11 Necesidad de auto evaluación. 107
7.4 POLÍTICAS DEL CSIRT 108
7.4.1 Política de clasificación de información.....108
7.4.1.1 Los activos de información deben ser inventariados. 108
7.4.1.2 La información debe tener un propietario. 108
7.4.1.3 La información debe ser clasificada.....109
7.4.1.4 La información debe ser etiquetada y clasificada. 109
7.4.2 Política de protección de datos. 111
7.4.3 Política de retención de información. 111
7.4.4 Política de destrucción de información.....112
7.4.5 Política de divulgación de información. 113
7.4.6 Política sobre el acceso a la información. 114
7.4.7 Políticas de uso apropiado de los sistemas del CSIRT. 114
7.4.8 Política de eventos y definición de incidentes de seguridad. 115
7.4.8.1 Clasificación. 115
7.4.8.2 Clasificación del equipo de respuesta. 115
7.4.8.3 Eventos de seguridad. 116
7.4.9 Política de gestión de incidentes. 116
7.4.9.1 Responsabilidades. 116
7.4.9.2 Descripción. 117
7.4.9.3 Cumplimiento. 118
7.4.10 Política de cooperación. 118
8 ESTUDIAR Y APLICAR EL INTERCAMBIO DE MODELOS.....120
8.1 CIBERSEGURIDAD Y MODELOS EN PAÍSES VECINOS 120
8.1.1 Análisis de ciberseguridad en Brasil. 120
8.1.2 Modelos de los CSIRT en Brasil. 121
8.1.2.1 NIC.br. 121
8.1.2.2 CEO / RedeRio. 122
8.1.2.3 CERT.br. 122
8.1.3 Análisis de ciberseguridad en Chile. 122
8.1.4 Csirt en Chile. 123
8.1.4.1 Csirt.gob.cl. 123
8.1.4.2 Herramientas y software. 125
8.1.4.3 CLCERT. 127
8.1.5 Análisis de ciberseguridad Ecuador. 127
8.1.6 Modelos de Csirt en Ecuador. 127
8.1.6.1 Ecuador ecuCERT. 128
8.1.6.2 CSIRT CEDIA. 128
8.2 MODELO EN BASE A LA METODOLOGÍAS COHERENTES 131

8.2.1 Análisis del modelo. 131
9 ATENCIÓN Y SEGUIMIENTO A INCIDENTES DE SEGURIDAD 133
9.1 DETECCIÓN DE INCIDENTES DE SEGURIDAD 133
9.1.1 Medios de detección. 133
9.1.1.1 Reporte de usuarios. 133
9.1.1.2 Monitoreo de sistemas de información. 133
9.1.1.3 Alertas de seguridad. 133
9.2 REPORTE DE INCIDENTES 133
9.2.1 Medios de reporte. 134
9.2.2 Formato de reporte. 134
9.2.3 Creación del incidente 135
9.2.4 Registro de incidentes 136
9.2.5 Asignación. 137
9.3 EVALUACIÓN 137
9.3.1 Evaluación. 137
9.3.1.1 Impacto crítico. 137
9.3.1.2 Impacto alto. 138
9.3.1.3 Impacto medio. 139
9.3.1.4 Impacto bajo. 139
9.3.1.5 Valor del Impacto. 139
9.3.2 Tiempos de respuesta 140
9.4 GESTIÓN DE INCIDENTES 140
9.4.1 Preparación del incidente 141
9.4.2 Identificación. 141
9.4.3 Contención. 141
9.4.4 Mitigación. 141
9.4.5 Recuperación. 141
9.4.6 Post incidente. 142
9.4.7 Modelo de atención a incidentes. 143
10 DEFINICIÓN DE PERFILES Y ORGANIGRAMA DEL CSIRT 145
10.1 MISIÓN Y VISIÓN DEL CSIRT 145
10.1.1 Misión 145
10.1.2 Visión. 146
10.2 DEFINICIÓN DE ROLES Y PERFILES 146
10.2.1 Dirección de Tecnología. 146
10.2.1.1 Perfil. 146
10.2.1.2 Formación académica. 146
10.2.1.3 Experiencia. 147
10.2.2 Jefe de operaciones. 147
10.2.2.1 Perfil. 148
10.2.2.2 Formación académica. 148
10.2.2.3 Experiencia. 148
10.2.3 Coordinador de infraestructura. 149
10.2.3.1 Perfil. 149

10.2.3.2 Formación académica. 149
10.2.3.3 Experiencia. 149
10.2.4 Coordinador de ciberseguridad. 150
10.2.4.1 Perfil. 150
10.2.4.2 Formación académica. 150
10.2.4.3 Experiencia. 151
10.2.5 Especialista en Ciberseguridad. 151
10.2.5.1 Perfil. 151
10.2.5.2 Formación académica. 152
10.2.5.3 Experiencia. 152
10.2.6 Especialista en Informática Forense. 153
10.2.6.1 Perfil. 153
10.2.6.2 Formación académica. 153
10.2.6.3 Experiencia. 154
10.2.7 Especialista Voz IP y Telefonía Móvil. 154
10.2.7.1 Perfil. 154
10.2.7.2 Formación académica. 154
10.2.7.3 Experiencia. 155
10.2.8 Especialista Infraestructura y Redes. 155
10.2.8.1 Perfil. 156
10.2.8.2 Formación académica. 156
10.2.8.3 Experiencia. 156
10.2.9 Especialista SO - Linux - UNIX - Windows. 157
10.2.9.1 Perfil. 157
10.2.9.2 Formación académica. 157
10.2.9.3 Experiencia. 157
10.2.10 Analista en Ciberseguridad. 158
10.2.10.1 Perfil. 158
10.2.10.2 Formación académica. 158
10.2.10.3 Experiencia. 159
10.2.11 Analista en Informática Forense. 159
10.2.11.1 Perfil. 159
10.2.11.2 Formación académica. 159
10.2.11.3 Experiencia. 160
10.2.12 Analista de Infraestructura. 160
10.2.12.1 Perfil. 160
10.2.12.2 Formación académica. 161
10.2.12.3 Experiencia. 161
10.3 ORGANIGRAMA DE CIBERSECURITY DE COLOMBIA LTDA. 161
10.3.1 Estructura interna CSIRT Cibersecurity de Colombia LTDA. 164
11 CONCLUSIONES 165
12 RECOMENDACIONES 167
13 ANEXOS 168

13.1 ANEXO 1: 168
13.1.1 Reporte incidentes de seguridad de la información. 168

LISTA DE TABLAS

pág.

Tabla 1. Nombres de Csirt. 59
Tabla 2 Análisis de las propiedades de un CSIRT.....86
Tabla 3. Puntos clave de los CSIRT. 87
Tabla 4. Socios esenciales para un CSIRT 103

LISTA DE CUADROS

pág.

Cuadro 1. Tipos de servicios ofertados.....102
Cuadro 2. Clasificación de incidentes.....123
Cuadro 3. Valores de criticidad de los impactos.....140
Cuadro 4. Tiempo de respuesta.....140

LISTA DE FIGURAS

pág.

Figura 1. Resultados Cibercrimen en Colombia.....24
Figura 2. Crecimiento de miembros por año.....32
Figura 3. Centros de atención registrado en Colombia según FIRST.....35
Figura 4. Estructura de un CSIRT.....56
Figura 5. Estructura a nivel de hardware, software y red.....58
Figura 6. Descripción de los estándares de la familia ISO.....68
Figura 7. La necesidad de seguridad como se convierte en riesgo.....69
Figura 8. Comparativo política y estrategia Ciberseguridad 2016 Vs 2020.....73
Figura 9. Comparativo Cultura Cibernética y Sociedad 2016 Vs 2020.....75
Figura 10. Comparativo Formación, Capacitación y Habilidades 2016 Vs 2020.....77
Figura 11. Comparativo Marcos Legales y Regulatorios 2016 Vs 2020.....79
Figura 12. Comparativo Estándares 2016 Vs 2020.....81
Figura 13. Situación digital en Colombia 2020.....82
Figura 14. Modelos organizacionales de los CSIRTs.....94
Figura 15 Etiquetado de documentos digitales.....110
Figura 16. Listado de Herramientas y Software.....126
Figura 17. Portafolio Universidades.....129
Figura 18. Portafolio institutos.....130
Figura 19. Portafolio Colegios.....131
Figura 20. Contenido del reporte de incidente de seguridad.....135
Figura 21. Nivel de impacto en los incidentes de seguridad.....137
Figura 22. Fases de la gestión de un incidente de seguridad.....142
Figura 23. Modelo de atención a incidentes de seguridad.....144
Figura 24. Organigrama Interno de Cibersecurity de Colombia LTDA.....163
Figura 25. Estructura CSIRT Empresa Cibersecurity de Colombia LTDA.....164

GLOSARIO

ACTIVOS**:** es un bien que posee una empresa, el cual se convierte en la razón de esta, se debe cuidar y proteger, pues le permitirá continuar operando en el mercado que este incursionando, de esta manera se convierte en el factor más importante que se cuenta, por lo que muchas empresas entienden el concepto y tratan de protegerlos al máximo.

AMENAZA: referencia de una causa potencial de un incidente de seguridad no deseado, el cual puede provocar daños a los sistemas de una la organización.

SISTEMA OPERATIVO: es el primer programa instalado en un equipo, es un programa maestro sobre el cual corren las aplicaciones, mientras se encarga de la administración de los recursos del sistema, conocido en la actualidad por diferentes fabricantes como por ej., *Windows* o Linux.

ATAQUE**:** acción que se puede realizar directa o indirectamente, mediante la utilización de programas maliciosos que buscan un fin inicial, el cual satisfaga las necesidades del atacante, son realizados con distintos objetivos, desde lo económico, político, personal y hasta fines desconocidos tanto para el atacante como para la víctima.

WIRESHARK: corresponde a un potente analizador de protocolos de red, este permite dar un vistazo general al tráfico que se está trasmitiendo por la red, mostrando la información importante que se debe conocer del análisis para que se tomen mejores decisiones en cuanto al funcionamiento de estas y las mejoras que se le deban realizar, adicional es muy importante para la parte de desarrollo[1].

HONEYPOT: este sistema operativo es utilizado, como un señuelo dentro de las redes y sistemas de información, con el fin de que pueda proteger a los sistemas, nos alerta de posibles ataques, así mismo, funciona como un señuelo que puede engañar a los atacantes, creando un sistema falso completamente aislado del sistema real, haciendo que dichos atacantes crean que ya pudieron ingresar a este y que han tomado el control, una de sus funciones es poder obtener información de los ataques, con el fin de poder identificar cuáles son sus objetivos, pues recolectando toda esta información, es de suma importancia para luego ser usada en la corrección de las vulnerabilidades que se detectaron en dicho ataque.

CRACKERS: son personas que construyen cosas para el bien de todos y ayudan a que los usuarios no sean víctimas de muchos ataques con las vulnerabilidades que

[1] INCIBE INSTITUTO NACIONAL DE CIBERSEGURIDAD. (España) Analizadores de red en sistemas de control. 10 de febrero de 2017 [Sitio Web]. [Consulta: 12 abril 2020] Disponible en: https://www.incibe-cert.es/blog/analizadores-red-sistemas-control

puedan tener en sus equipos o redes, así mismo ayudan a realizar pruebas de penetración a sistemas de organizaciones legítimas, con el fin de que estos detecten las vulnerabilidades que se tengan antes de que sean víctimas por las fallas que no han sido descubiertas en los sistemas.

CSIRT: es un centro conformado por un grupo de personas capacitadas que dan respuesta ante incidentes informáticos, este busca que las empresas puedan volver a sus operaciones normales con el menor impacto aceptable, de esta manera se da continuidad al negocio, reevaluando los daños y en lo posible se especializa en que estos sean menores, de fácil mitigación y recuperación.

TCPDUMP: herramienta utilizada para analizar redes de sistemas operativos Linux, con la línea de comandos, permitiendo tener información en tiempo real del tráfico de la red.

SEGURIDAD DEL SISTEMA: es un proceso que elimina la mayor cantidad de riesgos que puedan afectar la seguridad, a través de la desinstalación de programas, protocolos, servicios y utilidades del sistema que sean innecesarios.

RIESGO: el riesgo en seguridad de la información es básicamente la probabilidad de que existan amenazas que puedan ser explotadas, las diferentes vulnerabilidades que existen en los sistemas o partes de la infraestructura tecnológica de una organización, los riesgos siempre están presentes y por esta razón es que existen carreras tan importantes como seguridad de la información y seguridad informática.

HACKERS: según lo indica Malwarebytes en su página oficial, su actuar es destruyendo lo que encuentran y cuando logran crear algo lo hacen con el único objetivo, de obtener algún beneficio propio, ya que no les interesa que se dé a conocer la información que sirva para realizar prevención, todo lo contrario, tratan de ocultarla para que las posibles víctimas sean mucho más vulnerables y les faciliten el trabajo en el menor tiempo posible[2].

ISO 27001:2013: es la norma colombiana, diseñada y enfocada a la protección de todos los datos entre tanto sean públicos o privados, con el fin de que se puedan resguardar, proteger y tener bajo llave la confidencialidad de estos[3].

PHISHING: es un ataque que busca a través de estrategias como la ingeniería social de convencer al atacado a través de la suplantación de identidad, pretender

[2] MALWAREBYTES. Hacker. Todo sobre el hackeo [En Línea]. Santa Clara, California Estados Unidos. [Consulta: 12 marzo 2020] Disponible en https://es.malwarebytes.com/hacker/

[3] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27000: 2018. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario. Ginebra, Suiza. Edición 5. [Sitio Web] febrero 2018 [Consulta: 12 de marzo 2020]. P. 27. Disponible en: https://www.iso.org/standard/73906.html

que se dé, información confidencial, sin que este se dé por enterado de que será utilizada para luego cometer un ilícito dentro de la organización y de que de una u otra manera fue ayudado por una persona de la misma organización.

RANSOMWARE: *software* sofisticado y malicioso, que al insertar el virus o contaminar cualquier equipo, se tiene la capacidad total y completa de este, para luego apoderarse de la información que pueda tener, posteriormente se solicita a la víctima un pago por la recuperación de la información que fue secuestrada.

SOC: es un equipo de protección, reacción, monitoreo, para realizar los análisis, y dar respuesta a las amenazas de seguridad, estos equipos, se encargan adicional de investigar las vulnerabilidades, presentadas en ocasiones llegando a su origen, por lo general son contratados o puestos en marcha por organizaciones que ven la necesidad de proteger sus activos, ya que estos funcionan 24/7 lo cual permite tener un cubrimiento total de toda la operación durante la producción o fuera de ella.

VULNERABILIDAD: se determina como las condiciones y características del sistema (incluyendo quien lo maneja), lo que lo hace susceptible a amenazas, conllevando a sufrir algún daño a causa de estas.

COPIA DE RESPALDO: como lo indica la Institución Nacional de Ciberseguridad INCIBE, es el procedimiento disponible que se tiene para restaurar la información en el evento que en los archivos originales se presente alguna perdida o daño, permitiendo que la organización no tenga que reinventarse nuevamente, sino, que pueda arrancar desde determinado punto según sea su última copia de seguridad realizada[4].

IPS: sistemas de prevención de intrusiones, este tipo de sistema de prevención es de suma importancia dentro de la prevención que debe tener una red o sistemas de una compañía, pues este hace parte de las primeras líneas de defesa, complementado con los *firewalls*, estos sistemas de defensa permiten tomar acciones rápidamente ante un ataque, las principales características de protección de un IPS, son especialmente en las capas 3 y 7 del modelo OSI, una de las ventajas características que tienen los IPS, es que tienen la potestad de poder tomar control del sistema para protegerlo, aplicando políticas de seguridad que permitan salvaguardar las redes y su información[5].

[4] INCIBE INSTITUCIÓN NACIONAL DE CIBERSEGURIDAD (España) Copias de seguridad, una guía de aproximación para el empresario. [Citado en 12 marzo de 2020] Op. Cit. P. 3-32

[5] INFOTECS. IPS: Sistema de Prevención de Intrusos. Actualización: 13 de marzo de 2019. [En Línea] Blog. [Consulta: 12 marzo 2020] Disponible en: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

RESUMEN

En el presente proyecto, se podrá identificar la manera coherente como se debe llevar a cabo cada uno de los pasos para el estudio documental de un CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas) dirigido especialmente a la empresa Cibersecurity de Colombia LTDA. Dentro del documento se establecerán los objetivos que se desarrollaron, en los cuales se evidencia la organización y los requerimientos principales que tiene el CSIRT, como definir la necesidad del diseño documental, de un equipo de respuesta a incidente de seguridad para la empresa, justificando esa necesidad de seguridad dentro de la empresa y los demás sectores a los cuales los servicios pueden dar solución a los inconvenientes de seguridad, por los que pueda estar pasando, se explica en los marcos de referencia los pilares fundamentales de la seguridad informática, así como sus orígenes, dando a conocer el por qué es de suma importancia vigilar y cuidar los activos de cualquier organización, teniendo presente que siempre existen amenazas que pueden llevar a una organización a perderlo todo solo en cuestión de horas por un ataque informático, se recalca la importancia de colocar en práctica los diferentes estándares de la seguridad de la información, representación de la familia ISO 27000 entre otras que son un complemento esencial.

Se realizó consultas bibliográficas de los principales y más importantes CSIRT en todo el mundo, desde el sector militar, gobierno, educativo, bancario y los principales referentes de ciberseguridad, representados por organizaciones y personalidades expertas en materia de ciberseguridad moderna, los cuales son las defensas de muchas organizaciones y empresas que han tenido que sortear sobre muchos ataques informáticos, lo cual los llevó a tener mejores herramientas para poder enfrentar los enemigos de la red de Internet. Así mismo se resalta los equipos ya establecidos en el país, los cuales han sido y son una fuente de experiencia muy importante para los que pretenden incursionar en el mercado de la Ciberseguridad, otros equipos de gran importancia son los equipos de infraestructura crítica que se encuentran en cada uno de los países de América latina, pues en estos se hizo énfasis por su importancia y cercanía con Colombia, dichos equipos son los CSIRT nacionales de cada país, siendo los coordinadores nacionales y representantes de forma internacional. Dichos equipos han logrado generar unos antecedentes importantes en materia de seguridad de la información, dejando unas lecciones aprendidas y poder establecer números estadísticos que ayudan a la toma de decisión y mejoramiento de la seguridad informática.

En Colombia se han tomado medidas muy importantes en materia jurídica en relación con Ciberseguridad y la violación de datos informáticos, pues dichas acciones día a día cobra nuevas víctimas, sin ningún tipo de exclusión de género,

religión, estrato, actividad comercial o región, por esta razón se han decretado herramientas jurídicas que ayudan a imposición de penas, mediante la judicialización y condena de los actores que las cometen, es por esta razón que se definió un marco jurídico en el cual se expresan las principales leyes que se encargan de garantizar las penas y aprensión de los delincuentes informáticos tras las rejas, igualmente se determinó el tipo de cliente a los cuales se dirigió y los servicios que se prestarán, en el presente proyecto documental, indicando la manera en que se consultó la información necesaria para lograr determinar cómo se desarrollaría el mismo. Dichos servicios serán ofertados en tres segmentos, los servicios proactivos, reactivos y forenses, estos últimos son un valor agregado del CSIRT, con el fin de poder complementar los demás servicios, razón por la cual se determinaron las necesidades que este tendrá en su momento, muchas de estas necesidades serán solucionadas con la ayuda de las políticas y procesos que se determinaron para el CSIRT.

Se consultaron varios modelos existentes con el fin de que se pudiese aplicar uno que se acoplara con las necesidades e infraestructura ya existente de la empresa Cibersecurity de Colombia LTDA. De otra manera se pudo establecer la manera de cómo se llevaría a cabo la atención de los incidentes de seguridad de la información, elaborando un modelo de atención de incidentes, con un formato de recolección de la información necesaria para iniciar con el análisis y evaluación del mismo, este permite determinar si se debe pasar al colCERT nacional o se dará respuesta dentro del equipo con el apoyo del personal especializado del CSIRT, cada uno de los integrantes del grupo cuenta con un perfil, para la correcta atención de dichos incidentes de seguridad, obteniendo un cargo y funciones necesarias que deben cumplir, así mismo se estableció el organigrama de la empresa, así como la Misión y Visión.

Palabras clave: Seguridad, Información, confidencialidad, integridad, disponibilidad.

ABSTRACT

In this project, it will be possible to identify the coherent way how each of the steps should be carried out for the documentary study of a CSIRT (Computer Security Incident Response Team) aimed especially at the company. Cibersecurity de Colombia LTDA. Within the document, the objectives will be established, which were developed, in which the organization and the main requirements that the CSIRT has is evidenced, going through defining the need that led to the document design, of a security incident response team to The company, justifying this need for security within the company and the other sectors to which the services can provide a solution to the security problems they may be experiencing, the fundamental pillars of computer security are explained in the reference frameworks , as well as its origins, revealing why it is of utmost importance to monitor and take care of the assets of any organization, bearing in mind that there are always threats that can lead an organization to lose everything only in a matter of hours due to a computer attack, the importance of putting into practice the different standards of information security is emphasized, it represents ntation of the ISO 27000 family among others that are an essential complement.

Bibliographic consultations were made of the main and most important CSIRTs around the world, from the military, government, educational, banking sectors and the main cybersecurity references, represented by organizations and experts in modern cybersecurity, which are the defenses of many organizations and companies that have had to deal with many computer attacks, which led them to have better tools to face the enemies of the Internet network. Likewise, the teams already established in the country are highlighted, which have been and are a very important source of experience for those who intend to enter the Cybersecurity market, other teams of great importance are the critical infrastructure teams that are in each one of the Latin American countries, as they emphasized their importance and proximity to Colombia, said teams are the national CSIRTs of each country, being the national coordinators and international representatives. Said teams have managed to generate an important background on information security, leaving some learned injuries and being able to establish statistical numbers that help decision-making and improvement of computer security.

In Colombia, very important legal measures have been taken in relation to Cybersecurity and the violation of computer data, since such actions daily claim new victims, without any type of exclusion of gender, religion, stratum, commercial activity or region, for For this reason, legal tools have been decreed that help to impose penalties, through the prosecution and conviction of the actors who commit them, it is for this reason that a legal framework was defined in which the main laws that are responsible for guaranteeing the penalties and apprehension of computer

criminals behind bars, the type of client to which it was directed and the services to be provided was also determined, in this documentary project, indicating the way in which the necessary information was consulted to determine how it would develop itself. These services will be offered in three segments, proactive, reactive and forensic services, the latter are an added value of the CSIRT, in order to complement the other services, which is why the needs that it will have at the time were determined, many of these needs will be addressed with the help of the policies and processes that were determined for the CSIRT.

Several existing models were consulted so that one could be applied that would be coupled with the needs and already existing infrastructure of the company Cibersecurity de Colombia LTDA. Otherwise, it was possible to establish the way in which the attention of the information security incidents would be carried out, developing an incident attention model, with a format for collecting the information necessary to start with the analysis and evaluation of the Likewise, this allows to determine if the national colCERT should be passed or a response will be given within the team with the support of the specialized CSIRT staff, each of the group members has a profile, for the correct attention of said security incidents, obtaining a position and necessary functions that they must fulfill, likewise the organization chart of the company was established, as well as the Mission and Vision.

Keywords: Security, Information, confidentiality, integrity, availability.

1 INTRODUCCIÓN

Debido al gran incremento del uso de Internet, los sistemas de información, en efecto, se han transformado en una infraestructura crítica la cual debe ser salvaguardada. Se entiende por infraestructura crítica todos aquellos servicios fundamentales y esenciales, de soporte que son obligatorios, para asegurar la operación de cualquier empresa sin importar su objeto, siendo que las telecomunicaciones, los sistemas de información, el transporte, los suministros alimenticios, la generación de energía, los sistemas de producción, de gas y petróleo, los sistemas bancarios y financieros, como también los servicios de salud y emergencias, todos ellos son sistemas de información, que han sido implementados en infraestructuras críticas, en diferentes partes del país. La expansión constante de Internet ha conllevado a un crecimiento exponencial de diferentes sistemas de información, todos ellos con un único propósito, poder aumentar la producción de datos informáticos, coadyuvando al incremento de la producción de mercados y productos, de cada una de las compañías que los implementa. Así como los sistemas de tecnología implementados día a día, tienden a distribuirse, también lo hace la gestión en sí misma. Es por ello que crece la demanda de servicios de seguridad informática, cada servicio implementado, requiere de un mantenimiento y unas medidas de protección, que le garanticen su producción y vida útil. Desafortunadamente el carácter dinámico e interconectado que se maneja de los sistemas, ocasiona que los ciberataques puedan ser articulados y propagados ágilmente en forma global, atravesando límites geográficos y jurisdicciones nacionales e internacionales, se considera con gran facilidad explotar un sin número de vulnerabilidades y problemas de seguridad, que se generan en Internet con la implementación de un nuevo sistema, con la desventaja del panorama, que es relativamente sencillo ocultar la indudable identidad u origen del individuo responsable del ataque. Siendo indispensablemente necesario contar con la posibilidad de coordinar, analizar y responder a ataques informáticos a través de servicios de atención a incidentes de seguridad, mediante Equipos de Respuesta ante Incidencias de Seguridad Informática[6].

Con respecto al párrafo anterior, se dará a conocer datos relevantes que demuestran la importancia de la seguridad informática en el país, así como los sectores más afectados por ataques informáticos y la cantidad de ataques recibidos en cifras hasta el año 2019, información aportada por varias entidades en Colombia, como lo son Policía nacional, Cámara colombiana de Informática e ImpactoTic,

[6] CAROZO Eduardo: MARTÍNEZ Carlos y VIDAL Leonardo. CERTuy: Hacia un CSIRT Nacional. CSIRT – ANTEL. Grupo de Seguridad Informática, Facultad de Ingeniería, Universidad de la República de Uruguay. [En línea] [Consulta: 12 octubre 2019] P. 18. Disponible en: https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

mediante análisis Tendencias de Cibercrimen en Colombia 2019-2020[7] tal como se aprecia en la Figura 1.

Figura 1. Resultados Cibercrimen en Colombia

Fuente: CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES, POLICÍA NACIONAL DE COLOMBIA Y IMPACTOTIC, [En línea] Tendencias de Cibercrimen en Colombia 2019-2020, [Consulta: 12 octubre 2019] P. 7-9 Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Actualmente se vive un mundo muy cambiante cada día y si se habla de la tecnología lo es aún más, pues, se ven nuevas herramientas que sorprenden e invitan a estar más y más conectados a las redes de internet, por la misma necesidad del futuro tecnológico que se aproxima cada día y de la sociedad misma como tal, principalmente la economía tan creciente, donde los nuevos mercados tienen la necesidad absoluta de la conexión a internet, como lo son redes información, comunicaciones y sistemas, son tan esenciales para cualquier sociedad, los cuales, establecen un factor muy importante del desarrollo monetario y social, sin importar la comunidad, la sociedad o factor socio económico que los componga, para todos y cada uno de ellos tiene el mismo significado y resultado. Siendo así que la sistematización, junto con las conexiones a internet, se han transformado en productos esenciales para cualquier comunidad, persona o compañía. Es por ello que, la seguridad informática en las redes o sistemas informáticos, son una cuestión que puede afectar o mejorar los intereses de la sociedad en general, es así, que la sistematización en caso negativo, pueden enfrentarse a una diversidad de problemas debido a la complejidad de los mismos, arrojando un sinnúmero de accidentes, a errores que desencadenaran en una serie de ataques cibernéticos, donde los más afectados son los sistemas de información,

[7] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES, POLICÍA NACIONAL DE COLOMBIA Y IMPACTOTIC, [En línea] Tendencias de Cibercrimen en Colombia 2019-2020, octubre 2019. [Consulta: 12 diciembre 2019] P. 7-36 Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

los cuales prestan servicios vitales de gran importancia, para el bienestar de una comunidad entera, en el caso más específico una organización o ciudadano del común. Muchas organizaciones nacionales e internacionales, luchan y apoyan a las demás en un común acuerdo, poder llegar a establecer mecanismos que garanticen la correcta protección de los sistemas de información y una correcta atención a los incidentes de seguridad que se presenten dentro del grupo o usuarios que se atiendan, una institución que se encuentra muy comprometida con esta causa es, La ENISA que apoya la creación de nuevos CSIRT mediante un documento titulado «Cómo crear un CSIRT paso a paso con una lista de comprobación complementaria», que ayudará a los lectores a entender, interpretar y poder implementar su propio CSIRT[8].

La importancia de un CSIRT representa un factor clave para las empresas, así como para los usuarios de Internet, los cuales se basan principalmente en brindar servicios de seguridad informática, de modo que la integridad de los datos informáticos, el software y la conservación del hardware, penden en gran manera de este componente. Además de solucionar problemas de seguridad informática, son pieza fundamental a la hora de educar a los usuarios para que no vuelvan a repetir errores, que generen incidentes de seguridad, lo anterior es de suma importancia, si se tiene en cuenta que, el crecimiento constante de los sistemas de información, así como la manifestación de múltiples mecanismos de información, el uso de otros sistemas informáticos y operativos, se han establecido interconexiones entre todos estos elementos, los cuales han favorecido de gran manera al desarrollo, comercial, competitivo y operativo, también se debe indicar que ha sido un factor determinante para la propagación de nuevas amenazas de ciberseguridad, en su mayoría son más sofisticadas cada vez, difíciles de resolver y poder determinar su origen, la seguridad de la información, brinda tres aspectos fundamentales, permitiendo establecer los lineamientos necesarios para poderlos cumplir, los cuales son, (Confidencialidad) garantía de acceso únicamente por usuarios autorizados, (Integridad) conservación única y exacta, así como la disponibilidad, de la garantía única al acceso del usuario autorizado que la necesite[9].

La tecnología ha cobrado la importancia necesaria, como para el desarrollo administrativo del presente proyecto aplicado, el cual se encuentra establecido en el diseño documental de un CSIRT Computer Security Incident Response Team,

[8] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. (Grecia). ENISA. cómo crear un CSIRT paso a paso. Producto WP2006/5.1(CERT-D1/D2) [Consulta: 12 abril 2020]. P. 12-90 Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

[9] URIBE RAYAS Edgar Felipe. Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática. Centro de Investigación de Matemáticas A:C: Obtener grado en Maestro en Ingeniería de Software. México. (CSIRT) [Consulta: 12 abril 2020]. P. 21-211 Disponible en: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/437/1/ZACTE42.pdf

Equipo de Respuesta ante Incidencias de Seguridad Informáticas, para la empresa Cibersecurity de Colombia LTDA. Se establece una metodología de consulta de información de autores que han realizado trabajos destacados, relacionando la implementación de este tipo de equipos de respuesta a incidentes de seguridad, o en algunos casos dan las pautas para realizar o implementarlos, como se pretende dar a entender en el presente proyecto aplicado, el cual se realiza mediante un enfoque administrativo, indicando la manera de como poder colocar en marcha el CSIRT mediante un trabajo escrito. Es así como estos autores han contribuido a que la seguridad de la información, cada día sea más competente en sus procesos, durante la consulta de estas fuentes y citas bibliográficas, se han resaltado aportes muy importantes, como los diferentes modelos de los CSIRT nivel nacional e internacional, lo que ha permitido entender de manera más detallada los diferentes enfoques que se pueden dar a los equipos que se pretendan crear, un documento que da una fuente de información muy importante es el redactado por la organización de los estados americanos OEA, el cual se titula “Buenas prácticas para establecer un CSIRT nacional” otro documento muy importante para la implementación de este tipo de equipos de emergencias de seguridad cibernética, es el redactado por Agencia Europea de Seguridad de las Redes y de la Información ENISA, el cual se titula, como crear un CSIRT paso a paso, entre otros que garantizan que la información que se pueda aportar a estos centros de atención a incidentes de seguridad, sea una información confiable para sus lectores y corroborada por las experiencias de estas organizaciones con los centros ya establecidos.

Las organizaciones que son el pilar fundamental de muchos centros de atención, como lo es (First) son de gran importancia para sus miembros, ayudándoles a mejorar procesos, garantizar mejores prácticas, entre muchas otras actividades e información que les pueda compartir, contribuyendo a los diferentes pasos que se deben dar para ir dando forma a los nuevos proyectos, es por esto que se da enfoque al presente proyecto en base a todos estos referentes que se relacionan en el mismo, a lo largo del presente documento, para dar forma, se establece un título para el proyecto, así como los objetivos, tanto general y específicos, de esta manera se proporcionan los materiales necesarios para dar marcha a la documentación, dentro de las consultas realizadas a autores importantes ya mencionados, se desarrollan los diferentes capítulos del trabajo, dando inicio en el planteamiento del problema y finalizando en el desarrollo de la estructura interna del CSIRT, donde se establecen los perfiles y funciones de los integrantes del equipo, se redactan los alcances y limitaciones, en los cuales se dará forma al proyecto, los alcances establecen o indican, hasta donde se pueden mencionar dichos parámetros del equipo, ahora las limitaciones, son las que recuerdan que no se debe realizar, o las que delimitan el proyecto, dejándolo en un término especifico, según lo pactado y sin que estas tengan injerencia en los objetivos específicos. Continua el desarrollo del trabajo con el Marco de Referencia, en el cual se describen los demás marcos en cada uno de sus capítulos, resaltando el Marco

Conceptual, en el cual se describen los diferentes CSIRT que existen, desde el CSIRT militar hasta el CSIRT académico, en este marco conceptual se detallarán con una breve explicación de los principales equipos existentes en los diferentes países, otro capítulo importante es el Marco Legar, donde se describen la normatividad vigente tanto nacional como internacional, en referencia a la ciberseguridad y los diferentes delitos penales que esto conlleva.

Uno de los puntos o capítulos más significativos del presente proyecto, es el desarrollo de los objetivos específicos, los cuales se describen desde el capítulo 7, donde se establece o se indica todo lo relacionado con el plan Comercial, Misión, Visión, así como el plan estratégico del CSIRT, donde se indican detalles de los aliados que debe tener todo equipo de respuesta a incidente, aliados estratégicos que les permita tener un conocimiento mucho más amplio de la forma en que operan los demás equipos, en lo relacionado a la atención de incidentes de seguridad y los demás servicios que puedan prestar, un asunto importante que todo equipo debería tener, son las políticas que cada equipo pueda implementar internamente, las cuales describen los procesos que se pretende proteger, así como mantener los lineamientos ya establecidos, finalmente se describirá la manera como el equipo funcionará internamente, desarrollando el proceso de atención a los incidentes de seguridad, determinando el ciclo de vida de los mismos, otro punto fundamental y final es el organigrama, los perfiles y funciones, con el fin de poder establecer la manera como funcionara el CSIRT.

2 DEFINICIÓN DEL PROBLEMA

El origen de un proyecto suele surgir a partir de una necesidad" lo cual indica que se debe buscar los aspectos específicos de la necesidad del problema, pues se remonta a la seguridad informática y sus intereses a la hora de resguardar cualquier tipo de información, tanto de manera física como lógica o en la nube., es por esto que en la actualidad las organizaciones demandan servicios de seguridad informática, los cuales son requeridos desde el ciudadano de a pie, hasta las grandes compañías, todo lo relacionado tiene un propósito en común, el cual consiste en poder resguardar sus datos informáticos, y que estos permanezcan de manera segura, en el lugar que se definió para su disponibilidad[10]. Evidenciando los grandes desafíos de las industrias por producir más y facturar grandes cantidades de dinero, en ocasiones olvidan un factor importante en sus organizaciones, el tema informático, siendo de gran importancia, sin importar el formato que estén manejando, produciendo o reproduciendo, estos pueden definirse en papel impreso, digital, audios, videos etc. Las organizaciones por lo general poseen una gran cantidad de información, la cual corresponde a datos confidenciales que solo ellas desean tener acceso y conservar hasta que se determine lo contrario, mediante el ciclo de vida de la información, según sus políticas de seguridad informática, la información siempre jugará un papel muy importante en las compañías, esta se puede trasmitir, de manera digital, impresa, por correo electrónico, en video y otros tantos medios de almacenamiento y reproducción[11].

Es por ello que la seguridad de la información tiene un papel sumamente importante en cualquier tipo de organización, retomando lo anteriormente dicho, es fundamental pues permite y ayuda a la mitigación de los riegos, la mejora de las oportunidades, la continuidad del negocio entre otras posibilidades que ofrecen los sistemas de información cuidados y ordenados, es por esto que las organizaciones han entendido que se requiere de políticas de seguridad que les ayuden a mantener sus negocios estables, con mecanismos de protección confiables y personal especializado que les pueda ayudar en las fallas que se puedan presentar en el día a día, tal como pretende hacerlo Cibersecurity de Colombia LTDA. Toda organización busca que sus sistemas, siempre estén trabajando de la mejor manera y que la información que estos manejan este segura y disponible para cuando se

[10] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD (Colombia) Gerencia de Proyectos Informáticos – 204030, definición del problema [En Línea] [Consulta: 12 febrero 2020] P. 1 Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/5586/DefProblema.pdf?sequence=1

[11] MURQUINCHO PUMA Diego Eduardo, Propuesta para la creación de un comité de respuestas ante incidentes de seguridad informática (CSIRT), en el ámbito de la educación superior. Caso de estudio Universidad Nacional de Loja Ecuador. 10 diciembre 2018 [En línea] Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables [Consulta: 12 febrero de 2019] P. 4-25. Disponible en: https://www.studocu.com/ec/document/universidad-nacional-de-loja/seguridad-de-la-informacion/resumenes/articulo-revision-sistematica-csirt/4027803/view

requiera, acá es donde se deben reunir esfuerzos de parte de la organización, logrando mejoras que les garanticen esa estabilidad informática que buscan, un buen comienzo se daría al poder contar con un sistema de defensa bien estructurado, adquiriendo servicios cibernéticos, como el que les ofrecerá el CSIRT[12].

La importancia de seguridad, en los sistemas informáticos siempre estará latente, un sistema nunca podrá predecir en qué momento será víctima de un ataque informático, los sistemas tradicionales de seguridad no son suficientes para las amenazas que se ven en la actualidad, los ataques son mucho más sofisticados, por lo que las defensas tradicionales solo podrán repelerlos y en ocasiones retenerlos por algún periodo de tiempo, las compañías deben enforcarse en garantizar que sus sistemas de información, tengan un considerable grado de seguridad, implementando políticas de seguridad, invirtiendo en infraestructuras más robustas y estables, esto tampoco garantiza que se vuelvan inmunes a un ataque informático, lo que se pretende obtener es un mayor grado de seguridad o respuesta a estos ataques que puedan ocurrir y en caso de que lo sean, se busca es reducir el impacto en los daños, logrando que estos sean lo más mínimos posibles, con lo anterior se da a entender que se puede garantizar cierto grado de seguridad en los sistemas, siendo una buena decisión poder contratar servicios preventivos y reactivos por parte de un CSIRT. Para atender la demanda de incidentes de seguridad que se puedan presentar, garantizando que se pueda realizar un seguimiento adecuado a estos y poder solucionarlos, de forma correcta, adicional se puede estudiar el posible origen de los ataques, garantizando que no se vuelvan a presentar en un futuro próximo, lo cual se podría realizar mediante una base de conocimiento, lo anterior es de suma importancia, para los gerentes de las compañías, si toman la decisión de apoyarse en las necesidades de políticas y sistemas de información que garanticen la continuidad del negocio en caso de un desastre informático, la empresa Cibersecurity de Colombia LTDA., ofrece un portafolio de servicios que permite estar más tranquilos en temas de seguridad, lo anterior son puntos importantes para dar a conocer la necesidad de un centro de atención a incidentes de seguridad para que las compañías medianas y pequeñas PYMES, puedan tener un poco de tranquilidad y así enfocarse mucho más en la producción de la demanda exigida del mercado que manejan, dejando la vigilancia y mejoramiento de la seguridad informática en manos de expertos.

Con la necesidad de la implementación documentada, de un centro de atención a incidentes de seguridad informática, para la empresa Cibersecurity de Colombia LTDA., se podrá mejorar la seguridad informática al interior de esta, así como en el grupo de clientes que pueda tener de manera externa, como las PYMES, pues la mediana empresa, es la más vulnerable a los ataques informáticos, los servicios

[12] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD, Óp. cit. P.3

informáticos, garantizan, mayor producción, mayor enfoque comercial, credibilidad, madures del negocio, respaldo tanto económico como productivo, confianza en sus clientes etc. Lo que se pretende indicar es que los sistemas de información en una organización sin importar su tamaño, es el motor dentro del proceso, sin dejar de lado las demás áreas, acá se busca resaltar el área de sistemas, porque, de esta dependen las demás áreas, pues se ha podido ver en oportunidades anteriores, en casos presentados en algunas organizaciones, donde los sistemas de información fallan y las demás áreas no pueden operar, como por ejemplo las ventas, es así que los sistemas de información, son de suma importancia para cualquier organización, la información anterior se relaciona con el fin de citar, la importancia de contar con servicios de atención a incidentes de seguridad de la información, como los ofrecidos por la empresa Cibersecurity de Colombia LTDA., mediante el CSIRT, los cuales van desde asesoramiento, protección, mitigación y monitoreo, de esta manera, se podrá contar con ambientes mucho más productivos que los actuales, que les permita y garantice la producción y demanda de servicios internos, para los clientes que los adquieren, evitando los factores y riegos que puedan ocasionar perdidas irreversibles, así que bajo esta necesidad es importante contar con la protección de los datos de cualquier compañía, sus activos y datos más importantes siempre deberán estar protegidos, lo cual, se puede garantizar, mediante la obtención de los servicios que prestará el CSIRT de Cibersecurity de Colombia LTDA.

2.1 ANTECEDENTES

2.1.1 Necesidad de la Seguridad. La necesidad de implementar sistemas de seguridad para los mismos sistemas de producción de una compañía, son muy importantes en cualquier organización que pretenda tener un mercado en la actualidad, para los años 80, específicamente en el año 1988 se vio por primera vez la necesidad de implementar sistemas de seguridad, que garantizaran infraestructuras de sistemas más seguras, dicho proceso se da, a raíz, de ver que se empezaron a presentar inconvenientes con la seguridad de la información, como consecuencia de la creación de un virus llamado “Morris" el cual causó daños considerables en su momento, afectando aproximadamente el 10% de los sistemas conectados a la compañía ARPANET, el antecesor de la actual Internet, es por esto que se inició con la creación del primer centro de incidentes de seguridad informática, DARPA (*Defense Advanced Research Proyects Agency*) determinó la necesidad de enfocar el problema de modo más organizado y estructurado, y patrocinó la creación del primer Equipo de Respuesta ante Incidentes, el CERT Coordination Center (CERT/CC10), ubicado en la Universidad *Carnegie Mellon*, en *Pittsburgh* (Pensilvania)[13].

[13] HARÁN Juan Manuel. WeLive Security. Malware de los años 80: recordando al virus informático Brain y al gusano Morris. Noviembre 2018.[En Línea] [Consultado: 12 mayo 2020] Disponible en: https://www.welivesecurity.com/la-es/2018/11/05/malware-anos-80-recordando-virus-informatico-brain-gusano-morris/

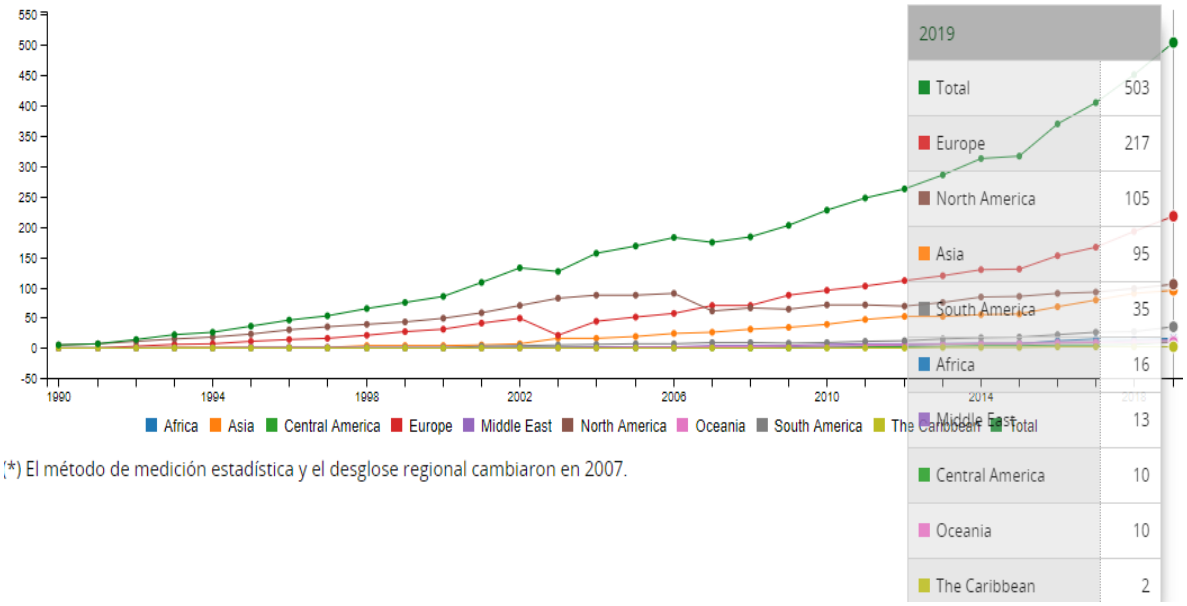
Desde la creación del primer CERT, se dio como inicio la creación de muchos centros de seguridad informática, todos bajo estas misma siglas, en distintas universidades de los estados unidos, lo cuales tenían la finalidad de publicar alertas de seguridad y amenazas de vulnerabilidades detectadas, así como un portafolio de servicios ´para ayudar al mejoramiento de la seguridad, tal como lo afirma URIBE RAYAS Edgar Felipe, en su trabajo Proceso para la Definición de Servicios Iniciales en (CSIRT) “velar por la seguridad de las redes y ordenadores, cada uno con su propio propósito, financiación, requisitos de información y grupo de clientes atendidos”[14], como consecuencia de lo anterior, se inició con la creación del CSIRT ya que se empezó hablar de la necesidad de completar el concepto de CERT, con el fin de dar un valor añadido, a los servicios preventivos y de gestión de seguridad, los cuales tuvieron importancia y en los años 90 se trasladó la idea a Europa, con el fin de que estos fueran implementados, y así continuaron creciendo en los diferentes países de Europa, pero las dificultades tampoco se hicieron esperar, tales como el idioma, la zona horaria y los estándares o convenciones internacionales, por lo que sumado a lo anterior en el año 89 un incidente de seguridad importante llamado "gusano Wank" fue el que dio inicio para crear el organismo FIRST en 1990, con el fin de que se mejorara la comunicación entre cada uno de los equipos creados hasta este entonces en el mundo[15].

En la Figura 2. Se aprecia el crecimiento que han tenido los países, registrados en él. Foro global de respuesta a incidentes y equipos de seguridad, en una línea de tiempo año tras año, es de aclarar que dicha información observada en la imagen esta actualizada hasta el año 2019 con un total de (503) equipos, sin embargo, para este año 2020 ya se cuenta con 527 equipos (CSIRTs) registrados en 96 países, siendo esta la última actualización realizada por First.

[14] URIBE, Óp. cit. P.23

[15] FIRST. Foro global de respuesta a incidentes y equipos de seguridad. Primera Historia. [Sitio Web] Estados Unidos de América: [Consulta: 12 octubre de 2019] Disponible en: https://www.first.org/about/history

Figura 2. Crecimiento de miembros por año



Fuente: FIRST. Foro global de respuesta a incidentes y equipos de seguridad. Primera Historia. [En línea] Estados Unidos de América: [Consulta: 12 octubre de 2019] Disponible en: https://www.first.org/about/history

2.1.2 Los CSIRT en América Latina. Se dice que uno de los primeros CSIRTs en América Latina fue creado en México, el cual fue nombrado Mx- CERT denominado como él (Equipo de Respuesta a Emergencias Informáticas de México). Denominado como iniciativa por el "Instituto Tecnológico y de Estudios Superiores de Monterrey", el cual se dice que ya no está en funcionamiento, en la actualidad se nombra como el primer "Csirt de latino América el "BA-Csirt", centro de ciberseguridad de Argentina, indica su director Gustavo Lineares, que el centro de ciberseguridad aborda desde los peligros más comunes en redes sociales hasta el secuestro de información (*Ransomware*) para informar a la población argentina"[16].

Así mismo los equipos con los que cuentan los diferentes países vecinos en la región de latino América, se realizará una pequeña descripción de los más importantes en cada país, los cuales han sido la guía para los demás que se han creado, dentro de los mismos países, igualmente para fortalecer las cooperaciones en ciberdefensa de la región latinoamericana, luchando día a día por ver fortalecidos todos los sistemas de cada país.

[16] POLÍTICA COMUNICADA. 'BA-Csirt' el primer centro de ciberseguridad en América Latina. [En línea] [Consulta: 12 octubre 2019] Disponible en: https://politicacomunicada.com/ba-csirt-el-primer-centro-de-ciberseguridad-en-america-latina/

2.1.2.1 Brasil CERT.br. Equipo Nacional de Respuesta a Emergencias Informáticas de Brasil, el CERT.br es responsable de manejar los informes de incidentes de seguridad informática y la actividad relacionada con las redes brasileñas conectadas a Internet[17].

2.1.2.2 Ecuador ecuCERT. Centro de respuesta a incidentes informáticos del Ecuador, este centro brinda sus servicios a todo el país, enfocándose en operadores de redes de telecomunicaciones, proveedores de servicios e infraestructura pública crítica del país[18].

2.1.2.3 Perú PECERT. Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional, este equipo está encargado de coordinar esfuerzos para resolver, anticipar y enfrentar todos y cada uno de los incidentes informáticos, así mismo de liderar la defensa ante los Ciberataques del Perú[19].

2.1.2.4 Chile CSIRT. Equipo de Respuesta ante Incidentes de Seguridad Informática, encargado de coordinar lo relacionado a incidentes de seguridad en el territorio nacional de Chile[20].

2.1.2.5 Uruguay CERTUY. Centro Nacional de Respuesta a Incidentes de Seguridad Informática, encargado de proteger y velar los intereses nacionales de ciberseguridad de la nación uruguaya[21].

2.1.2.6 Venezuela venCER. Sistema Nacional de Gestión de Incidentes Telemáticos de la República, su página oficial “http://www.vencert.gob.ve/”se encuentra fuera de servicio, por lo que se presume que no esté en funcionamiento en la actualidad.

[17] CERT.BR. Equipo Nacional de Respuesta a Emergencias Informáticas de Brasil. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en: https://www.cert.br/
[18] ECUCER. (Ecuador). Centro de Respuesta a Incidentes Informáticos. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en: https://www.ecucert.gob.ec/
[19] PECERT. (Perú) Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional. [Sitio Web] [Consulta: 12 de abril de 2020] Disponible en Internet: https://www.pecert.gob.pe/
[20] CSIRT. (Chile). El Equipo de Respuesta ante Incidentes de Seguridad Informática. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en Internet: https://www.csirt.gob.cl/
[21] CERTUY (Uruguay). Centro Nacional de Respuesta a Incidentes de Seguridad Informática. [Sitio Web] [consulta: 12 de abril 2020] Disponible en Internet: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/

2.1.2.7 Argentina CSIRT. Centro Nacional de Respuesta a Incidentes de Seguridad Informática, Es el equipo que brinda respuesta a todos y cada uno de los incidentes de seguridad informática en la nación, conformado por las fuerzas federales del estado. El CSIRT opera las 24/7 los 365 días del año[22].

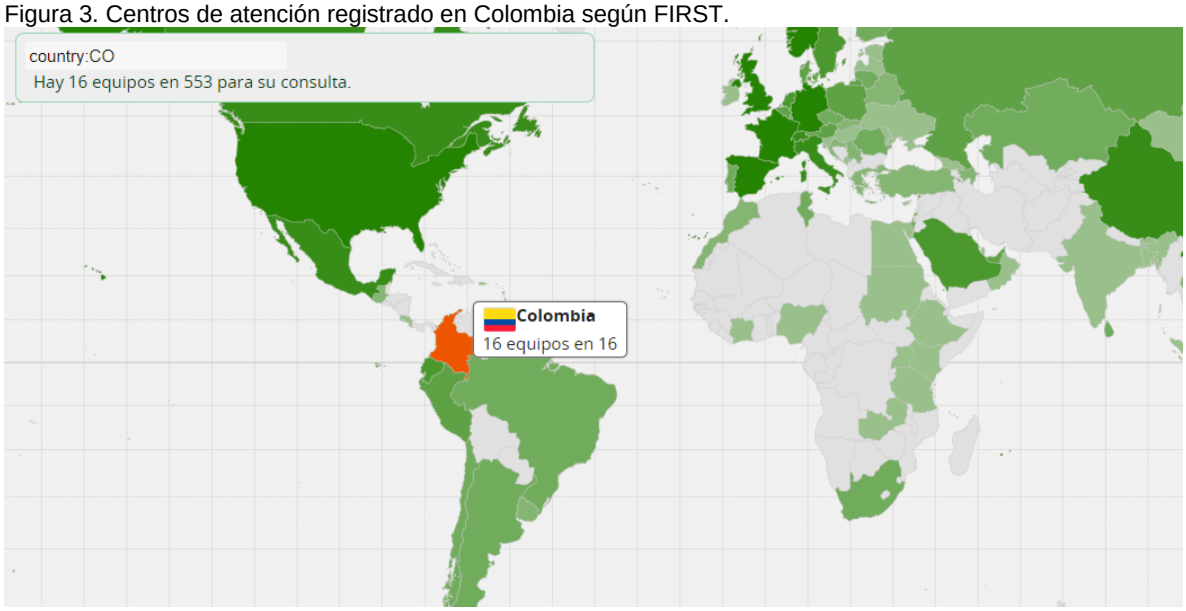
2.1.2.8 Colombia colCER. Grupo de Respuesta a Emergencias Cibernéticas, este tiene como su principal compromiso la gestión de todo lo relacionado con Ciberseguridad y Ciberdefensa en todo el territorio nacional, Su propósito será la coordinación de todas y cada una de las acciones necesarias, que conlleven a la protección en general de la infraestructura crítica, con relación a las emergencias de ciberseguridad, dentro del territorio nacional[23].

Como se mencionó anteriormente, se relacionan los países en América Latina con los CSIRTs principales en cada país, pero si lo tomamos de manera local en Colombia, se cuenta con varios de estos, muchos son del sector privado, como las empresas de telecomunicaciones, sector bancario, otros de soporte, los cuales tienen su grupo de clientes de diferentes sectores, tanto públicos como privados, se tienen del sector militar y de gobierno, con el fin de tener un concepto más claro de los centros de atención a incidentes de ciberseguridad, se nombrarán los que se encuentran actualmente registrados como miembros de (First) para Colombia[24].

En la Figura 3. Se observa la posición que ocupa Colombia dentro del (Foro global de respuesta a incidentes y equipos de seguridad de Estados Unidos de América) donde el país tiene un total de (16) CSIRT o Grupos de respuesta a incidentes de ciberseguridad, registrados en “FIRST” por parte de Colombia, de los cuales se dará una pequeña descripción uno a uno.

[22] CSIRT. (Argentina). Centro Nacional de Respuesta a Incidentes de Seguridad Informática. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en Internet: https://www.ba-csirt.gob.ar/
[23] colCERT. (Colombia). Grupo de Respuesta a Emergencias Cibernéticas. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en Internet: http://www.colcert.gov.co/
[24] FIRST. Op. cit.

Figura 3. Centros de atención registrado en Colombia según FIRST.



Fuente: FIRST. Foro global de respuesta a incidentes y equipos de seguridad. [En línea] Estados Unidos de América: [Citado en 12 octubre de 2019] Disponible en: https://www.first.org/members/map#country%3ACO

2.1.2.9 CSIRT - B-SECURE. Fundado el 17-06-2013, El centro de operaciones de B-SECURE, se caracteriza por su atención 24/7, al sector público y privado, en diferentes departamentos del país, cuenta con un equipo de expertos en relación con su producto, los cuales prestan, los servicios de prevención, así como (pruebas de seguridad), dentro de su portafolio de servicio cuentan con servicios de (monitoreo y descubrimiento de amenazas) entre otros como lo es la respuesta (gestión, contención y recuperación efectiva)[25].

2.1.2.10 CSIRT C-DOC. Fundado el 30-10-2014, el Centro de operaciones de defensa cibernética Cybershield, este, ofrece una gama de servicios para protección digital que abarca desde evaluaciones hasta implementación de soluciones, cuenta con una serie de clientes en diferentes partes del mundo en distintos continentes[26].

[25] B-SECURE (Colombia). Pasión por la seguridad. [En Línea] [Consulta: 12 abril de 2020] Disponible en: https://www.b-secure.co/

[26] CYBERSHIELD. (Colombia). Asegurando el mundo un Byte a la vez. [Sitio Web] [Consulta: 12 abril 2020] Disponible en: https://www.cybershield-us.com/

2.1.2.11 CSIRT Olimpia. Fecha de fundación 01-01-2012, sus clientes están en el mercado digital, sector público y privado, más específicamente a pequeñas, medianas y grandes empresas, ofrece servicios de tecnologías para la protección de la información, cuenta con aliados en diferentes partes del mundo[27].

2.1.2.12 CSIRT-CCIT. Fecha de fundación 01-01-2009 el Equipo de respuesta a incidentes de seguridad informática de la Cámara Colombiana de Informática y Telecomunicaciones, presta sus servicios a compañías tanto del sector privado como público, realiza colaboraciones con sectores militares, como Policía Nacional y Ejército Nacional, con el fin de cooperar contra el crimen organizado en el ciber espacio[28].

2.1.2.13 CSIRT-ETB. Fecha de fundación 2010-11-12 del Equipo de Respuesta a Incidentes de Seguridad Informática, Empresa de Telecomunicaciones de Bogotá SA ESP – ETB, este equipo, pertenece a la empresa de telecomunicaciones de la administración de la ciudad de Bogotá, la cual cubre los servicios de su infraestructura de servicios corporativos a nivel nacional, donde tiene clientes de todo tipo, desde líneas ADSL de tiendas de barrio hasta canales de internet dedicado y datos, de grandes clientes, como Terpel, Davivienda; universidades, Policía Nacional, alcaldías y gobernaciones, etc.[29].

[27] OLIMPIA. (Colombia). Plataformas para la transformación digital. [Sitio Web] [Consulta: 12 abril 2020] Disponible en: https://www.olimpiait.com/

[28] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. (Colombia). [Sitio Web] [Consulta: 12 abril 2020] Disponible en: https://www.ccit.org.co/

[29] EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ SA ESP – ETB. Equipo de Respuesta a Incidentes de Seguridad Informática. [Sitio Web] Csirt-Etb. [Consulta: 12 abril de 2020] Disponible en: https://etb.com/inicio.aspx

2.1.2.14 CSIRT PONAL. Fecha de fundación 2011-01-01, el CSIRT, también conocido como el centro cibernético policial, cuenta con una variedad de opciones disponibles para todo el mundo, desde análisis de Malware, Apps que te ayudan a proteger tu información, denuncias en línea, reportes de ataques informáticos, boletines informáticos, etc. Dispone de una variedad de opciones disponibles para el público en general, así mismo está en temas de ciberseguridad, apoya a diferentes organizaciones, del país, sin importar su ubicación, como su afinidad bien sea pública o privada, es un sitio web con una buena estructura digital, disponible para cualquier ciudadano, de modo que se puede realizar, desde consultas hasta verificación de información como consulta de sitios web sospechosos, es de aclarar que los servicios prestados por este grupo de uniformados, solo se presta en Colombia, pero cuenta con el apoyo de otras organizaciones de ciberseguridad a nivel mundial,[30].

2.1.2.15 CSIRT Digi. Fecha de fundación 2011-04-01 el Equipo de respuesta a incidentes de seguridad informática de DigiSOC Digiware, este centro de atención a incidentes de seguridad cibernética y digital presta servicios a un grupo de clientes en América latina, tiene centros de operaciones de seguridad en Bogotá, Medellín, Lima y Miami. Trabajan 7 x 24 x 365, lo que garantiza una protección global y completa de cualquier organización, dentro de sus servicios se pueden resaltar, (detención y respuesta gestionada, servicios de seguridad gestionados, digital exposición, nube y seguridad) servicios que pueden ser adquiridos a través de su sitio web[31].

2.1.2.16 CSIRT ETEK. Fecha de fundación 2005-01-01 CSIRT de ETEK, tiene como principal responsabilidad, garantizar la correcta atención de todos incidentes de ciberseguridad, tanto para los usuarios internos y externos de ETEK, así como los clientes que deseen del portafolio de servicios que ofrece, adicionalmente cuenta con una coordinación de respuesta ante los incidentes de ciberseguridad externa[32].

[30] POLICÍA NACIONAL DE COLOMBIA. Csirt Ponal Equipo de Respuesta de Seguridad Informática Incidentes de la Policía Nacional de Colombia. [Sitio Web] Centro cibernético policial. [Consulta: 12 abril de 2020] Disponible en: https://cc-csirt.policia.gov.co/

[31] DIGIWARE. Equipo de respuesta a incidentes de seguridad informática de DigiSOC. [Sitio Web] Colombia. [Consulta: 12 abril de 2020] Disponible en: http://www.digiware.net

[32] ETEK INTERNATIONAL. (Colombia) Equipo de respuesta a incidentes de seguridad informática de ETEK International. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: www.etek.com.co

2.1.2.17 CSIRT ITSSOC. Fecha de fundación 01-01-2015 el equipo de Servicios de seguridad de TI SAS ITSSOC-CSIRT, funciona principalmente como un punto focal de seguridad de la información y servicios de ciberseguridad, donde ofrece un portafolio de servicios a sus clientes, en los cuales, podemos encontrar los siguientes, (Centro de operaciones de seguridad, seguridad en tecnologías disruptivas, Gobierno, riegos y complimiento y Payment card industry data security standard) con un alto nivel de personalización siendo estos destinados en beneficio de las partes internas y externas. El pilar fundamental son sus clientes, provenientes de una amplia gama de sectores privados y públicos, principalmente del sector financiero y de seguros; Además, con el objetivo de mejorar constantemente las ofertas de la organización matriz, el CSIRT también es un proveedor de seguridad de su organización anfitriona[33].

2.1.2.18 CSIRT ShieldNow. Fecha de fundación 2016-11-12, este centro de atención a incidentes de seguridad tiene sus sedes en Colombia y estados unidos, La circunscripción de ShieldNow se compone de todos los elementos del sistema de información de O4IT (usuarios, sistemas y redes), presta sus servicios a diferentes sectores, tanto públicos como privados[34].

2.1.2.19 SOC Claro Colombia. Fecha de fundación 2011-07-11, este equipo conforma el Centro de Operaciones de Seguridad Equipo Claro Colombia, este completo centro de atención a incidentes ofrece una amplia gama de servicios avanzados, en el sector de las telecomunicaciones especialmente, donde se incluyen servicios relacionados con voz, datos, video, entre otros que tiene que ver con el acceso a Internet y las soluciones integradas para clientes en las pequeñas y medianas empresas, gracias a su capacidad en cobertura por sus redes de acceso y trasporte en todo el territorio nacional, Además cuenta con una expansión en operaciones en LATAM incluida Colombia[35].

[33] ITSSOC-CSIRT servicios de seguridad de ti Sas Soc Csirt, Equipo de Servicios de seguridad de TI SAS ITSSOC-CSIRT. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: https://www.itsecurityservices.com.co/
[34] SHIELDNOW. Equipo de respuesta a incidentes de seguridad. Colombia. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: https://shieldnow.co/
[35] CLARO Colombia. Centro de Operaciones de Seguridad Equipo Claro. SOC. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: http://www.claro.com.co

2.1.2.20 SOC-CCOC. Fecha de fundación 2012-10-30, el Centro de operaciones de seguridad - Comando de operaciones cibernéticas conjuntas, El SOC-CCOC es un sofisticado centro de atención en ciberseguridad, el cual proporciona gestión de incidentes en seguridad y de la información, en especial para las Fuerzas Armadas de Colombia y los propietarios y/u operadores de infraestructura crítica en Colombia, estos servicios son prestados bajo la modalidad del horario 7x8 lo cual es muy necesario para adherirse a los acuerdos con el CCOC[36].

Adicional, es importante resaltar que se cuentan con otros centros de atención a incidentes informáticos en Colombia, los cuales no están registrados en First, estos corresponden tanto al sector, privado, público y de gobierno, Colombia lidera en América latina el sector de ciberseguridad según informa First, ya que cuenta con un total de (16) centros registrados, sin contar los que aún no realizan su registro, en comparación con los demás países de América latina, Colombia está muy bien posicionado, si se realizara la comparación con el segundo en la lista, Ecuador tiene (7), en tercer lugar lo ocupa Perú con (5) y el cuarto lugar es para Brasil, Argentina y Chile con (4) cada uno, el quinto y último lugar es para Uruguay con tan solo (2), en comparación con los demás países del planeta Colombia también está bien Referenciado, Pues si se compara con el primero en la lista que es Estados Unidos de América, tiene un total de (99) registrados, el segundo es japón con un total de (39), el tercer lugar es para España con un total de (37) registrados y el cuarto lugar seria para Alemania con un total de (30) registrados, el 5 lugar es para el Reino unido, con un total de (18) registrados, si realizamos un comparativo internacional, Colombia está dentro de los primeros 10 países con mejor sistema de defensa ante incidentes de seguridad, donde ocuparía el puesto número 6, compartido con países como Noruega y Francia, también se puede decir que esta, mejor posicionado que países como Rusia, china y Canadá entre otros, es de aclarar que estos números solo se refieren a los registrado por First, pues los países pueden tener muchos más CSIRTs solo que no están registrados, en el Foro global de respuesta a incidentes y equipos de seguridad[37].

Para resaltar Colombia cuenta con un Csirt Financiero. El cual presta sus servicios al sector Bancario y está bajo el control de Asobancaria, es uno de los centros que aún no se encuentran registrados en el Foro global de respuesta a incidentes y equipos de seguridad First, este está encargado de atender los incidentes, amenazas, riesgos, vulnerabilidades, del sector financiero, este centro de atención

[36] COMANDO CONJUNTO CIBERNÉTICO (Colombia) Centro de operaciones de seguridad - Comando de operaciones cibernéticas conjuntas. SOC-CCOC. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: https://www.ccoc.mil.co/

[37] FIRST. Óp. cit.

a incidentes pertenece al sector Privado, ya que únicamente está enfocado en la protección comercial y operativa de Asobancaria[38].

2.2 PLANTEAMIENTO DEL PROBLEMA

Basados en las ideas y sugerencias del profesor Fabián Coelho, licenciado en letras de la universidad de los andes, en su artículo, Significado de Planteamiento del problema, se parte de la idea del estudio documental de un CSIRT, para la empresa Cibersecurity de Colombia LTDA., donde se ve y surge la necesidad, de tener en cuenta la seguridad de la compañía en cuanto a infraestructura, datos, sistemas, y recursos humanos, siendo estos parte esencial de los datos sensibles que se manejan diariamente en las diferentes empresas sin importar su tamaño. Por lo que su importancia es muy relevante, si se ve como punto de partida para las instituciones, teniendo en cuenta que les permite tener una referencia desde el pasado al futuro, esto les garantizará tener un concepto más claro referente al tema de la seguridad de la información, es decir, al momento de realizar análisis de los incidentes que se encuentran activamente involucrados en temas relacionados con seguridad informática, por lo que siempre pueden ser un riesgo para cualquier compañía., razón por la cual cada una de las operaciones en pro de la mitigación de los riegos internos, deberían ser mucho más habituales en una organización[39], la protección de incidentes de seguridad genera un gran impacto en las compañías medianas y pequeñas, y cualquier otra compañía, pero específicamente en las dos primeras, siendo que estos atacan directamente al activo que se considera más importante para las organizaciones, generado grandes pérdidas económicas a las mismas, según se indica en el documento: La guía de gestión y clasificación de incidentes de seguridad informática, del ministerio de las telecomunicaciones Mintic, este tipo de incidentes tienen una gran influencia en los diferentes propósitos u objetivos que desee una compañía, en otras palabras esto afecta directamente su reputación y buen nombre en el mercado al que esté compitiendo, dado que también se pueden ver involucrados en aspectos legales, por esta razón este tipo de incidentes de gran impacto y otros, deben ser atendidos con la mayor brevedad posible antes de que sea demasiado tarde y se deba llegar a lamentaciones por perdidas incalculables, una buena manera de poder enfrentar la problemática, es contratando servicios de seguridad eficientes[40].

---

[38]ASOBANCARIA. Csirt Financiero un Enfoque Colaborativo a la Ciberseguridad. [Sitio Web Colombia: [Consulta: 12 octubre de 2019] Disponible en: https://www.asobancaria.com/csirt/

[39]COELHO Fabián Significado de Planteamiento del problema, Ciencia y Salud, Universidad de los Andes, Bogotá D.C. [Sitio Web] Blog Significados.com [Consulta: 12 abril 2020] Disponible en: https://www.significados.com/planteamiento-del-problema/

[40]COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. boletín trimestral de las TIC, cifra tercer trimestre del 2019. [Sitio Web] Bogotá D.C. Colombia enero 2020. [Consulta 12 octubre de 2020] P.9-50 Disponible en: https://colombiatic.mintic.gov.co/679/w3-article-125648.html

Según se afirma en el documento Impacto de los incidentes de seguridad digital, en Colombia 2017, por la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y el Ministerio de Tecnologías de la Información y Comunicaciones, se ha logrado demostrar una gran acogida y amplia creciente en lo que se refiere a telecomunicaciones y tecnología de la información (TIC)" como se afirma en la página 48 del documento, aproximadamente el 60% y 70% de las medianas y pequeñas empresas, indicaron que nunca habían identificado un incidente de seguridad, lo cual debe preocupar al sector, pues se podría diferir que muchas de estas compañías posiblemente no lograron identificar un ataque informático, debido a que su infraestructura tecnológica, no cuenta con las herramientas y personal capacitado para poder identificar dichas amenazas que se pudieron presentar, así mismo el 51% de las grandes compañías, indicaron que si han identificado incidentes de seguridad, lo cual daría a conocer que estas compañías si cuentan con las herramientas, infraestructura tecnológica y recursos para poder hacer frente a los ataques informáticos que se puedan presentar en el presente y futuro, habría que decir también, que en la actualidad tenemos un país conectados a la red de redes Internet, las 24 horas, los 7 días a la semana y los 365 días al año, en su gran mayoría las horas de conexión son para pasar tiempo en redes sociales, en segunda medida se realizan consultas de trabajo y personales, según el boletín trimestral de las TIC, cifra tercer trimestre del 2019, "Colombia tuvo, un incremento a internet fijo de 7.0 millones de accesos a internet, fue un porcentaje mayor en comparación con el mismo trimestre del año anterior, donde se alcanzó un porcentaje de 6.7 millones de accesos a internet"[41], cifras que dan a conocer que los colombianos viven cada día más conectados a internet, lo anterior se entiende que, así como se detectan cada vez más conexiones, también aumentan los números de posibilidades de que las empresas, usuarios y demás navegantes, puedan estar más expuestas y expuestos a un ataque informático, como se ha dicho, es importante que las compañías en especial las medianas y pequeñas PYMES, inviertan en sus infraestructuras tecnológicas y recursos humanos especializados con el fin de poder mitigar los ataques que puedan sufrir en un futuro. siendo de gran ayuda, la oferta de servicios del CSIRT, pues dentro de su portafolio podrán encontrar variedad de servicios de prevención, monitoreo y capacitación, siendo estos una excelente fuente de cooperación interna para mitigar los incidentes de seguridad que las conexiones a internet les pueda generar, así como poder capacitar al talento humano en todas y cada de las áreas de estas compañías, dándoles a entender la gran responsabilidad que tienen al conectarse a internet, para realizar las actividades de su trabajo, como también las que se consideran personales[42].

[41] Ibid., P. 9.
[42] ESTADOS UNIDOS. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. BANCO INTERAMERICANO DE DESARROLLO y COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Impacto de los incidentes de seguridad digital en Colombia 2017. [En línea] Colombia, 2017. [Consultado: 12 diciembre 2019] P. 48-130 Disponible en: https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf

La compañía a la cual se dirige este proyecto Cibersecurity de Colombia LTDA y las (Pymes), deben tener claro que los ataques de delincuentes informáticos y la tendencia a estos ataques están en exponencial aumento, pues para tener protegido los activos de información que se tienen, es necesario contar con herramientas que puedan ayudar a gestionar los incidentes informáticos que se generen y poder estar al día en la atención de las vulnerabilidades presentadas y que estas puedan ser explotadas por algún delincuente informático, según indican la Policía Nacional, Cámara Colombiana de Informática e Impacto tic, en el informe tendencias de cibercrimen en Colombia 2019 – 2020 "La dinámica actual del Cibercrimen en Colombia refleja un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades, a través de los canales de atención a empresas y ciudadanos, en el ecosistema de ciberseguridad dispuesto por la Policía Nacional fueron registrados 28.827 casos en total, durante el 2019. indicando que estos casos en su mayoría fueron reportados y tipificados en la Ley 1273 del 2009"[43], se informa que los casos reportados corresponden al 54% de las denuncias realizadas durante este periodo de tiempo, este tipo de estadísticas son muy importantes con el fin de tener datos más concretos, frente a lo que sucede en el país en temas de ciberseguridad con las empresas, en especial a las que va enfocado el portafolio de servicios que se estará ofreciendo por el CSIRT, es evidente que en los sectores más golpeados obedece a que sus infraestructuras tecnológicas no cuentan con las medidas y herramientas necesarias de protección que deberían tener, para poder avanzar en la maduración y crecimiento en producción y la seguridad de los activos de la misma, garantizándole una mejor estabilidad, razón por la que se debe tener presente la adquisición de servicios de seguridad informática que les proteja[44].

En relación las Pymes el 44% de la fuerza laboral está en este sector, tal como se afirma en el estudio "Impacto de los incidentes de seguridad digital en Colombia 2017" producido por la Organización de los Estados Americanos. Banco Interamericano de Desarrollo y Colombia. Ministerio de Tecnologías de la Información y Comunicaciones[45], siendo uno de los sectores productivos más grandes del país, pues también son el sector más afectado por los ataques cibernéticos, así como también lo es, el sector bancario, este es uno de los sectores preferidos por los delincuentes informáticos, siendo este el lugar donde pueden obtener dinero con mayor facilidad y con más éxito en los ataques realizados,

[43] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. Bogotá D.C. (enero 5 de 2009) Diario Oficial. [En Línea] [Consultado: 12 de marzo de 2020] P. 1-4. Disponible en. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[44] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES, POLICÍA NACIONAL DE COLOMBIA Y IMPACTOTIC. Op. cit., P. 7.

[45] ESTADOS UNIDOS. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. BANCO INTERAMERICANO DE DESARROLLO y COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Op. cit., P. 34.

Colombia tiene importantes retos en la atención de incidentes de seguridad, el sector bancario, es uno de los preferidos por los ciberdelincuentes, se afirma que los ataques año tras año son más severos, lo que invita al sector a mejorar sus defensas informáticas, en especial las pequeñas sucursales y cooperativas, siendo estas las más desprotegidas, pues no cuentan con los mismos sistemas de defensa ante un posible ataque informático como el que pueda tener. P. ej., el grupo (AVAL), el Comando Conjunto Cibernético – CCOC[46], es el encargado de la Defensa para la Infraestructura Crítica Cibernética de Colombia, este equipo resalta la importancia de poder contar, con sistemas de protección de infraestructura crítica, mediante el apoyo de grupos como el Comando Conjunto Cibernético, les permite fortalecer criterios de protección y necesidades, frente a la creciente demanda de servicios de seguridad informática, en especial las compañías más vulnerables, estos sectores requieren del apoyo de una compañía como la empresa Cibersecurity de Colombia LTDA. mediante el CSIRT, que les ayude a poder enfocarse en la solución de sus problemas de seguridad informática internos, los esfuerzos estarán encaminados en la protección de los incidentes de seguridad, de todos los sectores, de las Pymes, en especial el sector privado, siendo este el que requiere y demanda más servicios de seguridad, enfocado mediante un plan comercial adaptable a cada cliente, de esta manera se logrará llegar a cada uno de ellos, con el fin de que se avance en materia, siendo este un punto importante para determinar esfuerzos y así poder llegar a sectores que posiblemente no tengan la información necesaria o pertinente sobre el tema de ciberseguridad, lo cual sería muy importante, si se tiene en cuenta que todos los sectores se beneficiarían de una u otra manera, dicho lo anterior, se lograría establecer mejoras importantes en relación con la seguridad de la información en las compañías que deseen los servicios del CSIRT.

Los servicios informáticos cada día, son más deseados por las compañías que pretendan incursionar en un mercado competitivo, los empleados de cualquier empresa se enfocan principalmente en sus funciones, las cuales pueden ser las ventas, la fabricación, el trasporte etc. Con lo anterior se entiende que solo un pequeño grupo de personas están pensando en la seguridad de la información, esto podría corresponder a un 10%, el 90% restante solo realizar las actividades encomendadas, dejando de lado la forma en como procesa la información que llega a sus manos y la protección que le da a la misma, deponiendo, que no es de su competencia o no está dentro de sus funciones realizar tal vez un Backup, como también, ver la manera en que la comparte con personas ajenas a su área o que tal vez no pertenecen a la compañía, se podría indicar, que este es el punto de partida, en un proceso de protección de activos informáticos, donde inicialmente toda compañía debe contar con políticas de protección de la información, con el fin de comprometer a todos y cada uno de los empleados en generar un hábito de

[46] COLOMBIA. COMANDO GENERAL DE LAS FUERZAS MILITARES - COMANDO CONJUNTO CIBERNÉTICO. Op. cit.,

apropiación y protección de los datos que puedan generar o que lleguen a sus manos, en función de sus actividades diarias, priorizando en que la información no debe ser personal, sino que pertenece a la compañía y que de esta manera la debe mantener bajo llave y segura hasta su reporte al lugar encomendado según las políticas pactadas por la organización. En relación con los párrafos anteriores, esto le permitiría a una organización, solo ocuparse de los problema externos ya que mediante una correcta educación, correspondiente a temas de seguridad informática todos y cada uno de sus empleados, puede mitigar hasta un 60% de los errores que comúnmente se comenten y que estos llevan a generar vulnerabilidades que luego se convierten en incidentes de seguridad, uno de los servicios que podría adquirir una empresa por parte de un CSIRT, seria servicios de asesoramiento en manejo de información a sus empleados o usuarios internos, mediante capacitaciones y charlas que les permitan comprender lo importante que es mantener los archivos bajo llave, tanto los físicos como los digitales, esto le permite a cualquier compañía ahorrase mucho dinero en la atención de incidentes de seguridad internos.

Las Pymes en Colombia, por su alto grado de probabilidad a sufrir ataques informáticos, independiente del mercado que maneje, deben tener claro la importancia de contar con sistemas de información debidamente protegidos, adoptando medidas externas y necesarias que les garantice estar protegidos, como se ha dicho en cada uno de los párrafos anteriores, una medida esencial es la solicitud de servicios de seguridad informática que ofrece el CSIRT, la adquisición de estos servicios, les permitirá realizar procesos más eficientes, dar a sus clientes sensación de seguridad en caso de que sus ventas sean online, es importante mantener procesos que les garantizaran estar a la vanguardia de las compañías que inspiran seguridad con sus clientes y empleados, las organizaciones se deben preocupar un poco más por su propia seguridad, condicionalmente de ello depende su incursión en el mercado que estén llevando en el momento, una mala experiencia de un cliente al realizar una compra de un producto de una compañía en particular, donde la plataforma que maneje para la transacción no sea segura, generara mucha desconfianza y esto no solo le garantizará la perdida de ese cliente, toda vez que el mismo cliente no recomendara el sitio o la página a otros clientes, si no que por el contrario, dará una mala calificación bien sea en la aplicación o el portal web, garantizando así, que muchos más cliente desconfíen y decidan abandonar la compra que posiblemente estén por realizar, por situaciones como la planteada anteriormente es que muchas empresas no solo bajan su rentabilidad, si no que pueden llegar a quebrar, por no prestar atención a detalles tan importantes y más en la actualidad en que vivimos, donde los clientes prefieren realizar sus compras online y que les sean enviadas a sus casas, con el fin de evitarse el tráfico y el estrés que produce las calles de las ciudades como, P. ej.: Bogotá. Lo anterior invita a las Pymes, a que no solo vean la necesidad, si no que la lleven a la práctica, protegiendo sus sistemas de información, así como garantizando una protección adecuada de sus activos, mediante la adquisición de

servicios de seguridad informática para la atención de incidentes de seguridad de la información.

2.3 FORMULACIÓN DEL PROBLEMA

¿Cómo establecer el proceso de estudio, para la implementación documental de un centro de respuesta a incidentes CSIRT?

2.4 ALCANCE Y LIMITACIONES

2.4.1 Alcance. El presente proyecto se encuentra entre los proyectos de infraestructura tecnológica y seguridad en redes y lo que pretende es realizar el diseño documental, para la creación del centro de respuesta a Incidentes CSIRT para caso de estudio “Escenario Administrativo” Cibersecurity de Colombia LTDA., donde podemos visualizar los diferentes servicios que prestará, los sectores a los cuales estará dirigido, así mismo se diseñará el tratamiento de los incidentes de seguridad, como el seguimiento que se les debe dar a cada uno de ellos, se analizaran los perfiles ya aplicados en CSIRT que están establecidos en Colombia y en otros países, se relacionaran los perfiles necesarios del equipo de trabajo del CSIRT, así como las diferentes funciones por cada uno de ellos.

2.4.2 Limitaciones. Es conveniente resaltar que el desarrollo del proyecto no abarcará temas como los que se definen a continuación:

A. La implementación de la infraestructura tecnológica y física.

B. Software y hardware que pueda requerirse para su implementación.

C. La implementación de planes comerciales correspondientes a los servicios que prestará el CSIRT.

D. No se relacionará el costo beneficio de la implementación, como de los servicios ofertados.

E. No se realizará estructuración de planes de capacitación necesarias para el talento humano.

3 JUSTIFICACIÓN

En la actualidad la seguridad informática a nivel internacional, es de suma importancia, pues esta representa no solo un factor clave, sí no que también está en juego la reputación de la empresa en general, la integridad de los datos de información y la preservación tanto de los equipos de hardware y las herramientas informáticas utilizadas, dependen estrictamente de este factor, los servicios que se ofrecerán por la empresa Cibersecurity de Colombia LTDA., serán de gran apoyo, para sus usuarios, dichos servicios brindaran las medidas necesarias de protección y mitigación, para que ataques relacionados con lo expresado por el Centro Criptológico Nacional, quien indica que esto conlleva a ataques a escala global, como también a los dirigidos y preparados, a los cuales se les dedico gran tiempo, con el fin de que las víctimas sean las adecuadas, es decir ataques más personalizados, complejos y sigilosos (así como son las APT, son ataques que se realizan mucho más perfeccionados, son difíciles de detectarlos, con poca probabilidad de que sea así, son muy persistentes, pues si tienen que modificar sus estrategias en pro de lograr sus objetivos lo realizar, así que tengan que hacer nuevos desarrollos con el fin de volver sus ataques mucho más efectivos en caso de que las víctimas ya fijadas se resistan, es importante indicar que muy seguramente para este tipo de ataques, los sistemas convencionales de protección de las compañías, los que se destacan como, detección de vulnerabilidades y antivirus de protección, no sean suficientes para detener este tipo de ataque APT, el cual tiene su preparación y organización con una dedicación determinada, para que sea efectivo, en relación con lo anterior se puede indicar que el auge de las redes de telecomunicaciones, junto con el surgimiento de las múltiples plataformas tecnológicas que a diario se están implementando, así como los distintos proyectos de interconexión que se generan, estos elementos mencionados, logran establecer conexiones múltiples, que favorecen a toda una comunidad en general, tanto empresarial, sectorial y del común, si bien esta, ayuda enormemente al favorecimiento en todo el ámbito comercial, desde los desarrollos y lo operativo, lo cual es de suma importancia, pues brinda, una mejora en la producción de las empresas, se debe decir que, igualmente favorece al surgimiento de nuevas amenazas, dado que, conforme se ve crecer los negocios y la utilización de conexiones a internet, igualmente se ve con el incremento de los ataques cibernéticos[47].

Los procesos que se han mencionado, son de gran importancia para la seguridad de las empresas en general, pues estas siempre van a requerir de servicios de seguridad informática, es por esto que mediante el desarrollo de dicho proyecto con

[47] CENTRO CRIPTOLÓGICO NACIONAL. (España). Principios y recomendaciones básicas en Ciberseguridad [En línea] (CCN-CERT BP/01) octubre 2017, [Consultado: 12 diciembre de 2019] P. 6-28 Disponible en: https://www.ucm.es/data/cont/media/www/pag-114974/CCN-CERT_BP_01.pdf

la empresa Cibersecurity de Colombia LTDA., los usuarios internos y las empresas externas que requieran de estos, los podrán solicitar, adquiriendo con ellos, seguridad de sus sistemas de información y los activos más importantes para estas empresas, dichos servicios iniciales que se podrán prestar, serán muy importantes para los clientes, dentro de los servicios ofertados se podrán encontrar tales, como lo son, el tema de asesoramiento en cuanto a seguridad de la información en general, mediante estos servicios que ofrecerá la empresa Cibersecurity de Colombia LTDA., con la implementación del CSIRT, se podrán desarrollar planes de asesoramiento y campañas que ayuden a la generación de medidas de seguridad de la información, como lo indica la Agencia Europea de Seguridad de las Redes y de la Información, en el documento como crear un CSIRT paso a paso, "un CSIRT puede asesorar y orientar sobre las mejores prácticas de seguridad aplicables en las operaciones comerciales del grupo de clientes atendido", de esta manera se daría inicio, al proceso de oferta de los servicios que ofrecerá el CSIRT, pues inicialmente debe brindar a los clientes un asesoramiento en cuanto a la seguridad de su infraestructura y el proceso que se debe seguir, para lograr corregir dichos inconvenientes que se estén presentando dentro de la misma, como lo pueden ser vulnerabilidades, fallas del software y hardware, como los demás aspectos de seguridad que puedan tener, dicho de otra manera, con el fin de erradicar, disminuir el impacto que estos generan en la organización, estos servicios por lo general intervienen en la operación, mediante recomendación, identificación, de cada uno de los requisitos y necesidades de la compañía, así como en recomendaciones de instalación o protección de los nuevos sistemas que la compañía pueda adquirir, de esta manera serán más efectivos los procesos de mejora, tales como se podrían mencionar terminales de red, software, los distintos procesos de toda la empresa[48].

Un factor importante de ayuda, en los servicios que se tiene por parte de la empresa Cibersecurity de Colombia LTDA., es que, estos darán significativamente una renovación en la mejora de la seguridad informática de sus clientes y usuarios, corrigiendo los factores de riego en seguridad que puedan tener actualmente estas empresas, así mismo la optimización de sus procesos los cuales serán mucho más efectivos y rápidos, mediante la adquisición de estos servicios las empresas, ahorraran dinero adquiriendo otro tipo de medidas de protección, como antivirus y otros, es así que, los servicios del CSIRT, le permitirán a las empresas poder mantener una línea de protección y garantizar a sus clientes, en un ambiente de seguridad, donde podrán realizar sus transacciones de compras online, sin mayor preocupación, lo anterior obedece a la evolución tecnológica del ahora, donde vemos un significativo aumento en las ventas por catálogo, mediante aplicaciones y sitios web, se refiere en cuanto a seguridad de la información de clientes actuales y futuros clientes para las empresas que tienen este tipo de modalidades de ventas y adquisición de productos, estableciendo retos muy importantes para la

[48] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. Óp. cit. P. 77-78

ciberseguridad. Como respuesta a estos retos, las compañías deberán tener mejores sistemas de información, que les permita tener una competencia mucho más justa en relación a las organizaciones mejor posicionadas según su línea de negocio, de esta manera se establecerá una muy buena opción de protección con los servicios del CSIRT, los cuales tienen un objetivo principal, que consiste en repeler de manera oportuna y eficaz, a los incidentes reportados, en las organizaciones, en cuanto a este tema, los antecedentes del reporte de los mismo incidentes, manifestados por los más importantes organismos de protección de la información en el país, como lo es el, CAÍ Virtual policía nacional, el CSIRT del comando conjunto cibernético, entre otros, representados por el estado Colombiano, indican que, este tipo de ataques se podrían presentar en casi cualquier organización, como también lo podría trasmitir a sus clientes, siendo muy grave que un cliente de una empresa pueda ser víctima, por la relación que pueda tener con un proveedor, dando más claridad al tema, las empresas tienen clientes, que, condicionalmente son atendidos por la filosofía del negocio, que casi toda organización maneja, manteniendo una relación muy cercana, que en algunos casos, se mantienen interconectados por los productos y servicios que manejan, en muchas ocasiones no se toman las medidas necesarias de seguridad, lo que puede conllevar a que, este sea un punto débil de cualquier organización, por lo que, aparte de autoprotegerse también debe proteger los clientes con los cuales tiene relación directa o algún tipo de conexión por redes de internet, donde posiblemente pudieran resultar afectados en un ataque cibernético inicialmente para la compañía y no directamente para sus clientes o colaboradores, pero que, de una u otra manera resultaron afectados, con el ejemplo anterior, se responden a los interrogantes del porqué, de la necesidad de servicios de seguridad informática y el para que, se requieren dichos servicios que serán ofertados por el CSIRT[49].

De ahí que para eliminar o reducir la marca de estos sucesos informáticos de alto riesgo para la entereza y seguridad Informatica, es necesario un proceso que les garantice y les permita mantener los datos seguros, por esta razón, la importancia de realizar un diseño documental, por medio de la empresa Cibersecurity de Colombia LTDA., y así dar forma a un Equipo o centro de atención a incidentes de ciberseguridad (CSIRT), donde se establecerán unos procesos y definiciones de los servicios que se prestaran, como también es indispensable que el equipo de trabajo o el CSIRT, pueda tener unas políticas y procedimientos documentados, los cuales cumplan los deseos de los clientes y así satisfacer sus necesidades, brindando la protección mediante los servicios ofertados, para sus infraestructuras tecnológicas y digitales, es por esto que desde las perspectivas adyacentes al negocio, los servicios ofrecidos podrían llevar a las organizaciones a plantear una serie de escenarios, como, P ej.: la gestión de manera interna en cada una de ellas, como también la buena gestión de sus procesos misionales y los diferentes puntos

[49] URIBE, Óp. cit. P.21

de vista técnicos que les permitan crecer desde su interior, de esta manera garantizando una línea de producción más prospera, pues, si cuenta con un buen sistema de seguridad, entonces la atención a los incidentes de seguridad que se puedan generar en los procesos que desarrolla, serán mucho más fáciles y rápidos de solucionar, garantizando que no debería invertir más dinero y tiempo en buscar salvavidas, en casos de crisis de emergencias cibernéticas, punto importante para la retención y captura de nuevos clientes en sus negocios, ya que, en la actualidad, los clientes buscan compañías que garanticen seguridad y prosperidad, un cliente nunca invertiría su dinero o dejaría sus procesos en manos de una empresa que no le brinde la suficiente confianza de ello, por esta razón, es que se debe fortalecer toda operación o proceso productivo en cualquier compañía mediante medidas de seguridad, eficientes y garantizadas.

Se dice que Colombia tiene su mayor fuerza laboral en las Pymes, lo cual indica que este sector es el que más aporta al país, tanto en procesos de producción como en fuentes de empleo, es por esto que, toda pequeña y mediana empresa debería contar con una línea de defensa que le permita proteger su actividad productiva y sus activos de información, cubiertos por los servicios que prestara el CSIRT, generando grandes beneficios a las organizaciones que requieran de dichos servicios, logrando alcanzar en poco tiempo resultados tangibles, desde el primer momento, gracias a su flexibilidad se adaptaran fácilmente a los presupuestos del portafolio de servicios ofertados, los Equipos de Respuesta ante Emergencias Informáticas, han obtenido un valor muy alto, no solamente para las instituciones, si no para las compañías que requieran que se les resguarde su información, siendo así que algunos equipos pioneros de ciberseguridad y responsables de las seguridades internas en los países donde se encuentran, resaltan la importancia de adquirir servicios de seguridad informática cada día, para proteger los intereses informáticos de cada una de ellas, la seguridad en los sistemas de algunas compañías, son un concepto integral, dado que se les rinde mucha importancia a los temas relacionados con ataques informáticos, es así como también cobran mucha más importancia los Equipos de Respuesta ante Emergencias Informáticas, que dedican su tiempo y procesos en evitarlos y mitigarlos.

Para complementar, un CSIRT es muy necesario para cualquier empresa, con procesos ya establecidos, si se tiene en cuenta que les permitirá generar seguridad mediante los procesos de respuesta en los incidentes informáticos que se reporten al interior, de manera rápida y oportuna, sin tener que afrontar o pasar por momentos de incertidumbre al no saber que hacer, como también, les garantizara una infraestructura más segura y con más rendimiento en sus operaciones, por lo que, no deberán gastar esfuerzos en atención a inconvenientes de seguridad, pues estos serán atendidos directamente por el CSIRT, podrán tener la tranquilidad de realizar transacciones más seguras y eficientes con sus respectivos clientes, dando una sensación de seguridad al interior y exterior de la misma, además de que,

debería ser un tema de suma importancia para cualquier organización, es un aspecto clave para las compañías, si lo que se pretende es preservar la integridad de sus datos, como, de todo lo relacionado con el equipo tecnológico e infraestructura, teniendo en cuenta la evolución o nueva generación de tecnologías y herramientas, se deben establecer retos que les garanticen, asegurar cualquier información que se considere importante, mediante la implementación de acciones, procesos o políticas, que les garanticen que siempre serán adecuadas y necesarias, en materia de protección de la información, lo anterior se podrá garantizar con los servicios del CSIRT, es importante resaltar que estos, estarán enfocados principalmente a las compañías que no adquieren sofisticados sistemas informáticos y el talento humano para su administración, si se tiene en cuenta que son las primeras o serán las más vulnerables a cualquier ataque cibernético global.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar la documentación, para el desarrollo y esquema de un CSIRT para la empresa caso de estudio Cibersecurity de Colombia LTDA. Que este satisfaga, las necesidades de sus clientes, mediante soporte especializado en la atención de incidentes.

4.2 OBJETIVOS ESPECÍFICOS

A. Estructurar la información, para determinar las necesidades del CSIRT, como los servicios, según la oferta y la clasificación que se utilizará.

B. Analizar modelos aplicados a los CSIRT, en los países vecinos, con el fin de seguir una metodología Coherente.

C. Diseñar un tratamiento de atención y seguimiento de incidentes de seguridad.

D. Definir los perfiles del equipo de trabajo, así como sus funciones, dando un esquema general del organigrama del equipo del CSIRT.

5 MARCO DE REFERENCIA

5.1 MARCO TEÓRICO

5.1.1 Seguridad informática e Internet. los sistemas informáticos, tiene sus inicios, desde el momento que fue creado internet, esto si hablamos de la protección de datos lógicos, tanto en sistemas de información, como en las bases de datos, en la nube. etc. Internet y la seguridad de la información, se podría decir que tienen algunos puntos en común o más bien que la seguridad de la información depende de internet y que esta se ve amenazada por el uso de internet, se dice que internet es la conexión de redes y de miles de equipos de cómputo, un conjunto descentralizado de redes de comunicación interconectadas, también se le conoce como la mayor autopista de información, la cual utiliza la familia de protocolos TCP/IP, en la actualidad en el año 2020, este número ya alcanza los 4.540 millones de usuarios conectados, es decir, que se ha alcanzado el 59% de la población mundial conectada a la red de redes, se dice que sus orígenes se remontan a la creación en el año 1969, dando un punto de vista muchos más amplio, se puede decir que es una de las maneras de poder entender dichas comunicaciones que están cambiando el mundo, en todos los ámbitos que se pueda conocer, ahora la seguridad informática son los protocolos y medidas que se puedan crear y establecer para que mediante la utilización de internet no se vulnere dicha información o se alteren sus principios fundamentales como lo son (Integridad, Disponibilidad y Confidencialidad), Básicamente internet se usa para el intercambio de información, la cual puede estar en riesgo, si no se da un buen uso al internet, para transferir la información[50].

Se tiene cuatro características u adjetivos importantes que se deben mencionar, las cuales definen lo que es, el concepto más apropiado para referirse a “Internet”.

A. Grande: La mayor red de computadoras que puede existir en todo el mundo, ya que es considerada la autopista más grande de las redes, lo que permite que se tenga una conexión global a internet.

B. Cambiante: Esta se adapta continuamente año tras año a las nuevas necesidades y circunstancias, de todos los usuarios y mercado que acceden a la red más grande conexión existente.

[50] GALEANO Susana. El número de usuarios de Internet en el mundo crece un 7% y alcanza los 4.540 millones (2020) m4rketing Ecommerce. digital. [Sitio Web] enero de 2020: [Consulta: 12 abril 2020] Disponible en: https://marketing4ecommerce.net/usuarios-internet-mundo/

C. Diversa: Da un acceso ilimitado a los equipos que se han conectado según las necesidades de los fabricantes más importantes del mundo, que tienen el *hardware* para dichas conexiones, redes, dominios, tecnologías, plataformas, medios físicos de transmisión, usuarios y otro sin número de conexiones importantes que garantizan la conexión diversa de internet.

D. Descentralizada: Esta parte es fundamental, tanto para el ciudadano del común, hasta los gobiernos más poderosos y polémicos, pues no permite presión política, económica, ni religiosa sobre su operación, no existe una persona que actúe como ordenador inmediatamente oficial, sino que está vigilada por los millones de propietarios de cada una de las grandes o pequeñas redes que puedan existir en todo el mundo, por lo que su independencia es muy importante como se mencionó anteriormente, garantizando comportamientos éticos, respecto a la intimidad de cada uno de los usuarios[51].

5.1.2 Seguridad de la Información. Es una serie de procedimientos, estrategias y herramientas, tal como indica (Rafael Barzanallana) en el documento titulado, Gestión de la Seguridad en Sistemas de Información, su concepto es, "La seguridad de los sistemas informáticos se limita, en general, a garantizar los derechos de acceso a los datos y recursos de un sistema mediante el establecimiento de mecanismos de autenticación y control que garanticen que los usuarios de dichos recursos solo tienen los derechos que se les conceden"[52]. Dicho lo anterior, se da a conocer que la seguridad cibernética, dentro de sus criterios de seguridad, indica que su principal objetivo es permitir que la información siempre esté disponible pero segura, solo para las personas autorizadas y que estas cuenten con los permisos necesarios para tener el acceso a ella, de esta manera se da aplicabilidad a las políticas que se refieren, siendo estas las que se deben seguir estableciendo día a día y que endosan, la conservación mediante lo confidencial, integral y disponible, de toda la información que se procesa en cualquier compañía, sin importar el medio en el cual este almacenada, aplicando estos principios elementales, en las actividades diarias de cualquier organización, por parte de los individuos que estén autorizados para realizarlas, son de suma importancia, por lo que, se está garantizando que la información que se encuentre bajo almacenamiento o trasmisión mediante cualquier medio electrónico, tenga los niveles mínimos de la seguridad de la información, a continuación, se describen los tres principios elementales de la seguridad de la información[53].

[51] VALLEJOS Oscar. Introducción a Internet. Facultad de Ingeniería. [En línea] [Consulta: 12 abril 2020]. P. 2-23 Disponible en: http://ing.unne.edu.ar/pub/internet.pdf
[52] BARZANALLANA Rafael. Gestión de la Seguridad en Sistemas de Información. Introducción a la Seguridad Informática. [En Línea]. España. UMU. [Consulta: 12 abril 2020] P. 18-65 Disponible en: https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf
[53] URIBE, Óp. cit., P. 1.

A. **Integridad:** Implica mantener la consistencia, asegurando que los datos no sufran ningún tipo de cambios sin autorización previa del dueño, así como la claridad y habilidad de los datos informáticos durante todo el ciclo de vida, son muy importantes, lo que garantice que los datos nunca sean inalterados, a menos que sea modificado por personal autorizado o por su único dueño, desde el punto de vista, en que, la perdida de integridad puede acabar en un fraude, todos los sistemas tienen información que debe ser protegida de alteraciones y modificaciones imprevistas, las cuales no han sido autorizadas, así como los accidentes que puedan ocurrir y que lleven a dicho desastre.

B. **Confidencialidad:** Se refiere al amparo o privacidad de los datos almacenados, frente a cualquier propagación no autorizada por el administrador o dueño, lo que Implica que dicha información siempre deba estar disponible o sea manifiesta exclusivamente a los individuos, entes y procesos considerados autorizados, de modo que la Confidencialidad de la información, puede terminar en problemas legales para la compañía, así como la pérdida de su credibilidad y hasta el negocio mismo, pues todos los sistemas de información que contienen datos que se requiere que tengan cierto grado de protección, contra divulgación no autorizada, deben estar amparados bajo la premisa de Confidencialidad, estos pueden ser datos de información comercial, personal o en su defecto, datos que hayan sido patentados de algún producto que la compañía pueda estar desarrollando, en caso de que se violara dicha confidencialidad estos podrían quedar obsoletos y sin ningún tipo de valides[54].

C. **Disponibilidad:** Hace referencia a la continuidad operativa de cualquier empresa en cuanto a sus datos, teniendo la capacidad de estar siempre disponibles, para que san procesados, como también la manipulación o edición por parte del personal autorizado, por lo que esta Implica la accesibilidad a dicha disponibilidad, en su almacenamiento, bien sea en software y hardware, de lo contrario la perdida de la misma, implica el detrimento o quebranto de la productividad o credibilidad en la compañía, los sistemas contienen información y proporcionan servicios que siempre deben estar disponibles, respetando siempre los formatos para la recuperación de la misma de forma correcta, y así satisfacer requisitos de la misma compañía o clientes involucrados, evitando perdidas esenciales como sistemas de seguridad o reconocimiento comercial[55].

---

[54] SEGURIDAD INFORMÁTICA [Anónimo]. Capítulo 1, [En línea] seguridad informática conceptos básicos. [Consulta: 12 abril de 2020]. P. 3-4.19 Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf

[55] ACOSTA UBAQUE Nubia Esperanza y LEÓN PATIÑO Tania Kruskaya. diseño del sistema de gestión de seguridad de la información (s.g.s.i.) para el centro de datos de la personería de Bogotá d.c. bajo las normas ntc-iso-iec 27001:2013 y ntc-iso-iec 27002:2013. UNAD. [En línea] Escuela de Ciencias Básicas, Tecnología e Ingeniería 2017. [Consulta: 12 abril de 2020] P. 21-219 Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11940/35508879.pdf?sequence=1&isAllowed=y

5.1.3 Amenazas de la seguridad informática. En la historia de seguridad informática en el año 1971 se presentó “el primer programa malicioso o virus informático que cuenta nuestra historia”[56], el cual prendió las alarmas y de paso puso en funcionamiento los primeros aspectos de la seguridad informática, como ver las estrategias que se requerían para el aseguramiento de los datos en la red, este virus lleva por nombre (enredadera) este no era un programa malicioso, ya que solo se propago por la red de aproximadamente 50 ordenadores de ARPANET, este programa se propagaba de un ordenador al otro mientras que viajaba por la red, mostrando un mensaje que decía lo siguiente, "Soy una enredadera. ¡Atrápame si tú puedes!". De esta manera dio, inicio el primer virus informático, y así mismo en la mesa las estrategias de seguridad informática, con el fin de poder contrarrestar este tipo de ataques a los ordenadores de la época, para la fecha este sería el primer virus informático de la historia, desde entonces ha surgido la competencia entre los ataques informáticos y la seguridad de la información[57].

5.2 MARCO CONCEPTUAL

5.2.1 Definición de CSIRT. Significado Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática). El CSIRT es un centro u organización conformado por un grupo de expertos en seguridad informática, los cuales tienen como misión la prevención y respuesta ante incidentes de seguridad informática, que se presenten día a día dentro de un grupo de clientes atendidos, tal como lo indica URIBE RAYAS Edgar Felipe en su documento Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática, dice, “además, ayuda con la gestión de la seguridad dentro de su grupo de clientes atendidos, comunicando y coordinando su trabajo con otros CSIRTs y empresas de seguridad informática”[58].

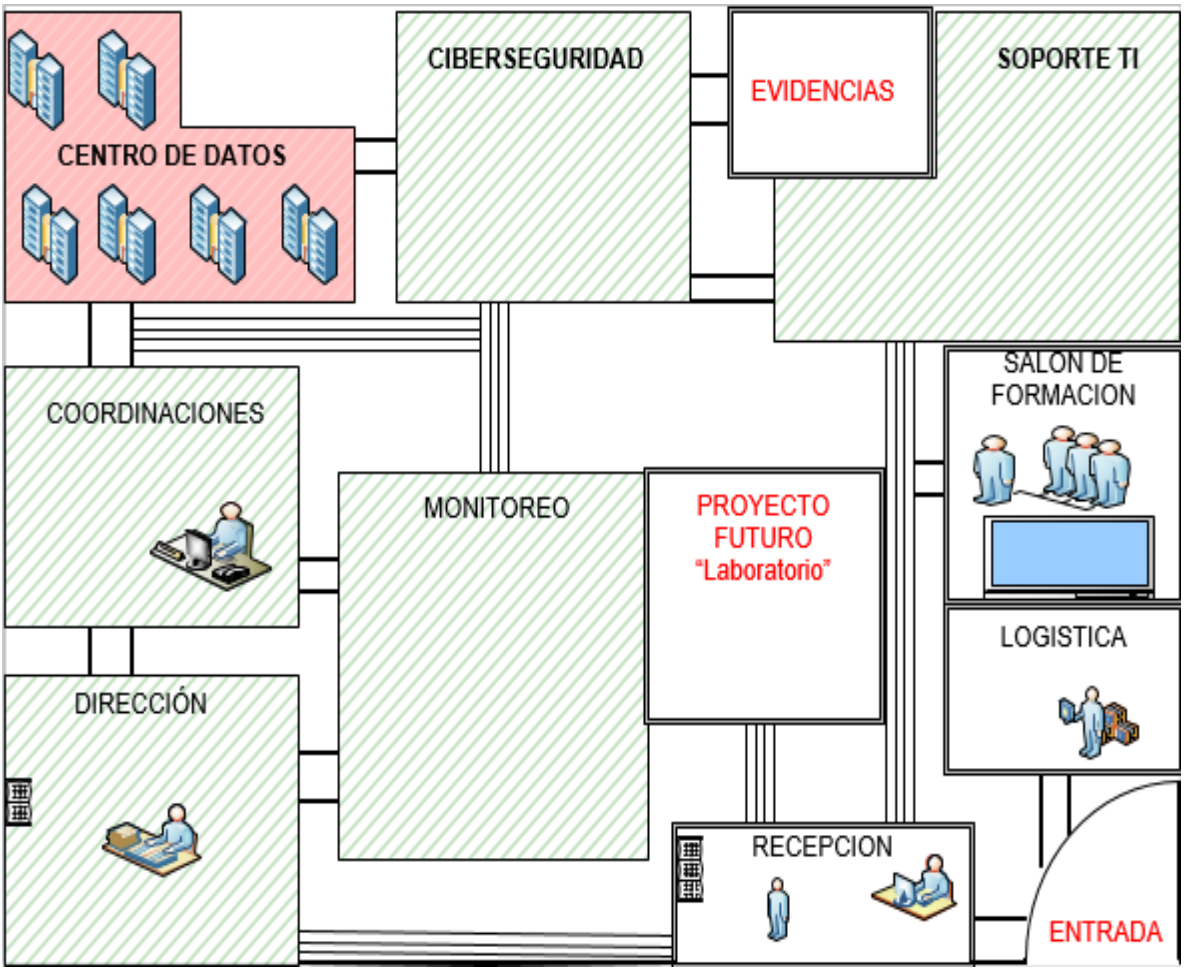
[56] YÚBAL Fm. Xataka. La historia de Creeper, el primer virus informático jamás programado. Historia Tecnológica. [Sitio Web] 06 de mayo del 2018. México: [Consulta: 12 octubre 2019] Disponible en: https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado

[57] IZQUIERDO Robin. Pandorafms. Historia de los virus informáticos: Creeper y Reaper. Monitoring Blog. [Sitio Web] Colombia. octubre 10, del 2018 [Consulta: 12 octubre de 2019] Disponible en: https://pandorafms.com/blog/es/reeper-y-reaper/

[58] URIBE, Óp. cit. P.3

5.2.1.1 Infraestructura física. Dentro de las instalaciones del CSIRT, este debe contar con una serie de especificaciones que no solo le garanticen la seguridad de este en cuanto a fallas sísmicas, incendios, inundaciones, sino que también provea seguridad interna contra personal no autorizado y demás, por esta razón se deben especificar las instalaciones mediante un plano que garantice, que este debe estar separado de las demás áreas de la empresa o personal que esta lo componga, adicionalmente se debe especificar los cuartos de los centros de datos, estos deben contar con un sistema de aires acondicionados, sistemas de incendios, así como todas las medidas de seguridad para el acceso a los mismo solo por el personal autorizado, se debe especificar, las salas de monitoreo, salas de evidencias y demás especificaciones que componen el CSIRT, con el fin de complementar la información se dará un esquema general de la estructura física y grafica del centro de atención a incidentes de Ciberseguridad, en la Figura 4, se evidencia mejor el esquema general de un CSIRT.

Figura 4. Estructura de un CSIRT

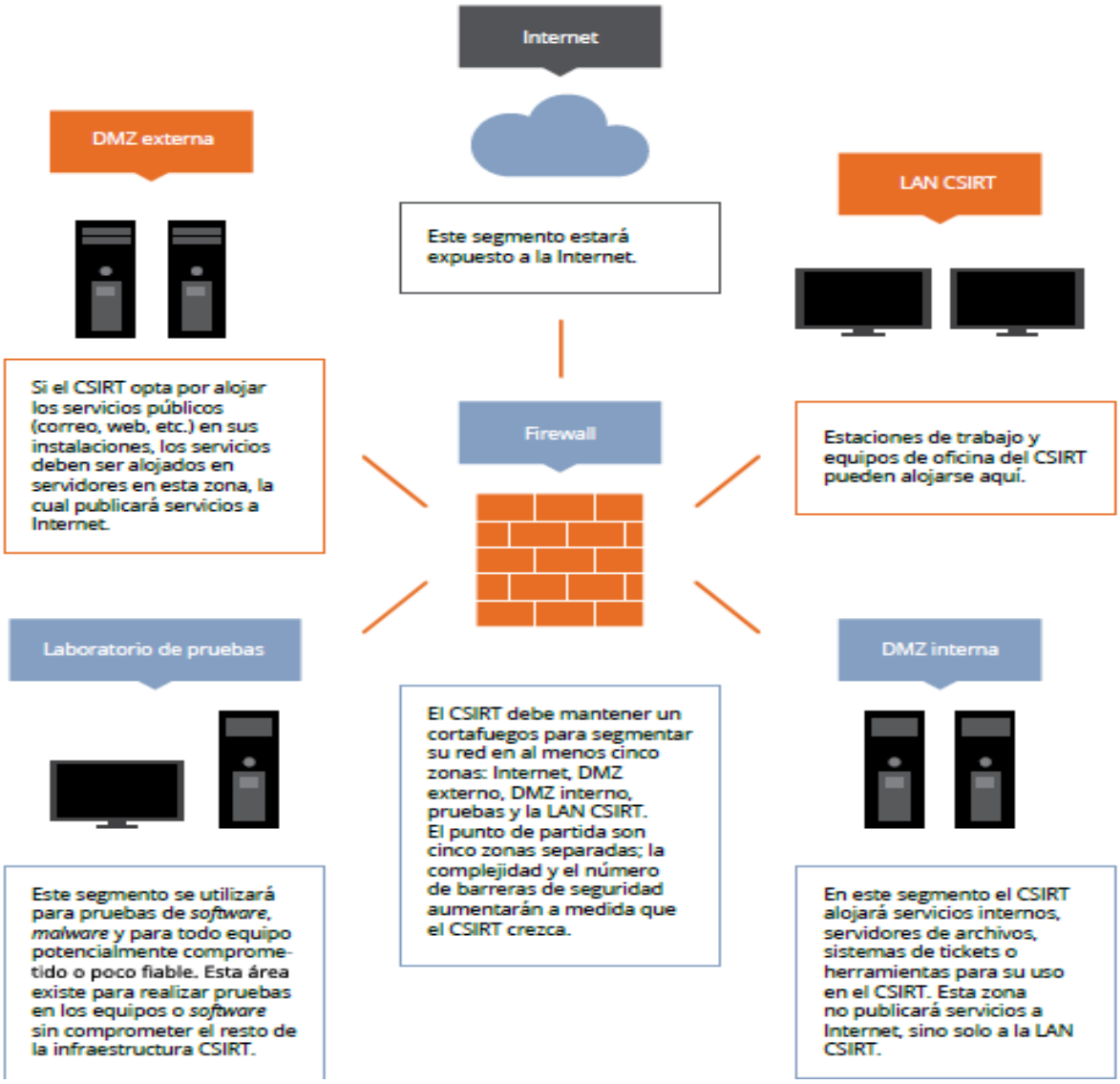


Fuente: Elaboración Propia.

La estructura de los CSIRT, es de suma importancia con el fin de que se tenga una idea de cómo funciona tanto interna como externamente, es por esto por lo que la Organización de los Estados Americanos en la guía de Buenas prácticas para establecer un CSIRT, indica los pasos necesarios con el fin de poder establecer la estructura básica de un equipo de respuesta a incidentes, de esta manera se logra diseñar las que se requieran o se estén pensadas en materializar por parte de las organizaciones o estados que desean implementar dichos centros de atención a incidentes de seguridad, así como ya se indicó la estructura física, se observara la estructura en cuanto a nivel de hardware, software, red y telecomunicaciones, en cuanto al software que requiere el equipo, como lo es el Firewall, para la protección y seguridad, para la mitigación de ataques y protección de la plataforma tecnológica, una buena opción sería (*Radware*), para realizar la consulta de páginas web, también (*Websense*), para la protección de amenazas tipo ATT, lo es, la herramienta (*FireEye*), pasando a la protección de las redes de comunicación y verificación de consumo, una buena herramienta de monitoreo de estas lo es (*Cacti IFX*), dependiendo de las necesidades del servicio se debe contratar un canal de datos e internet dedicado, que garantice el flujo de datos, así mismo contratar con otro canal de datos o internet, con diferente proveedor, con el fin de tener redundancia evitando fallas en la operación, toda vez que este funcionaria como Backup, ahora en el tema relacionado con la adquisición de hardware, en la imagen se da un ejemplo, de los equipos básicos que se podrían adquirir para el funcionamiento del CSIRT. Tal como lo indica la (OEA) en la guía Buenas prácticas para establecer un equipo de respuesta a incidentes de seguridad, se indica en la página 39, que los equipos básicos, pueden ser utilizados de manera equitativa, tanto para el monitoreo como para la protección, así como los servidores que pueden ser utilizados para el almacenamiento de información interna del CSIRT y del grupo de clientes que puedan tener, la información se puede apreciar en la Figura 5[59].

[59] OEA. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (Estados Unidos) Buenas prácticas para establecer un Csirt Nacional. [En línea] abril de 2016. [Consulta: 23 abril 2020] P. 15-55. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Figura 5. Estructura a nivel de hardware, software y red.



Fuente: OEA. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (Estados Unidos) Buenas prácticas para establecer un Csirt Nacional. [En línea] [Consulta: 23 abril 2020] P. 39. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Los equipos de respuesta a incidentes de seguridad informática, son de gran ayuda para toda la comunidad en general, siendo así que se comparten experiencias y situaciones ya afrontadas en la atención de dichos incidentes de seguridad, mediante una base de conocimiento, también se puede establecer que muchos de los CSIRT en la actualidad, también ofrece a algunos clientes los servicios preventivos y educativos, los cuales son publicados en sus sitios web o páginas de acceso exclusivo para dichos clientes, donde se pueden ver los avisos sobre las

vulnerabilidades del software y el hardware en uso, así mismo se indican los programas maliciosos y los virus que están afectando los sistemas en la actualidad, de este modo, los clientes podrán corregir y actualizar rápidamente sus sistemas[60].

5.2.2 Tipos de CSIRT. (Computer Security Incident Response Team). En la actualidad entre los más sobresalientes CSIRT (Computer Security Incident Response Team) o más conocido como equipo de respuesta a incidentes de seguridad informática, como se observan en la Tabla 1.

Tabla 1. Nombres de Csirt.

Listado de CSIRT (Computer Security Incident Response Team) en el mundo.	
1.	CSIRT del sector Académico
2.	CSIRT Comercial
3.	CSIRT del sector Público
4.	CSIRT interno
5.	CSIRT del sector Militar
6.	CSIRT Nacional
7.	CSIRT del sector de la pequeña y mediana empresa (PYME)
8.	CSIRT del sector Financiero

Fuente: Elaboración Propia.

5.2.2.1 CSIRT del sector Académico. Este tipo de CSIRT tienen funciones tanto proactivas como también reactivas. Entre las primeras, se pueden encontrar lo que refiere al permanente monitoreo de las instituciones o institución a la cual prestará sus servicios, con el fin de detectar los incidentes que se presenten en la cotidianidad de la institución, por otro lado se puede encontrar información y vulnerabilidades reportadas de diversas fuentes de la misma institución, permite investigar nuevas tecnologías y herramientas en materia de ciberseguridad, de lo cual se debe generar toda la documentación necesaria al respecto y el desarrollo de talleres, como también otras actividades de capacitación, prevención y concientización a los usuarios de la institución sobre el tema. En el caso de las funciones reactivas, el CSIRT se encarga de alertar de forma oportuna a la institución o las instituciones en el momento que se presente algún tipo de incidente de seguridad, así como de mantener un sistema automático de reportes de incidentes de seguridad para toda la comunidad académica, es importante mencionar que en la actualidad Colombia no cuenta con un CSIRT académico que brinde el soporte de ciberseguridad que las instituciones educativas requieran[61].

[60] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. Óp. cit. P. 8.
[61] RASSELI JUNIOR Luiz Alberto. Casos y Voces – Red clara. Conozca CSIRT.REUNA, el centro de respuesta ante incidentes de seguridad exclusivo para instituciones de I+E. [Sitio Web] (enero 2020). [Consulta: 12 abril de 2020] Disponible en: https://www.redclara.net/index.php/es/noticiasyeventos/casos-y-voces/2018-nace-csirt-reuna-el-centro-de-respuesta-ante-incidentes-de-seguridad-exclusivo-para-instituciones-de-i-e

5.2.2.2 CSIRT Comercial. Los centros de respuesta de ciberseguridad del sector comercial, principalmente prestan sus servicios a empresas del sector comercial, los cuales van desde los reactivos como también los proactivos, así mismo puede prestar servicios a entidades privadas, de sectores educativos, telecomunicaciones, vigilancia, entre otros, incluso a los sectores bancarios, que también cuentan con sus propios centros de respuesta a incidentes de seguridad, que para el caso, Colombia cuenta con el Csirt Financiero, de Asobancaria, son servicios pagados, por lo que se pueden prestar estos a cualquier sector, incluido los sectores públicos.

5.2.2.3 CSIRT del sector Público. Se caracterizan por mantener actualizados y vigentes los estándares tecnológicos para el Sector Público, los servicios están enfocados a agencias públicas, así como a ciudadanos que requieran también servicios de ciberseguridad, estos grupos son los encargados de prestar el servicio de ciberseguridad a las entidades gubernamentales, tanto en las capitales, como los departamentos que tengan entidades de gran infraestructura de datos, que requieran que sus activos estén bajo control.

5.2.2.4 CSIRT interno. Este equipo de respuesta a incidentes, únicamente prestan los servicios de ciberseguridad a las organizaciones a las que pertenecen, estos tipos de CSIRT, Por lo general, no mantienen información propia en los sitios web de manera pública. En ocasiones mantienen relaciones de cooperación con otros Csirt de sectores diferentes, con relación al Grupo de clientes atendido, se enfocan únicamente al Personal y departamento de TI de la organización a la que pertenece el CSIRT.

5.2.2.5 CSIRT del sector Militar. Los CSIRT del sector militar, únicamente prestan los servicios de atención a incidentes de seguridad a las instituciones a las que pertenecen, así como algunas entidades o instituciones que mantienen algunas relaciones estrechamente relacionadas con estos grupos de atención a incidentes de seguridad. Es muy importante mencionar que sus actividades se limitan generalmente a la defensa, control, verificación o a las capacidades cibernéticas ofensivas de la nación a la que pertenecen. Además de las tecnologías de respuesta a incidentes cibernéticos, un aspecto importante que se relaciona de estos CSIRT es que a menudo tienen conocimiento específico de las TIC para uso militar, incluyendo, por ejemplo, armamento y sistemas de radares, muchos casos estos tienen relaciones muy estrechas con los ministerios de defensa de las naciones donde operan.[62]

[62] OEA. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Óp. cit., P. 8

5.2.2.6 CSIRT Nacional. Son conocidos específicamente por servir a una comunidad definida, estos grupos de atención a incidentes de seguridad, por lo general asume el papel de coordinador nacional y también la responsabilidad general de coordinación de los demás sectores, por lo que son el punto de contacto para incidentes nacionales e internacionales, se podría entender que tienen el concepto de que son el último punto de contacto de los demás CSIRTs de la nación donde se encuentran, resaltan por tener una amplia responsabilidad nacional de la comunidad que los rodea, adicionalmente el objetivo de un CSIRT nacional varía en función de las necesidades de sus administradores y como también de sus roles designados y de la existencia de otros centros. Ya que, por ejemplo, si no hay un CSIRT estrictamente definido o enfocado en la infraestructura critica, los CSIRTs nacional podrían asumir las responsabilidades de estos. Por lo que, ya mencionado anteriormente, esto permite que se les considere como un "CSIRT de último recurso", como también de las actividades de ciberseguridad de las cuales nadie más está a cargo. De este modo, es muy común ver a varios CSIRTs, siendo parte, de la comunidad a la que sirve el CSIRT nacional.[63]

5.2.2.7 CSIRT del sector de las (PYMES). Por el tamaño y la naturaleza de las Pymes, la defensa de ciberseguridad, no está a la orden como se esperaría, por lo que a menudo no les permiten a las Pymes implementar equipos de respuesta a incidentes de manera individual, si tomamos como Ejemplo a Colombia, las Pymes no cuentan con un CSIRT propio, o que este dedicado específicamente para ellas, por lo que tienen que solicitar estos servicios a los diferentes centros que existen en el país, para que les presten los servicios de ciberseguridad, como lo es, el "CSIRT-CCIT de la Cámara Colombiana de Informática y Telecomunicaciones"[64], de esta manera surge la necesidad de concentrar esfuerzos, profundizar en materia y crear un estudio documentado que sirva como guía, en algunos aspectos relevantes a la hora de implementar un CSIRT que pueda prestar los servicios de ciberseguridad a las Pymes, así como también responda a las necesidades de esta comunidad, uno de los propósitos de este estudio y proyecto, es la implementación documentada de un CSIRT dedicado las 24 horas los 365 días del año a la seguridad de la infraestructura de la compañía Cibersecurity de Colombia LTDA, como una buena opción de mercado con los clientes que pueda obtener de las Pymes, viendo como ejemplo, en España donde el Instituto Nacional de Tecnologías de la Comunicación, sociedad anónima estatal adscrita al Ministerio de Industria, el INTECO-CERT o que desde el 2012 es conocido como (INCIBE) [65], que dirige sus servicios a PYMES y ciudadanos según sus necesidades.[66]

[63] CENTRO CRIPTOLÓGICO NACIONAL. Óp. cit., P. 29.
[64] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Óp. Cit.
[65] INCIBE INSTITUTO NACIONAL DE CIBERSEGURIDAD (España) [Sitio Web]. [Consulta: 12 abril de 2020] Disponible en: https://www.incibe.es/
[66] OEA. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, Óp. cit., P. 8.

5.2.2.8 CSIRT del sector Financiero. Esos CSIRT proporcionan servicios a las entidades bancarias del país donde se encuentran, sus servicios son reactivos como también los proactivos, manejan campañas de sensibilización dentro de la organización bancaria a los usuarios finales, así evitar la propagación de incidentes de seguridad, siendo estas preventivas, dentro de su plan de enfoque manejan el desarrollo y establecimiento de comunidades de intercambio de inteligencia cibernética con otros centros Nacionales o Internacionales, Colombia, cuenta con el CSIRT Financiero de Asobancaria, el cual está dedicado específicamente a la atención de la infraestructura critica del sector bancario del país, este centro fue creado en 2018 por Asobancaria, dentro de sus funciones podemos contar la de anticipar y mitigar riesgos derivados de amenazas cibernéticas, como también el apoyo a la respuesta de los incidentes en el sector financiero Colombiano.[67]

5.2.3 Ventajas de tener un CSIRT. Colombia cuenta con diferentes centros de atención a respuesta de incidentes de seguridad, como se ha mencionado en los párrafos anteriores, los cuales son de orden territorial y otros como Asobancaria de orden privado, Disponer de un equipo dedicado a la seguridad de las compañías, en especial de las pequeñas y medianas empresas Pymes, ayuda a mitigar y evitar los incidentes graves y a proteger su patrimonio, así mismo se tiene alcance a los conocimientos necesarios para la atención de incidentes de seguridad, otra ventaja importante es perder atender los aspectos jurídicos, si se tiene en cuenta que muchas veces los ataques informáticos terminan en un procesos penal, tener experiencia en la atención de incidentes de seguridad[68].

5.3 MARCO HISTÓRICO

5.3.1 Familia de normas ISO. A lo largo de la historia de la seguridad informática y los delitos informáticos, los estándares de las normas ISO, relacionadas con la seguridad de la información y seguridad informática, han teniendo gran referencia en la materia, motivo por el cual se les reconocerá su importancia y se hablara un poco de cada una de ellas en los siguientes capítulos, como lo son las pertenecientes a la familia ISO 27000, son de gran importancia para cualquier implementador de sistemas de información, así como de los auditores y demás funcionarios que tengan relación directa con temas de seguridad de la información, la familia ISO tiene sin números de normas, las cuales indican y especifican su apoyo al objetivo por el cual fueron implementadas, muchas de ellas han tenido cambios sustanciales, como mejoras e incluso han cambiado de nombre, se realizara un listado de alguna de ellas, con la información más actualizada que se pueda obtener actualmente.

[67] ASOBANCARIA. Óp. Cit.
[68] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. Óp. cit., P. 8.

5.3.1.1 ISO 27000. Vocabulario estándar para el SGSI, Publicada en 2007, la ISO 17799 se renombra y pasa a ser la ISO 27002, contiene el vocabulario en el que se apoyan el resto de las normas. Es similar a una guía/diccionario que describe los términos de todas las normas de la familia. Estándar para el SGSI. Introducción y base para el resto. Publicación original: 2009. Revisiones y actualizaciones: 2012, 2014, 2016, 2018[69].

5.3.1.2 ISO 27001. Es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado en el contexto de los riesgos comerciales generales de la organización. Es la certificación que deben obtener las organizaciones. Aumentando la cantidad de controles (de 133 a 114), 35 objetivos de control y ha incrementado la cantidad de dominios (de 11 a 14). En la revisión 2013, se eliminaron algunos requerimientos como las medidas preventivas y la necesidad de documentar determinados procedimientos. En el que se detallan, las líneas generales de los controles propuestos por el estándar. Norma que especifica los requisitos para la implantación del SGSI. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Publicación original: 2005 Revisiones: 2013, 2013/Cor 1:2014, 2013/Cor 2:2015. Se realizó revisión de la norma sin cambios de fondo, aunque si en la estructura de la parte principal[70].

A. Numeral A 16: este numeral hace parte del Anexo A de la norma ISO 27001, el cual brinda la información de importancia para la correcta Gestión de Incidentes en Seguridad informática, entre otros puntos de gran importancia como la manera de realizar el reporte de eventos, como también los procedimientos de respuesta, las debilidades del sistema, las responsabilidades y también un punto destacado como lo es la recolección de evidencias[71].

[69] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27000: 2018. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario. Óp. cit.
[70] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27001: 2013. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. Óp. cit.
[71] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27001: 2013. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Numeral A16. Óp. cit.

5.3.1.3 ISO 27002. Dentro de esta norma se encuentra, una recopilación de buenas prácticas para la Seguridad de la Información, que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles. Es un código de buenas prácticas para la gestión de seguridad de la información. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799, Publicada el 1 de julio de 2005 como ISO 17799:2005, Nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007. Última versión: 27002:2013, 25 de septiembre de 2013[72].

5.3.1.4 ISO 27003. Es una guía que, contiene las directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001, indicando las directivas generales e Incluye instrucciones precisas para la correcta implementación de un SGSI con éxito. Publicada el 1 de febrero de 2010, Actualizada el 12 de abril de 2017, No es certificable[73].

5.3.1.5 ISO 27004. Guía para el desarrollo y utilización de métricas y especifica cómo configurar métricas, qué medir, con qué frecuencia, cómo medirlo y la forma de conseguir objetivos. Proporciona orientación sobre el desarrollo y uso de medidas y Utilizando técnicas aplicables para determinar la eficacia de un SGSI, así mismo de los controles o grupos de controles implementados según ISO/IEC 27001, Publicada el 15 de diciembre de 2009, Revisada en diciembre de 2016, No certificable[74].

[72] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27002: 2013. Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. Óp. cit.

[73] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27003: 2017. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Orientación. Óp. cit.

[74] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27004: 2016. Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Monitoreo, medición, análisis y evaluación. Óp. cit.

5.3.1.6 ISO 27005. Es una guía que Proporciona directrices y recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información, Apoya los conceptos generales que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información, basada en ejemplos, de posibles amenazas, vulnerabilidades e impactos, adicional para ayudar a la implementación satisfactoria de la seguridad de la información, establecida en un enfoque de gestión de riesgos. Publicada: 15 de junio de 2008, Segunda versión: 1 de junio de 2011. Actualización 2018[75].

5.3.1.7 ISO 27006. Es un conjunto de requisitos, que tiene como objetivo principal apoyar la acreditación para las organizaciones certificadoras. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Publicada: 1 marzo de 2007. Segunda versión: 1 diciembre de 2011, Tercera versión: 30 septiembre de 2015. Actualización 2020[76].

5.3.1.8 ISO 27007. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. Establece qué se debe auditar y cuándo, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, etc. Proporciona orientación sobre la gestión de un programa de auditoría del SGSI, sobre la realización de auditorías y sobre la competencia de los auditores, Será remplazada por: ISO/IEC DIS 27007. Publicación original: 14 noviembre de 2011. Revisiones: 09 de octubre de 2017. Actualización 2020[77].

[75] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27005: 2018. Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información. Óp. cit.
[76] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27006: 2015 / AMD 1: 2020. Tecnología de la información. Técnicas de seguridad. Requisitos para organismos que realizan auditorías y certificación de sistemas de gestión de seguridad de la información. Enmienda 1. Óp. cit.
[77] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27007: 2020. Seguridad de la información, ciberseguridad y protección de la privacidad: directrices para la auditoría de sistemas de gestión de seguridad de la información. Óp. Cit.

5.3.1.9 ISO 27008. Guía de auditoría de los controles seleccionados en el marco de implantación de un SGS. Proporciona orientación sobre la revisión y evaluación de la implementación y operación de los controles de seguridad de la información, incluida la evaluación técnica de los controles del sistema de información, Publicada: 15 de octubre de 2011, Revisiones: 2019, No certificable[78].

5.3.1.10 ISO 27009. Define los requisitos para el uso de ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector de mercado). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del Anexo A., Publicada: 15 de junio de 2016. Actualización 2020. No certificable[79].

5.3.1.11 ISO 27010. Consiste en una guía para la gestión de la seguridad de la información, que proporciona directrices, además de la orientación a la familia de estándares ISO/IEC 27000, para implementar la gestión de la seguridad de la información, en las comunidades que comparten información. Cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, a nivel nacional e internacional. Publicación Original: 20 de octubre de 2012. Revisada: 10 de noviembre de 2015[80].

Las normas ISO, son las herramientas esenciales de cualquier administrador o implementador de sistemas, son su diccionario para la puesta en marcha de un sistema de información y el apoyo para la aplicación de políticas, como también pueden ser las aliadas más importantes, a la hora de algún tipo de inconveniente con los sistemas de información, es por esta razón que se relacionan otros estándares que son muy importantes, los cuales se alejan del consecutivo que se lleva.

[78] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC TS 27008: 2019. Tecnología de la información. Técnicas de seguridad. Directrices para la evaluación de los controles de seguridad de la información. Óp. Cit.
[79] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27009: 2020. Seguridad de la información, ciberseguridad y protección de la privacidad. Aplicación sectorial específica de ISO / IEC 27001. Requisitos. Óp. Cit.
[80] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27010: 2015. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información para las comunicaciones intersectoriales e interorganizacionales. Óp. Cit.

5.3.1.12 ISO 27035. Norma muy importante, en lo correspondiente a la atención de incidentes de seguridad de la información, Tecnología de la información. Conceptos básicos y fases de la gestión de incidentes seguridad de la información, Técnicas de seguridad. En la Parte 1 de esta, indica sobre los Principios de gestión de incidentes. Determina el enfoque estructurado correspondiente para el proceso de detectar, evaluar, informar y responder a los incidentes de seguridad informática, así como también, aplicar las lecciones aprendidas, última actualización 2016-11[81].

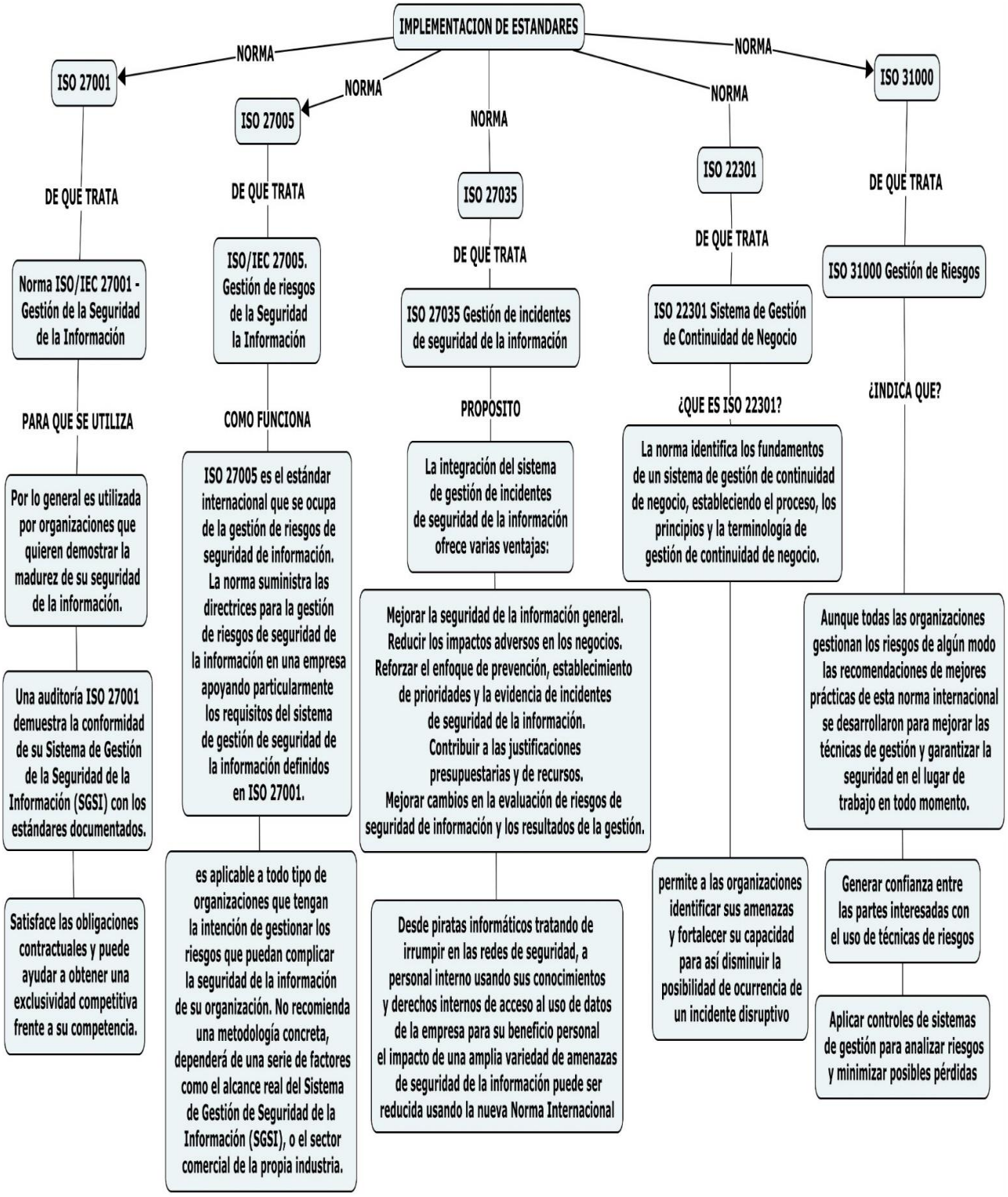
5.3.1.13 ISO 22301. La presente norma representa los requisitos que las organizaciones necesitan, para la gestión de la continuidad del negocio, independientemente de su ubicación, tamaño, actividad o sector, para que las empresas, puedan estar mejor preparadas y con más confianza a la interrupción. Son los incidentes los que pueden interrumpir la operación de una organización en cualquier momento, la aplicación de la presente norma ISO 22301, garantiza que puedan responder y continuar con sus operaciones normalmente, última actualización en 2013[82].

5.3.1.14 ISO 31000. Con la implementación de la presente norma, las empresas, podrán realizar la Gestión de riesgos, dicha norma expresa el - Vocabulario, que trata evaluación de riesgos, específicamente con la terminología de gestión de riesgos y relacionados con la gestión de identidad, está destinada a ser utilizada a cualquier organización, la protección y gestiones de los riesgos informáticos, son de suma importancia, si lo que se pretende, es mantener la Seguridad de la información, ciberseguridad y protección de la privacidad de los activos de las organizaciones[83].

En la Figura 6. Se observan algunas de las nomas, que se mencionaron anteriormente de la familia 27000, así como una explicación, de lo que son estas normas ISO.

[81] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 2: Directrices para planificar y prepararse para la respuesta a incidentes. Edición 1. Óp. Cit.
[82] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO 22301: 2012, la seguridad societal - sistemas de gestión de la continuidad del negocio. Óp. Cit.
[83] ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC Aplicación de ISO 31000 para la evaluación de riesgos relacionados con la gestión de identidad. Óp. Cit.

Figura 6. Descripción de los estándares de la familia ISO



Fuente: Elaboración propia.

Ya habiendo conocido más de fondo lo relacionado con la seguridad de la información y sus tres principios fundamentales, los cuales permiten tener ideas claras acerca de lo que refiere a la seguridad de la información y las acciones que se deben adelantar, con el fin de que se mantenga a salvo los secretos de cualquier compañía. Es de suma importancia que se tenga conocimiento pleno de la forma como toda necesidad de seguridad es dependiente de salvaguardas que le permitan mantener las amenazas controladas, de esta manera se protegen los activos, así mismo las amenazas incrementan el riego de que se dichas amenazas se conviertan en vulnerabilidades que estas luego puedan ser explotadas y afectar directamente los activos de la compañía donde se originan, convirtiéndose en un ciclo que se debe controlar, por lo que se debe tener claridad que todo lo referente a seguridad de la información inicia desde una necesidad de la misma, por proteger cada uno de los activos que las compañías desean tener seguros, corrigiendo las amenazas evitando que sean explotadas, que no afecten los activos y estos no generen impactos negativos, para representar lo anterior, se podrá observar gráficamente en la Figura 7.

Figura 7. La necesidad de seguridad como se convierte en riesgo

Fuente: BARZANALLANA Rafael. Gestión de la Seguridad en Sistemas de Información. Introducción a la Seguridad Informática. [en línea] España. UMU. [Consulta: 12 abril del 2020]. P. 18-65 Disponible en: https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf

5.4 MARCO ESTADO ACTUAL

La ciberseguridad en todo el mundo, cada día cobra más importancia, por su alto grado de relevancia en diferentes aspectos, entre los más importantes los económicos, pues si bien la seguridad de la información, cubre diversos campos en la protección de datos y procesos informáticos, es importante indicar que la mayoría de las empresas en Colombia, se preocupan principalmente por la seguridad de dichos datos, si bien estos representan el activo más importante con el que cuentan, es por esta razón que tanto las compañías, como el gobierno realizan esfuerzos con el fin de fortalecer cada día la seguridad digital en el país. Dado una importancia relevante al tema, motivo por el cual Colombia ha venido fortaleciendo su capacidad de respuesta en lo relacionado con la ciberseguridad, como se indica en el reciente estudio realizado por la Organización de los Estados Americanos OEA y el Banco Interamericano de Desarrollo BID, mediante el documento denominado (Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe), en dicho reporte se resalta la participación de Colombia en los diferentes aspectos de la seguridad informática que se llevan actualmente en el continente y su relación con las organizaciones mundiales que lideran las estrategias contra las amenazas de la ciberseguridad, como lo son la (OEA) y el (BID), los cuales están liderando este estudio en los diferentes países de América Latina, donde resaltan la continua participación de Colombia, así como los esfuerzos realizados en relación con seguridad digital, en dicho reporte, destacan las dos políticas nacionales adoptadas en Colombia, en cuanto a la seguridad Cibernética, los recursos invertidos en seguridad digital, haciendo mención al colCERT, centro cibernético policial y los demás centros de atención de incidentes de seguridad informática y ciberseguridad, es así como el compromiso en materia que ha permitido que se creen espacios y compromisos con las diferentes instituciones tanto públicas como privadas, con el fin de fortalecer la seguridad de la información en la población, los ministerios han realizado esfuerzos económicos para brindar becas a los empleados públicos para complementar o fortalecer sus estudios en seguridad digital, así mismo el gobierno nacional ha exhortado a las instituciones universitarias, para que mejoren las temáticas de enseñanza en temas relacionados con la seguridad digital, brindando mejor calidad en la educación y fortaleciendo los ´procesos de educación con recursos públicos[84].

[84] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. [En Línea] [Consulta: 10 abril de 2020] P. 81-204 Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

5.4.1 Estado actual de la seguridad cibernética en el país. Los aspectos actuales de la seguridad digital en el país se encuentran de la siguiente manera, según comparativo realizado desde el 2016 al 2020, por OEA y BID en el reporte de ciberseguridad 2020, resaltando el buen manejo y la importancia que se le ha dado al tema, así como la proyección que se realizó en los últimos años en temas de seguridad digital, dentro de este comparativo que se realizara, se resaltaran tomas de gran importancia como lo son[85]:

A. Política y estrategia de seguridad cibernética.

B. Cultura cibernética y sociedad.

C. Formación, capacitación y habilidades de seguridad cibernética.

D. Estándares, organizaciones y tecnológicas.

E. Marcos legales y regulatorios.

5.4.1.1 Política y Estrategia de Seguridad Cibernética. Dentro del comparativo, de política y estrategia se evalúan en la comparación los siguientes puntos específicos:

A. Estrategia Nacional de Seguridad Cibernética. En esta se puede apreciar, como han aumentado factores tan importantes como:

I. **Desarrollo de la estrategia:** en el año 2016 la estrategia se tenía implementados 3 puntos y para el año 2020 se desarrollaron 2 para completar los 5 en total que se tenían proyectados, teniendo un incremento de la estrategia de un 66%, lo cual indica que fue muy bien recibida.
II. **Organización:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.
III. **Contenido:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 33% pendiente 1 punto por desarrollar.

B. Respuesta a Incidentes. Se identifican cuatro factores con un crecimiento sumamente importante.

I. **Identificación de Incidentes:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 puntos por desarrollar.

[85] Ibid., P. 82.

II. **Organización:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.
III. **Coordinación:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.
IV. **Modo de Operación:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 400% en la estrategia, pendiente 1 punto por desarrollar.

C. Protección de la Infraestructura Crítica (IC). Se observa un crecimiento de gran importancia en un punto de suma importancia para la seguridad cibernética del país.

I. **Identificación:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 punto por desarrollar.
II. **Organización:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.
III. **Gestión de Riesgos y Respuesta:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.

D. Manejo de Crisis.

I. **Manejo de Crisis:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.

E. Defensa Cibernética.

I. **Estrategia:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.
II. **Organización:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.
III. **Coordinación:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 punto por desarrollar.

F. Redundancia de Comunicaciones.

l. **Redundancia de Comunicaciones: Organización:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar. Todos los datos anteriormente mencionados, son recopilados en la Figura 8.

Figura 8. Comparativo política y estrategia Ciberseguridad 2016 Vs 2020

Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. [En Línea] [Consulta: 10 abril de 2020] P. 82 Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

5.4.1.2 Cultura Cibernética y Sociedad. Dentro del comparativo, Cultura Cibernética y Sociedad, se evalúan en la comparación los siguientes temas:

A. Mentalidad de Seguridad Cibernética un incremento moderado.

I. **Gobierno:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 4 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 1 punto por desarrollar.
II. **Sector Privado:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.
III. **Usuarios:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.

B. Confianza y Seguridad en Internet, el incremento no fue el esperado.

I. **Confianza y Seguridad en el Internet del Usuario:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.
II. **Confianza del Usuario en los Servicios de Gobierno Electrónico:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.
III. **Confianza del Usuario en los Servicios de Comercio Electrónico:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 punto por desarrollar.

C. Comprensión del Usuario de la Protección de la Información en Línea.

I. **Comprensión del Usuario de la Protección de Información Personal en Línea:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 200% en la estrategia, pendiente 3 punto por desarrollar.

D. Mecanismos de Denuncia.

I. **Mecanismos de Denuncia:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 300% en la estrategia, pendiente 2 punto por desarrollar.

E. Medios y Redes Sociales.

I. **Medios y Redes Sociales:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del

300% en la estrategia, pendiente 2 puntos por desarrollar. Todos los datos anteriormente mencionados, son recopilados en la Figura 9.

Figura 9. Comparativo Cultura Cibernética y Sociedad 2016 Vs 2020

Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. [En Línea] [Consulta: 10 abril de 2020] P. 82 Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

5.4.1.3 Capacitación y Habilidades de Seguridad Cibernética. Dentro del comparativo, de Formación, Capacitación y Habilidades, se evalúan en la comparación los siguientes temas:

A. Sensibilización.

I. **Programas de Sensibilización:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.
II. **Sensibilización Ejecutiva:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 punto por desarrollar.

B. Marco para la Formación.

I. **Provisión:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.
II. **Administración:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.

C. Marco para la Capacitación Profesional.

I. **Provisión:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 punto por desarrollar.
II. **Apropiación:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar, tal como se observa en la Figura 10.

Figura 10. Comparativo Formación, Capacitación y Habilidades 2016 Vs 2020

Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. [En Línea] [Consulta: 10 abril de 2020] P.82 Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

5.4.1.4 Marcos Legales y Regulatorios. Dentro del comparativo, de Marcos Legales y Regulatorios, se evalúan en la comparación los siguientes temas:

A. Marcos Legales.

I. **Marcos Legislativos para la Seguridad de las TIC:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 punto por desarrollar
II. **Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos

para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.

III. **Legislación Sobre Protección de Datos:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 300% en la estrategia, pendiente 2 punto por desarrollar.

IV. **Protección Infantil en Línea:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 300% en la estrategia, pendiente 2 punto por desarrollar.

V. **Legislación de Protección al Consumidor:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 200% en la estrategia, pendiente 3 punto por desarrollar.

VI. **Legislación de Propiedad Intelectual:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 300% en la estrategia, pendiente 2 punto por desarrollar.

VII. **Legislación Sustantiva Contra el Delito Cibernético:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.

VIII. **Legislación Procesal Contra el Delito Cibernético:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.

B. Sistema de Justicia Penal.

I. **Fuerzas del Orden:** su progreso fue el siguiente, de 3 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 2 punto por desarrollar.

II. **Enjuiciamiento:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.

III. **Tribunales:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.

C. Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético.

I. **Cooperación Formal:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 300% en la estrategia, pendiente 2 punto por desarrollar.

II. **Cooperación Informal:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 200% en la estrategia, pendiente 3 punto por desarrollar, según se observa en la Figura 11.

Figura 11. Comparativo Marcos Legales y Regulatorios 2016 Vs 2020

Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. [En Línea] [Consulta: 10 abril de 2020] P. 82 Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

5.4.1.5 Estándares, Organizaciones y Tecnologías. Dentro del comparativo, de Estándares, Organizaciones y Tecnologías, se evalúan en la comparación los siguientes temas:

A. Cumplimiento de los Estándares

I. **Estándares de Seguridad de las TIC:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.
II. **Estándares en Adquisiciones:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.
III. **Estándares en el Desarrollo de Software:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 3 punto por desarrollar.

B. Reciliencia de la Infraestructura de Internet

I. **Reciliencia de la Infraestructura de Internet:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 50% en la estrategia, pendiente 2 punto por desarrollar.

C. Calidad del Software

I. **Calidad del Software:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 200% en la estrategia, pendiente 3 punto por desarrollar.

D. Controles Técnicos de Seguridad

I. **Controles Técnicos de Seguridad:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 3 puntos para el año 2020, un incremento del 300% en la estrategia, pendiente 2 punto por desarrollar.

E. Controles Criptográficos

I. **Controles Criptográficos:** su progreso fue el siguiente, de 0 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 200% en la estrategia, pendiente 3 punto por desarrollar.

F. Mercado de Seguridad Cibernética

I. **Tecnologías de Seguridad Cibernética:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.
II. **Seguro Cibernético:** su progreso fue el siguiente, de 2 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 0% en la estrategia, pendiente 3 punto por desarrollar.

G. Divulgación Responsable

I.Divulgación Responsable: su progreso fue el siguiente, de 1 puntos implementados en el año 2016 a 2 puntos para el año 2020, un incremento del 100% en la estrategia, pendiente 3 punto por desarrollar, según Figura 12.

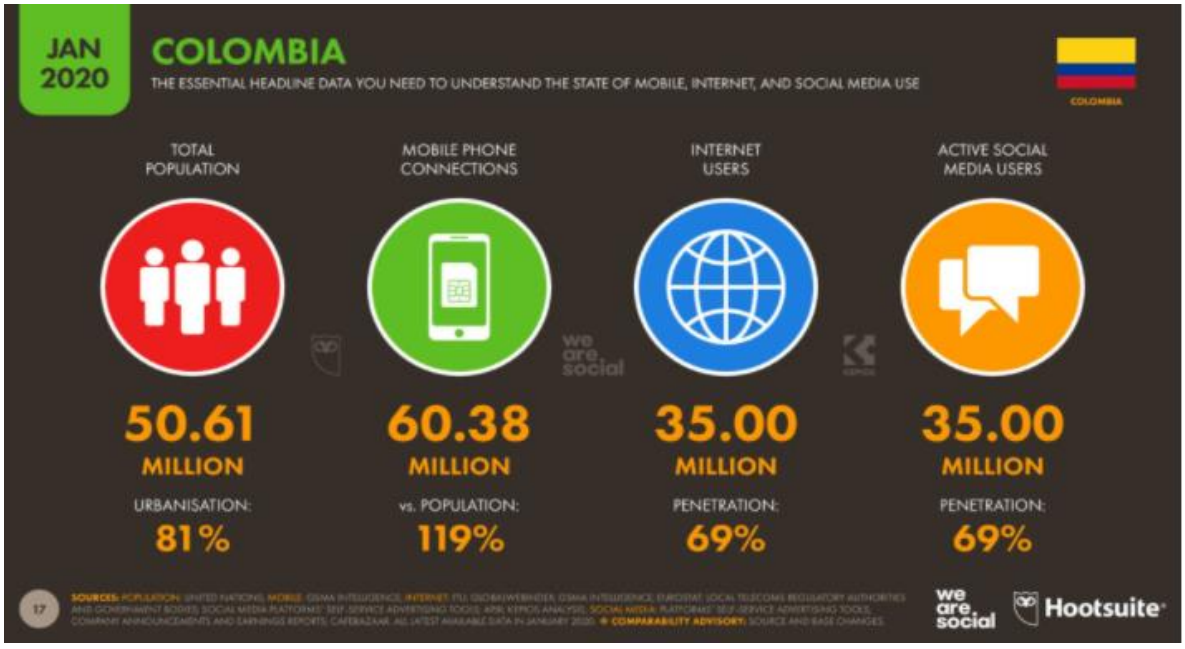
Figura 12. Comparativo Estándares 2016 Vs 2020

Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. [En Línea] [Consulta: 10 abril de 2020] P. 82 Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

5.5 MARCO TECNOLÓGICO

5.5.1 Avances Tecnológicos. La tecnología es una de las ramas más importantes que la sociedad pueda tener en la actualidad, tanto para sus ratos de ocio, su entretenimiento, negocios, trabajo, compras y estudios, entre las más importantes por mencionar, es por ello que los gobiernos, instituciones, empresas, comercios y ciudadanía en general, siempre quieren tener la mejor tecnología disponible, todo con el fin de poder acceder a miles de procesos que faciliten las actividades diarias que se realizan, dependiendo del rol en el que se esté desarrollando, Colombia ha logrado importantes avances tecnológicos, que la han posicionado en el mercado digital, aunque se requieren mayores esfuerzos se ve con buenos ojos los avances que se han logrado al año 2020, donde se evidencian cifras que resaltan el trabajo realizado, indicando que ha logrado una conexión total de 35 millones de ciudadanos en internet, lo cual representa el 69% de la población, se observa que 50,61 millones de ciudadanos cuentan con conexión a internet desde sus teléfonos, y que actualmente se tienen 60,38 millones de líneas telefónicas activas, esto representa un número mayor al de la población actual, indicando que una persona puede tener más de una línea telefónica con conexión a internet, otro dato importante es que la misma cifra de conectados a internet, está conectada en redes sociales 35 millones, estos datos son los publicados en junio de este año, para mejor observación de las cifras, en la Figura 13.

Figura 13. Situación digital en Colombia 2020



Fuente: Yi Min Shum. Situación digital, Internet y redes sociales Colombia 2020. [En Línea] [Consulta: 12 septiembre de 2020] Disponible en: https://yiminshum.com/social-media-colombia-2020/

5.5.2 Importancia de la tecnología. La tecnología inicialmente fue creada para fines expresamente específicos en especial los militares, pero con el pasar de las décadas y los años, ha cobrado gran importancia en miles de aspectos de la vida diaria de las personas, hoy día, su principal foco está en la economía y la industria, lo cuales han hecho que la tecnología tenga la importancia que tiene en la actualidad, pues esta ha sido la que ha revolucionado la industria y con ello la economía de las naciones, tal como se pudo demostrar en la pandemia por el COVID 19, colocando en evidencia que se necesitaba de una tecnología y redes robustas, para suplir la demanda que se generó, tanto para el trabajo en casa, como compras online, telemedicina, creación de negocios digitales, educación virtual y miles de actividades que requerían de la tecnología moderna[86].

5.5.3 Infraestructura tecnológica. la infraestructura tecnológica actual en las organizaciones y empresas colombianas es de gran relevancia, pues si se tiene en cuenta las necesidades del servicio, así debe serlo. Pasando a lo especifico dentro de una infraestructura tecnológica moderna se deben incluir herramientas que suplan las necesidades de los servicios que se prestan dentro de cada campo como tal, es por ellos que la empresa Cibersecurity de Colombia LTDA. Debe fortalecer su infraestructura tecnológica para que pueda prestar un buen servicio a cada uno de sus usuarios, debe incorporar dentro de estas herramientas, software y hardware de buena calidad que le permita un eficiente proceso en la atención de incidentes de seguridad de la información.

5.5.3.1 Software para ciberseguridad. Dentro de las herramientas de software que se mencionaran más adelante, en este mismo numeral, para el tratamiento de incidentes, monitoreo, análisis y demás actividades que desarrolla el CSIRT, se pueden mencionar algunas de ellas que brindan algún tipo de garantía en la seguridad de la infraestructura tecnológica que se pretende proteger, tal como se afirma en el sitio web de Ciberseguridad denominado, Noticias relevantes sobre este sector en auge[87].

A. ***FireMon:*** se trata de una plataforma para realizar la gestión de políticas de seguridad especialmente para las de red (NSPM), la cual brinda a los equipos destinados a la seguridad y operaciones, la visibilidad como también el análisis automatizado para dichos dispositivos de seguridad de la red. La interfaz para el usuario está basada en la web, esta permite a los usuarios analizar sus políticas de

[86] ADR Formación. Día de Internet 2020: la importancia de la tecnología durante la crisis sanitaria. Mayo de 2020. Blog. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.adrformacion.com/blog/dia_de_internet_2020_la_importancia_de_la_tecnologia_durante_la_crisis_sanitaria.html

[87] Ciberseguridad. Noticias relevantes sobre este sector en auge. Software de seguridad informática. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://ciberseguridad.com/herramientas/software/

seguridad de red, localizar fallas de cumplimiento y evaluar vulnerabilidades de seguridad.

B. ***Qualys Cloud Platform*:** este software se encarga de la gestión de seguridad y vulnerabilidades de las redes, ofreciendo exploración y seguridad de las aplicaciones, como también el mapeo para la detección de dispositivos de red. *Qualys Cloud Platform*, es de suma importancia en la programación y corrección de prioridades de vulnerabilidades, existe una versión local, *Qualys Private Cloud Platform*, la cual es utilizada para las empresas con estrictas reglas de soberanía de datos, para los parches.

C. ***CrowdStrike:*** ofrece un sistema antivirus, para la suite *Falcon Endpoint Protection*, siendo de suma importancia en la detección de amenazas, la detección de *malware* de aprendizaje automático y la actualización sin firma.

D. ***Wireshark:*** es una de las mejores herramientas de código abierto que proporcionará un profundo análisis exhaustivo de la red. Este Software cuenta con una gran variedad de características interesantes, como ser compatible con muchos protocolos y sistemas operativos entre los más importantes Windows, Linux o Mac iOS, puede realizar el análisis sobre una red existente, sobre un mapeado, como también sobre un archivo existente en el disco. Puede incluir un amplio diccionario, para luego aplicar los filtros a la navegación, con la posibilidad de reconstruir una sesión TCP, mediante el flujo de datos analizado, rastreando la navegación que se genera desde la red[88].

E. ***Metasploit:*** este es un tipo de software que permite realizar pruebas de código de explotación tanto en un ambiente controlado, como en un servidor activo, siempre y cuando se esté seguro de lo que se va a realizar y los resultados que se buscan, es un software de código abierto fundamentalmente diseñado para el desarrollo avanzado de aplicaciones y sistemas, se podría decir que es uno de los softwares más populares para análisis de seguridad informática.

5.5.3.2 Hardware para ciberseguridad. El hardware es muy importante en lo relacionado con ciberseguridad, pues tanto el software como el hardware deben ser de muy buena calidad si lo que se busca es tener una excelente barrera de protección contra los ataques informáticos.

A. ***Routers:*** este equipo se encarga de realizar el enrutamiento del tráfico de la red en la que se encuentra, enviando paquetes a cada uno de los puertos y puestos de trabajo a los que se está conectado, existen varios modelos marcas, entre los

[88] Esaú A. Top 10 Aplicaciones de Seguridad. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://openwebinars.net/blog/top-10-aplicaciones-de-seguridad/

más sonados (Cisco, Huawei, Avaya, Asus, Linksys, Netgear, entre otros que son muy buenos) estos equipos prestan funciones tanto para el hogar, como para las grandes compañías, lo cual ya son equipos mucho más robustos y con una mejor estructura interna para el servicio que prestara, para que este equipo preste un buen servicio, adicional de la marca y características, se debe realizar una muy buena configuración, con el fin de que se garanticen las políticas de trasmisión de datos y seguridad de la información[89].

B. ***Firewalls:*** existen de diferentes tamaños, marcas, modelos, como por ejemplo, (Firewall DPI, Firewalls capa 3, Firewalls capa 7, entre otros) se configuran de diferentes maneras, se encuentran tanto en hardware como en software, y funcionan de la siguiente manera, son una barrera de seguridad, tanto en una red como en un equipo, bien sea pc o servidor, según sean las configuraciones que se le realicen, se podría decir que funciona como un guarda de seguridad, el cual se encuentra en el límite o división entre internet y el ingreso a la red de protección, esto, tomando como referencia un firewall físico, que realizara un análisis del tráfico y determina si lo deja pasar o simplemente lo bloquea, pues en caso de ver peticiones que no provengan de la red interna o del propio sistema restringe dicho tráfico, sea al interior o al exterior de la red, lo último con el fin de evitar la pérdida de datos[90].

C. **Servidores:** son equipos físicos o en Nube, los cuales se caracterizan por su alto flujo de trabajo, son equipos que permiten a una compañía poder almacenar, grandes cantidades de datos, si se habla de servidores de almacenamiento dentro de la infraestructura tecnológica, física o en la Nube, así mismo se tienen servidores de aplicaciones, existen otros que son para la virtualización, entre otras opciones que se pueden encontrar en el mercado, el valor depende de muchos factores, los núcleos por zócalo, capacidad de almacenamiento, diseño, unos pueden ser alojados en un rack o dentro de un gabinete, depende del fabricante, siendo distintos dependiendo de la marca, dentro de los fabricantes más importantes en el mercado, se tienen los siguientes, (Dell. IBM. Lenovo. Intel. Cisco. Microsoft. Oracle. Huawei, entre otros.) en la actualidad está en auge la adquisición de servidores en la nube, debido a la digitalización, el hardware está perdiendo terreno, así como la disminución de costos[91].

---

[89] INFORMATICA MODERNA. Routers Poe. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: http://www.informaticamoderna.com/Router.htm

[90] CIBERSEGURIDAD INDUSTRIAL BY LOGITEK. ¿Qué es un firewall industrial DPI (Deep Packet Inspection)? [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.ciberseguridadlogitek.com/que-es-un-firewall-industrial-dpi-deep-packet-inspection/

[91] NET CLOUD ENGINEERING. Servidor Cloud vs servidor local para empresas. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://openwebinars.net/blog/top-10-aplicaciones-de-seguridad/

5.6 MARCO CONTEXTUAL

5.6.1 Propiedades de los Csirt Internacionales. Para poder tener información más detallada de las propiedades de cada uno de los CSIRTs internacionales y los más importantes, los cuales fueron analizados por las investigadoras, Mirna Muñoz & Lizbeth Rivas, en su investigación, aportan información muy importante de los componentes internos de cada uno, para poder obtener similitudes o información que sirva como guía a los demás, en temas de operación, mejora, implementación, proyección, entre otros que son muy importantes a la hora de implementar un centro de atención a incidentes de seguridad[92].

Los CSIRTs y los CERT, se evidencia las propiedades de estos, así mismo permite ver la similitud en algunos puntos, en los cuales se puede apreciar que el CERT es quien tiene más propiedades que lo caracterizan, lo cual podría indicar que tienen una operación más completa y eficaz en relación con los demás, dicho lo anterior se podrá observa en la Tabla 2, los conceptos que determinan cada grupo de respuesta a incidentes de seguridad informática.

Tabla 2 Análisis de las propiedades de un CSIRT

Propiedades	CERT	CSIRT	CERT Nacional	CERT Militar
Contar con un fin definido	✓	✓	✓	✓
Definir cada uno de los servicios	✓	✓	✓	✓
Definir la audiencia	✓	✓	✓	✓
Estudio de la región	✓	✓		✓
Contar con la Misión	✓	✓	✓	✓
Contar con la Visión.	✓	✓	✓	✓
Tener la idoneidad de identificar los riesgos	✓	✓	✓	✓
Tener políticas	✓		✓	✓
Mejora de la calidad	✓			
Contar con oficinas		✓	✓	✓
Establecer coordinación	✓	✓	✓	✓
Manejan análisis financiero	✓	✓		
Personal calificado	✓	✓	✓	✓
Cooperación con otros CERT	✓	✓	✓	
Mejora continua	✓			

Fuente: CENTRO CRIPTOLÓGICO NACIONAL. (España). Principios y recomendaciones básicas en Ciberseguridad [En línea] (CCN-CERT BP/01) octubre 2017, [Consultado: 12 diciembre de 2019] P. 12-60. Disponible en: https://www.ucm.es/data/cont/media/www/pag-114974/CCN-CERT_BP_01.pdf

[92] MUÑOZ Mirna, RIVAS Lizbeth. Revista ibérica de sistemas y tecnologías de información. DOI: 10.17013/risti.e 3.1-15. [En línea] [Consulta: 12 abril de 2020] P. 10-15 Disponible en: http://www.scielo.mec.pt/pdf/rist/nspe3/nspe3a02.pdf

Las propiedades de los CERT y CSIRT, son muy importantes, porque de ellas depende la cantidad de servicios que podrán prestar a su grupo de clientes atendidos, así mismo se debe mencionar que aparte de sus propiedades, existen otros factores dentro de las estructuras de estos grupos, las cuales ayudarán a dar forma a cada uno de ellos, de esta manera se podrá proyectar cada equipo según las necesidades que pretendan alcanzar, se listarán algunos puntos importantes que se requieren para la implementación de cualquier grupo de atención a incidentes de seguridad, los cuales pueden ser una guía para futuros proyectos de creación de CSIRT, mantener la línea de implementación, según los estudios realizados son las propiedades que mayor aporte le generan al centro de atención a incidentes, como se observa en la Tabla 3,[93].

Tabla 3. Puntos clave de los CSIRT.

Punto Importante	Descripción
Visión	Proyección que tendrá el CSIRT.
Misión	El propósito al cual se orientará el CSIRT.
Región	Estudio de las necesidades y la delimitación según el lugar y la geografía que tendrá el CSIRT.
Financiamiento	Recursos económicos para financiar el CSIRT.
Gerencia	Líderes que orienten el CSIRT.
Productos	El portafolio que se ofrecerá.
Tipo organizacional	Capacidad del CSIRT según el modelo que se otorgue
Recursos	Adquisición de recursos en general para el CSIRT.

Fuente: Elaboración Propia.

[93] CENTRO CRIPTOLÓGICO NACIONAL. Óp. cit. P. 26

5.6.2 Modelos de los CERT y CSIRT. Adicional a las propiedades de los CERT y CSIRT, también se deben mencionar los modelos que maneja cada uno de estos equipos, son varios los que existen, entre los más populares están los modelos organizacionales. Son de suma importancia en cualquier estudio que se realice para la implementación de un CSIRT, de esta manera se podrá ir dando forma a la implementación que se pretende, siendo que ellos permitirán que se enfoque en uno de ellos y así poder tener una visión más acertada de lo que se requiere y pretende. Con el fin de tener una mejor clasificación de los CSIRTs, teniendo en cuanta la guía "creación de un CERT / CSIRT." Roldán Félix Sanz, existen modelos específicos que les ayuda a un grupo determinado de CSIRT, a mantenerse comunicados y así poder responder de manera oportuna a cada uno de los incidentes, estos modelos pueden ser los (Coordinados y los Centralizados), cada uno de ellos, ofrece un proceso diferente para la operación, dependiendo de los servicios que pretenda ofrecer, se podrá escoger el modelo que se ajuste a las necesidades, dependiendo del volumen de clientes que pueda tener, así como el mercado que manejen estos clientes, se logrará determinar cuáles servicios son los que más les favorece y cuáles son los que más se adaptan a esos mercados que maneja cada uno de los clientes del CSIRT[94].

5.6.3 Modelo Incrustado. Para la implementación de este modelo, es importante tener y contar con las infraestructuras listas y adecuadas, por lo que el CSIRT se crea dentro de la empresa ya existente, y utiliza el mismo departamento de sistemas ya existente de la empresa u organización, el Csirt, será dirigido por el jefe existente o uno nombrado para el nuevo cargo, siendo el encargado de llevar todas y cada una de las actividades del centro de respuesta a incidentes. Este nuevo líder debe contacta con los especialistas necesarios para atender y resolver todas las solicitudes de incidentes de seguridad que sean reportados, se podrá contar adicionalmente con una asistencia especializada adicional dentro de la empresa en caso de ser necesaria. Es un modelo que se puede adaptar con el fin de afrontar situaciones específicas a medida que surgen dentro de la atención de los incidentes, inicialmente el equipo de respuesta a incidentes, tendrá un número fijo de especialistas o técnicos, los cuales tendrán una jornada completa, el puesto seleccionado para la atención a los clientes o usuarios será un (abuse desk) en un ISP p. ej. es claramente un trabajo que se deberá realizar a jornada completa para una o más personas, según la necesidad de la operación, este modelo es muy popular en países como (Estados Unidos), (España), (Reino Unido) entre otros de Europa [95].

[94] CENTRO CRIPTOLÓGICO NACIONAL. Óp. cit. P. 7

[95] MODELO DE COORDINACIÓN y Atención de Emergencias en el ámbito de la Sociedad de la Información. [Anónimo] [En Línea] [Consultado: 12 de abril de 2020] P. 83-117 Disponible en: http://catai.net/blog/wp-content/uploads/2009/01/premioacademiacanariaseguridad.pdf

A. **Fortalezas:** No requiere de gastos cuantiosos para su puesta en marcha, permite a la organización, tener un apoyo oportuno en la atención de incidentes de segundad de la información, permitiendo mantener el control de la operación dentro de sus posibilidades.

B. **Debilidades:** No cuentan con la experiencia suficiente para afrontar situaciones de atención máxima, como un ataque tipo (APT), no cuenta con los aliados necesarios para soparte en temas relacionados, deben perfeccionar una línea de atención a incidentes hasta que lleguen a contar con la experiencia necesaria.

5.6.4 Modelo Organización Independiente. Este es un tipo de CSIRT o CERT de características de extendido, actuando como organización independiente, en el sentido, de que cuenta con sus propios directivos y empleados, se podría indicar que se trata de una organización o empresa que puede ser directamente financiada, por otro tipo de organizaciones que requieren estos servicios, o miembros de la comunidad a la que pertenecen, los cuales desean ampliar sus servicios a otras naciones o continentes, con el fin de fortalecer sus negocios de seguridad de la información, mediante la prestación de servicios de seguridad, a clientes que requieran dichos servicios, este tipo de centros de atención a incidentes de seguridad, son muy populares en Europa y Asia[96].

A. **Fortalezas:** Cuentan con recursos económicos constantemente, para poder implementar sistemas que mejoren la seguridad de su grupo de clientes o usuarios, así como también cuentan con la posibilidad de tener personal altamente competitivo en sus funciones.

B. **Debilidades:** cambios constantes por la metodología de negocio, pues deben atender diferentes clientes en diferentes partes del mundo, lo cual implica un mayor consumo de recursos tecnológicos y humanos, los cuales deben estar constantemente actualizados para lograr satisfacer las necesidades de los clientes, Ejemplo el Idioma entre otros.

[96] CENTRO CRIPTOLÓGICO NACIONAL. Óp. cit. P. 21

5.6.5 Modelo campus. Los CSIRT de estos modelos son muy típicos en los sistemas educativos de los países, los centros académicos que cuentan con estos modelos, para la atención de sus incidentes de seguridad, se caracterizan por tener instituciones educativas en diferentes regiones de los países donde se encuentran instalados, incluso podrían prestar servicios a instituciones con sedes en diferentes partes del planeta, no solo prestan servicios a instituciones educativas, sino que también a centros de investigación y campus, En este modelo se puede representar la existencia de una sede central y muchas sedes distribuidas con una cierta independencia de un CSIRT principal, debido a que estos cuentan con uno o varios Csirts más pequeños dependientes del primero. Este modelo es ideal para grandes organizaciones, con elevada descentralización, como por ejemplo en una institución educativa con numerosas sedes tanto en el mismo país, como fuera de él. Estos equipos de seguridad principales suelen proporcionar los servicios claves además de distribuir información muy importante sobre incidencias a los demás equipos del campus, de esta manera logran reducir esfuerzos y costos generales. Este tipo de modelo no se conoce en Colombia, es popular en los Estados Unidos y Europa[97].

A. **Fortalezas:** Gran capacidad de respuesta cuenta con grandes sistemas de información y tecnología que le permite a sus clientes o usuarios tener respuestas rápidas y oportunas.

B. **Debilidades:** Solo está enfocado en instituciones grandes, de gran reconocimiento tanto en lo general como en lo académico, la necesidad de recursos y presupuesto es de gran tamaño, con el fin de mantener operación.

5.6.6 Modelo voluntario. Este tipo de CSIRT o modelos, son muy populares, al tratarse de un proyecto desarrollado por un grupo de la comunidad o de expertos en la materia de seguridad informática y atención de incidentes de seguridad. Este modelo consta de (especialistas) que se juntan para proporcionar consejos y apoyo mutuo a la misma comunidad, de manera voluntaria. Es una comunidad o grupo de personas que depende en gran medida de la motivación de sí mismos y entrega de los demás participantes, se dice que Las redes WARP son un ejemplo de este modelo, popular en Europa, Estados Unidos y parte de Asia.

A. **Fortalezas:** Es fácil de implementar ya que no se requiere de grandes cantidades de dinero, pues parte de la mano de obra y asesoría no tienen costo, así mismo cuenta con el reconocimiento de expertos en la materia, lo cual puede ser de gran provecho para la experiencia de los miembros del equipo.

[97] MODELO DE COORDINACIÓN. Óp. cit. P. 84

B. **Debilidades:** Puede presentar problemas de organización, ya que, no cuenta con un líder sólido y libre, al tener tantas opiniones divididas puede que no se logren tomar decisiones conjuntas que le favorezcan.

5.6.7 Modelo Coordinador. Como su palara lo indica, se trata de un modelo de CSIRT. Que trabaja con otros CSIRTs diferentes, donde su rol primordial es la asesoría a equipos de otras entidades u organizaciones, proporcionando información muy importante y relevante que sea de gran ayuda, es de aclarar que, sobre estos otros grupos o equipos, necesariamente no se debe o llega a ejercen ningún tipo de autoridad directa. Por lo que se dice que su función principal es proporcionar análisis importante, relacionado principalmente con la gestión de incidentes y de vulnerabilidades, siendo así como se logra establecer, de una manera adecuada, una gran fuente de información y soporte como también algunos servicios de coordinación, realmente son equipos que garantizan y proporcionan diferentes fuentes de apoyo informativo y alertas, de gran reconocimiento e importante despliegue a los demás equipos, por lo que también, se establecen apoyos documentales, como lo son algunas guías de información relevantes, se puede indicar que adicionalmente los boletines son una fuente importante de información a la hora de establecer canales informativos entre sí, para destacar se proporciona una cooperación en el compartir de información, de sus mejores prácticas, alertas de ataques y vulnerabilidades. Este modelo es muy popular en distintos países de Europa, América latina, América del norte, entre otros[98].

A. **Fortalezas:** Es un gran referente para otros equipos de respuesta CSIRT, lo que le permite tener reconocimiento y respeto en la materia, son equipos de gran tamaño, que por su estructura cuentan con importantes sistemas de información que garantizan seguridad.

B. **Debilidades:** Se focaliza más en las recomendaciones que en las acciones. Son equipos para organizaciones de gran tamaño, dejando de lado las pequeñas organizaciones que también requiere de sus servicios.

[98] EINAR LANFRANCO Lic y PÉREZ ESTÉVEZ Ernesto ¿De qué se trata?, modelos posibles, servicios y herramientas. [En línea] Colombia: [Consulta: 12 de octubre de 2019] P. 18. Disponible en: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

5.6.8 Modelo Distribuido. Este modelo de CSIRT, costa de varios equipos de respuesta a incidentes de seguridad informática, (según tipo de incidentes, áreas dentro de la organización o áreas geográficas), varios equipos conforman el CSIRT, por lo que se denomina distribuido, ya que, de varios lugares geográficamente, se realizan los reportes de dichos incidentes, a simple vista se podría decir que tiene que ver mucho con el CSIRT centralizado, pero no lo es, por lo que se entiende que el equipo distribuido es una organización con una estructura más pequeña en la atención de incidentes, se destaca la coordinación para garantizar la consistencia del servicio de respuesta a incidentes, El personal del equipo del CSIRT, está distribuido de manera previamente existente dentro de la misma organización, por lo que solo se le asignaran estrictamente responsabilidades explicitas con relación a seguridad, a las cuales deberá dedicar tiempo parcial o total a la atención de los incidentes asignados, dependiendo de su nivel de requerimiento, se dice que este modelo se puede adecuar muy bien a organizaciones grandes[99].

A. Fortalezas: fácil de manejar, no requiere de muchos recursos económicos, debido a que ya cuenta con las instalaciones, pues es la misma empresa quien lo ejecuta, cuenta con el personal de la misma organización, así mismo está enfocado solamente en la organización que lo implementa y en ocasiones a distintos clientes pequeños a los cuales ofrece sus servicios.

B. Debilidades: Carece de experiencia en la atención de incidentes de seguridad por tanto los miembros del equipo no son lo suficientemente capacitados, teniendo en cuenta que son los mismos miembros del equipo de sistemas de la organización que lo implementa.

[99] CAROZO Eduardo. Et al. Análisis del Desarrollo de un Centro de Respuesta Nacional para la República Oriental del Uruguay. [En Línea] Universidad de Montevideo [Consulta: 12 de octubre 2019] P. 1-23. Disponible en: http://revistas.um.edu.uy/index.php/ingenieria/article/view/264/323

5.6.9 Modelo Centralizado. Este tipo de CSIRT son muy populares en todo el mundo, en lo general son los equipos que representan a un país, en relación con el manejo de los incidentes de seguridad, este es un único equipo de respuesta a incidentes que se encarga del manejo de todos los incidentes relevantes, que son escalados por los demás CSIRT. Podría decirse que en Colombia este puesto le corresponde al (colCERT y el SOC-CCOC) los cuales son los puntos centrales en la recopilación de incidentes de seguridad de relevancia o infraestructura critica, en el país, estos CSIRT son adecuados para organizaciones de gran jerarquía, es decir para organizaciones mocho más grandes cuya infraestructura tecnológica no se encuentre en sitios geográficamente distantes. Este equipo de respuesta centralizado es el único punto de contacto en toda la organización o país que los utiliza para la respuesta a incidentes informáticos, vulnerabilidades y reportes de ciberseguridad[100].

A. Fortalezas: Poseen gran conocimiento en materia de seguridad de la información y experiencia en atención a incidentes de ciberseguridad.

B. Debilidades: Son los directos responsables en los países donde funcionan como equipos de referencia a los demás de manera local, siendo los encargados de la solución de los incidentes de ciberseguridad e infraestructura critica que los demás no logran dar respuesta.

Con la explicación de los modelos anteriores de los diferentes CSIRTs, según las clasificaciones de cada uno de ellos, se podrá observar un esquema general, de los modelos ya explicados en los párrafos anteriores, de modelos organizacionales representados en la Figura 14.

[100] EINAR. Óp. cit. P. 11

Figura 14. Modelos organizacionales de los CSIRTs

Fuente: MUÑOZ Mirna, RIVAS Lizbeth. Revista ibérica de sistemas y tecnologías de información. DOI: 10.17013/risti. 3.1-15. [En línea] [Consulta: 12 abril de 2020] Disponible en: http://www.scielo.mec.pt/pdf/rist/nspe3/nspe3a02.pdf

5.7 MARCO LEGAL

5.7.1 Ley 527 de 1999. “Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales”[101].

5.7.2 Ley 599 del 2000. “Por la cual se expide el código penal colombiano”[102].

[101] COLOMBIA, CONGRESO DE LA REPUBLICA, LEY 527 de 1999. comercio electrónico y de las firmas digitales. (21 de agosto de 1999) Diario Oficial No. 43.673. [En Línea] [Consulta: 12 de octubre de 2019] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html
[102] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599. Óp. cit., p. 1.

5.7.3 Ley Estatutaria 1266 de 2008. “Por la cual se dictan una serie de disposiciones legales y generales, hábeas data”[103].

5.7.4 Ley 1273 de 2009. “Por la cual se le hacen modificaciones importantes al código penal, con el fin de incorporar el mecanismo de justicia más importante en la historia de Colombia, en temas de ciberseguridad y las comunicaciones”[104].

5.7.5 Ley 1341 de 2009. “Por la cual se determinó todos los requerimientos necesarios sobre la información informática y el ministerio de las TIC”[105].

5.7.6 Ley Estatutaria 1581 de 2012. “Por la cual se dan disposiciones específicas y general para la protección de datos personales de personas y entidades”[106].

5.7.7 Ley 1712 de 2014. “Transparencia y del Derecho de Acceso a la Información Pública”[107].

5.7.8 Decreto presidencial 1081 del 2015. “por el cual se reglamenta el acceso a la información pública”[108].

5.7.9 Directiva NIS (UE) 2016/1148. Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea[109].

5.7.10 Reglamento (UE) 2019/881. “Reglamento sobre la Ciberseguridad” del Reglamento Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) No 526/2013[110].

---

[103] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Op. cit.
[104] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Op. cit.
[105] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341 Op. cit.
[106] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley Estatutaria 1581. Op. cit.
[107] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1712 Op. cit.
[108] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto Número 1081. [En Línea] (mayo 26 de 2015) Bogotá. D.C. [Consulta: 12 de octubre de 2019] Disponible en: http://es.presidencia.gov.co/normativa/normativa/Decreto-1081-2015.pdf
[109] BÉLGICA UNIÓN EUROPEA. directiva (UE) 2016/1148 del parlamento europeo y del consejo. Diario Oficial de la Unión Europea. [En Línea] de 6 de julio de 2016. [Consulta: 12 de octubre de 2019] P. 1-30. Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf
[110] BÉLGICA. UNIÓN EUROPEA. Op. cit., 1.

6 DISEÑO METODOLÓGICO

6.1 ESTUDIO METODOLÓGICO

El estudio metodológico estará fundado en una investigación cualitativa, realizando una observación de las áreas de internes, y así obtener la información necesaria de la población tomada.

6.2 ENFOQUE METODOLÓGICO

El enfoque que se le dará a la investigación realizada, del presente proyecto de estudio, es de tipo aplicada, de esta manera se podrá dar a conocer los principales instrumentos documentales que requiere el proyecto de investigación, de la empresa Cibersecurity de Colombia LTDA, con el fin de implementar mediante el diseño documental, para el Equipo de Respuesta ante Incidencias de Seguridad Informáticas CSIRT.

El área general de conocimiento del proyecto está enfocada en la gestión de seguridad informática.

El área específica del conocimiento del proyecto está enfocada directamente en la atención de incidentes de seguridad de la información.

6.3 POBLACIÓN Y MUESTRA

Se determina que la población donde se tomará la muestra es el personal que labora y conforma la empresa Cibersecurity de Colombia LTDA., determinando que se tomará como muestra de esta población el 100% de los empleados, un total de 17 empleados, los cuales están distribuidos en los siguientes cargos.

A. Director de tecnología, cantidad de personas 1.

B. Subdirector de tecnología, cantidad de personas 1.

C. Jefe de operaciones, cantidad de personas 1.

D. Jefe de infraestructura, cantidad de personas 1.

E. Jefe de ciberseguridad, cantidad de personas 1.

F. Especialista Voz IP y Telefonía Móvil, cantidad de personas 1.

G. Especialista Infraestructura y Redes, cantidad de personas 1.

H. Especialista SO - Linux - UNIX – Windows, cantidad de personas 1.

I. Especialista en Ciberseguridad, cantidad de personas 3.

J. Analistas, cantidad de personas 6.

6.3.1 Fuentes de información. Las fuentes de información tomadas para la recolección de esta se describirán en una primaria y una secundaria, las cuales se relacionan de la siguiente manera, en los siguientes puntos.

A. **Fuente de información primaria:** como fuente de información primara, para la elaboración y desarrollo de la presente investigación, se tomó las fuentes de información suministradas por los empleados de la dirección de tecnología de la empresa Cibersecurity de Colombia LTDA., los cuales durante su trayectoria en las funciones que desarrollan diariamente en las instalaciones de la compañía en el área de sistemas de información y seguridad informática, producto de las actividades diarias de su cargo y desempeño laboral.

B. **Fuente de información secundaria:** documentación mediante referente bibliográfica que permita identificar la manera correcta del diseño documental para la implementación de un Equipo de Respuesta ante Incidencias de Seguridad Informáticas CSIRT.

6.3.2 Recolección de información. Para la recolección de dicha información, se deberán utilizan técnicas como la observación, dentro de las instalaciones de la empresa Cibersecurity de Colombia LTDA., con el fin de registrar los patrones de conducta de los usuarios y funcionarios, que hacen parte de la dirección de tecnología y cada una de sus áreas, adicionalmente se realiza la entrevista no estructurada o diálogo con el personal, de esta manera se obtendrán datos más precisos y actualizados, siendo esta una forma eficiente de obtener la información de primera mano, de quienes la procesan a diario en el actuar de sus funciones relacionadas con la seguridad Informática, atención a incidentes de seguridad y ciberseguridad.

6.4 FASES DE TRABAJO

Las fases se establecerán en función de los objetivos para la implementación del proyecto, estudio documental, para la creación del centro de respuesta a incidentes CSIRT para caso de estudio “escenario administrativo” Cibersecurity de Colombia Ltda.

6.4.1 Fase 1. Estructurar la información, para determinar las necesidades del CSIRT, como los servicios, según la oferta y la clasificación que se utilizará.

Actividad 1: Realizar una estructura interna del CSIRT. Mediante organigrama.
Actividad 2: La elaboración de la Misión y Visión del CSIRT.
Actividad 3: Elaboración del plan comercial del equipo de respuesta a incidentes de seguridad.
Actividad 4: Realizar un plan estratégico del CSIRT, mediante el apoyo y cooperación de aliados estratégicos nacionales e internacionales, dando solución a las necesidades del Equipo de Respuesta ante Incidencias de Seguridad Informáticas.
Actividad 5: Se establecieron las políticas internas del CSIRT, dando forma y seguimiento a las actividades diarias con el fin de tener control de cada uno de sus procesos.

6.4.2 Fase 2. Analizar modelos aplicados a los CSIRT, en los países vecinos con el fin de seguir una metodología Coherente.

Actividad 1: Análisis de los diferentes modelos de los Equipos de Respuesta ante Incidencias de Seguridad Informáticas.
Actividad 2: Descripción de los principales CSIRT en los países vecinos.

6.4.3 Fase 3. Diseñar un tratamiento de atención y seguimiento de incidentes de seguridad.

Actividad 1: Establecer un tratamiento adecuado para la atención de incidentes de seguridad.
Actividad 2: Indicar el ciclo de vida a cada uno de los incidentes de seguridad.

6.4.4 Fase 4. Definir los perfiles del equipo de trabajo, así como sus funciones, dando un esquema general del organigrama del equipo del CSIRT.

Actividad 1: Realizar de definición de los perfiles de cada uno de los funcionarios del equipo.
Actividad 2: Establecer las funciones de cada integrante del grupo.
Actividad 3: establecer el organigrama del equipo.

7 SERVICIOS QUE PRESTAR Y NECESIDADES DEL CSIRT

En el presente capítulo se establecerán puntos importantes que se requieren en la estructuración documental del CSIRT, se debe establecer una estructura que le permita al CSIRT, poder darse a conocer, un punto importante es el desarrollo de los servicios ofertados al interior de la compañía Cibersecurity de Colombia LTDA. Y sus potenciales clientes, se debe establecer un plan comercial, dentro del cual se indican dichos servicios que se prestaran o se ofertaran, los cuales están compuestos desde los reactivos y proactivos, adicionalmente se han establecidos unos servicios forenses, los cuales serán ofertados a los clientes que los requieran, se han indicado las necesidades que el CSIRT requiere para su funcionamiento, los cuales se componen, con lo anteriormente dicho, que es el plan comercial, las alianzas con otros actores importantes relacionados con seguridad informática, nacionales e internacionales, con los cuales se debe tener algún tipo de contacto, estableciendo aliados en la lucha contra la atención a incidentes de seguridad y ciberseguridad, finalmente se establecieron políticas de seguridad, las cuales serán de gran aporte al CSIRT, en los procesos que se adelantaran internamente y externamente.

7.1 DESARROLLO DEL PLAN COMERCIAL.

Toda organización de ciberseguridad, que pretenda incursionar en el mercado de la atención a incidentes de seguridad informática, debe tener dentro de sus instrumentos comerciales un proceso de servicios o plan comercial, el cual servirá como guía o listado de servicios que los clientes podrán ver como ofertados, el CSIRT debe tener claro cuál será su plan de servicios que prestará, dicho lo anterior, esto le permitirá tener objetivos más claros, a la hora de preparar sus proyectos comerciales y de infraestructura, permitiéndole obtener un posicionamiento en el mercado, por lo que dependiendo de este plan, junto con la oferta comercial, se podrá determinar los servicios a prestar, junto con el grupo de clientes internos como externos, que puedan ser atendidos mediante los servicios que se ofertaran, a cualquier entidad u organización que los requiera contratar, que se encuentre dentro de los clientes a los cuales van dirigidos este paquete de servicios, principalmente para la compañía Cibersecurity de Colombia LTDA., así como las medianas y pequeñas Pymes del país, en vista, de que la demanda es muy grande en cuanto a los servicios solicitados por parte de los potenciales clientes que se puedan conseguir, se debe indicar, que es muy difícil que se presten todos los servicios de ciber seguridad por parte de un solo CSIRT, de ahí que, como lo indica ENISA, “Son muchos los servicios que un CSIRT puede prestar, pero en la actualidad, ningún CSIRT o CERT los presta todos, dado lo anterior se debe estudiar muy bien la población a la cual van dirigidos y tener información

detallada de las necesidades que esta población requiere en lo relacionado con la atención de incidentes de seguridad Informática y ciberseguridad[111].

Es necesario recalcar, que la empresa Cibersecurity de Colombia LTDA., mediante el estudio documental, para la creación de un CSIRT, prestara los siguientes servicios dentro de su oferta comercial, los cuales están relacionados con un paquete de servicios, que se ofrecerá según los siguientes puntos donde se detalla uno a uno, con el fin de indicar, los servicios que se prestaran por parte del CSIRT, los cuales son los servicios básicos y un valor agregado en los servicios de Informática forense, siendo un poco más específicos, los servicios que inicialmente se prestaran son los que tienen que ver con los reactivos, en la parte de monitoreo de plataformas, y todo lo que se requiera según lo necesiten los clientes, así como el análisis de incidentes y la atención de los mismos, se puede avanzar con el tiempo en los siguientes servicios que se tiene planeado ofertar, como son los proactivos y los de informática forense, todo como resulte la puesta en marcha de los primeros pilotos de atención a incidentes de los servicios reactivos.

7.1.1 Servicios reactivos. Este tipo de servicios están enfocados principalmente para responder a solicitudes de asistencia, reportes de incidentes, comunicaciones de incidentes atendidos por el CSIRT, como cualquier ataque o amenaza que llegase a presentarse en contra de los sistemas del cliente al cual se está prestando los servicios. Este tipo de servicios también se pueden determinar mediante la gestión de vulnerabilidades, la gestión de código malicioso, pruebas de calidad del software, reportes y recomendaciones, asesoría y atención a usuarios, tratamiento de incidentes, etc. Algunos de estos servicios se pueden iniciar mediante un importante monitoreo o por los seguimientos y registros de los sistemas, en los logs de eventos, como también las alertas, otra opción puede ser las notificaciones de terceras partes, entre otros mecanismos de alertas tempranas que se puedan implementar en los sistemas a proteger[112].

[111] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. Óp. cit., P. 12
[112] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. Óp. cit., P. 69

7.1.2 Servicios Proactivos. En seguridad Informática, se puede decir que uno de los principales objetivos de los servicios Proactivos, es el análisis de la información, la cual es recolectada en diferentes actividades, como la lectura de información, mediante correo electrónico, blogs, noticias, artículos, páginas web de seguridad Informática, entre otros medios, adicional podemos indicar, los procesos de mejora de la infraestructura y la calidad de servicios prestados a los clientes, lo anterior con el fin de que sean prevenidos antes de que en sus sistemas ocurra un incidente o evento de seguridad Informática, por lo que se les alerta sobre vulnerabilidades, técnicas de ataques o virus informáticos entre otras, dando una posición de seguridad preventiva ante la ocurrencia de cualquier vulnerabilidad de seguridad Informática, que pueda ser explotada por un atacante, los cuales posiblemente en varias ocasiones no podrán ser detectados por las firmas de antivirus o por los software especializado para tal fin, siendo esta una excelente opción para evitar los posibles incidentes de seguridad Informática que se puedan presentar[113].

7.1.3 Servicios de Informática forense. Este servicio de Informática Forense, se puede definir como la ciencia de descubrir, preservar, resguardar, obtener, amparar, presentar, etc. a través de un conjunto de dispositivos y aplicaciones especializadas que permiten, que todos, estos datos que hayan sido procesados en alguna ocasión electrónicamente y almacenados en cualquier tipo dispositivo de almacenamiento informático, de una manera adecuada en un proceso penal, permitiendo que estos sean válidos dentro de un proceso legal o de investigación. Logrando dar una solución tecnológica a los clientes que requieran dichos servicios ofertados, en la gestión de incidentes de seguridad Informática[114].

Dado lo anterior es de suma importancia dar a conocer el portafolio de servicios que el CSIRT ofertara a sus clientes, dentro de su plan comercial, indicando a detalle cada uno de los servicios que se ofertaran, dentro de la matriz comercial, se categorizan de la siguiente manera, Servicios que van desde los Reactivos, hasta los Proactivos, así como también encontramos otro tipo de servicios, que sean muy prometedores dentro del plan comercial que se ofertara, se trata de los servicios “de valor añadido” o que también se darán a conocer con el nombre de “Informática Forense” los cuales están incluidos dentro del paquete de servicios que el Csirt ofertará a sus potenciales clientes, según el Cuadro 1 describe detalladamente uno a uno.

[113] POLICÍA NACIONAL DE COLOMBIA. cc-csirt. [Sitio Web] servicios-proactivos. [Consulta: 12 abril de 2020] Disponible en: https://cc-csirt.policia.gov.co/servicios/servicios-proactivos

[114] INTERNET SECURITY AUDITORS. Informática Forense y Peritajes. [Sitio Web]. 2020. Bogotá D.C. [Consulta: 12 abril de 2020] Disponible en: https://www.isecauditors.com/informatica-forense-peritajes

Cuadro 1. Tipos de servicios ofertados.

Reactivos	Proactivos	Informática forense
1. Tipos de Alertas y advertencias que se presenten vulnerabilidades e incidentes totales. 2. Tratamiento de los incidentes de seguridad. 3. Análisis de incidentes. 4. Respuesta a incidentes en sitio y remoto. 5. Apoyo a la respuesta a incidentes. 6. Coordinación de la respuesta a incidentes. 7. Tratamiento de vulnerabilidades. 8. Análisis de vulnerabilidades. 9. Respuesta a vulnerabilidades. 10. Coordinación de la respuesta a la vulnerabilidad. 11. Asistencia remota a incidentes.	1. Comunicados y anuncios. 2. Observatorio de tecnología. 3. Evaluaciones o auditorías de la seguridad. 4. Desarrollo de herramientas de seguridad. 5. Servicios de detección de intrusos. 6. Difusión de información. relacionada con la seguridad. 7. Programas de gestión de listas de configuración segura de sistemas TIC. 8. Monitorización de redes.	1. Análisis forense. 2. Análisis de información. 3. Recuperación de datos. 4. Borrado seguro. 5. Análisis forense de la imagen. 6. Recuperación de datos. 7. Diagnostico preliminar de la evidencia digital. 8. Tomas de imágenes de Discos duros. 9. Análisis e informe de evidencia recolectada. 10. Recolección y preservación de evidencias.

Fuente: Elaboración propia.

Dentro de los compromisos estratégicos, se debe garantizar, el cumplimiento de los objetivos en los escenarios propuestos por los clientes, dando garantías en sus infraestructuras, dado que siempre se debe preservar la total integridad de sus activos, según corresponda a lo ofertado, implementando soluciones que contribuyan al Core del negocio, con el fin de que las operaciones funcionen de una manera adecuada y optima, según lo acordado en la adquisición de los paquetes que se le ofertaron a los clientes. Es importante que se genere un sentido de pertenencia en los empleados con el fin de que realicen su trabajo de manera dinámica, comprometida, proactiva, para que los resultados sean los deseados, dado que si se logra generar compromisos por parte del recurso humano involucrado en la atención de los incidentes y demás servicios, junto con la aplicación de un plan de mejora continua, según aplique, se lograran los objetivos y se cumplirá con los propósitos por el CSIRT en su Misión y Visión, de esta manera

contaremos con clientes satisfechos, empleados comprometidos y dispuestos a dar lo mejor de sí, para que se cumpla con las exigencias del negocio[115].

7.2 PLAN ESTRATÉGICO

7.2.1 Socios Estratégicos para el CSIRT. Dentro del plan estratégico es muy importante tener claras las ideas y la proyección que se dará al CSIRT, teniendo en cuenta que de este depende su futuro, como lo es también mantener buenas relaciones con CSIRT/CERT locales e internacionales, tal como lo indica Mindefensa en su presentación en 2019, donde se hace recomendación de crear alianzas que fortalezcan la cooperación, estos socios estratégicos deben ser entidades reconocidas del país, Fiscalía General de la Nacional, Policía Nacional, Fuerzas Armadas, los sectores de telecomunicaciones, las universidades, los centros de investigación, Etc. Los cuales puedan aportar información y experiencia, tanto en la atención a incidentes de seguridad Informática, como también en nuevas amenazas, nuevos controles, estrategias, entre otros, dichas estrategias serán de suma importancia, principalmente en un punto estratégico e importante para el país, el cual corresponde a la infraestructura critica, por lo que teniendo en cuanta el último informe del colCERT referente a “La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio” para el año 2019, la infraestructura crítica, fue una de las más atacadas en el país, expresado lo anterior, será de gran ayuda al centro de incidentes de seguridad Informática, con el fin de que se consolide según sus objetivos., en la Tabla 4, se puede observar la relación de socios que se debe tener, en el radar, en cuanto a socios estratégicos, con el fin de que el CSIRT sea mucho más competitivo, para sus socios estratégicos, usuarios, clientes y el interés interno del mismo[116].

Tabla 4. Socios esenciales para un CSIRT

[115] HERNÁNDEZ José Carlos. Universidad de Granada. Estrategias nacionales de ciberseguridad en américa latina [En Línea] (España). ISSN: 2340-8421. 2018. [Consulta: 25 de abril de 2020] Disponible en: https://global-strategy.org/estrategias-nacionales-de-ciberseguridad-en-america-latina/

[116] A Wilson y PRIETO h. Mindefensa colCER. Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT. La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio” [En Línea] Colombia 2019. [Consulta: 12 de octubre de 2019] P. 18-24 Disponible en: https://web.certicamara.com/files/eventos/CiberseguridadCiberdefensaColombia.pdf

Socios esenciales para un CSIRT

1.	CSIRT Nacionales
2.	CSIRT Internacionales
3.	Policía Nacional
4.	Fiscalía Nacional
5.	Ministerios, en especial Min Tic y Defensa
6.	Proveedores de internet o ISP
7.	Proveedores de software
8.	Proveedores de Antivirus
9.	Expertos en seguridad de diferentes sectores
10.	Universidades nacionales e internacionales
11.	Medios de comunicación especializados
12.	Proveedores de infraestructura crítica: como luz, alcantarillado, agua.

Fuente: Elaboración propia.

7.2.2 Cooperación Internacional. Dentro del plan de cooperación nacional e internacional de los CSIRT ya implementados, según, la organización de los estados americanos, en el "2004 los Estados Miembros de la OEA aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética", en donde se puede destacar la atención de los temas de seguridad, siendo una buena fuente de información, por lo que se pueden despejar varios escenarios de dudas y desconocimiento del procedimiento que se debe realizar, es importante contar con los enlaces o contactos de estos centros de información, bien sea de comunicación directa o indirecta como las fuentes que se publican mediante sus reportes e informes estadísticos, otra medida importante a tener en cuenta es el plan de capacitación, siendo de suma importancia, su fortalecimiento, mediante las visitas a otros centros de atención de incidentes, a fin de que los integrantes del grupo se familiaricen con las funciones y responsabilidades dentro del campo de ciberseguridad que allí se manejen, con el acompañamiento de expertos que les indiquen los procesos y mejores prácticas para ser implementadas en el CSIRT de la compañía Cibersecurity de Colombia LTDA.[117].

Para el mes de octubre del año anterior (2019). Se llevó a cabo reunión académica entre el Ministerio de Tecnologías de la Información y las Comunicaciones y entidades invitadas, entre ellas la embajada de los Estados Unidos de América en Colombia, donde expertos norteamericanos capacitaron a servidores públicos del país en protección de datos, diseño de servicios digitales, gestión de espectro,

[117] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. Óp. cit., P. 11.

tecnologías 5G y ciberseguridad, logrando un importante intercambio de información, fundamental para la lucha contra la ciberdelincuencia en el país, uno de los puntos principales de esta reunión fue el fortalecimiento de la infraestructura critica del país, la cual ha sido fuertemente atacada en los últimos años, según los reportes realizados por el colCERT mediante, La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio Colombia 2019". La preocupación de Colombia frente al tema es la "economía", por lo que estos ataques a la infraestructura critica le afectan directamente, afirmo la ministra, (Sylvia Constaín) otros temas que también tuvieron mucha importancia fueron Política de Datos, la Economía Digital y despliegue de tecnología 5G[118].

7.3 NECESIDADES

Las necesidades básicas o principales del Equipo de Respuesta ante Incidencias de Seguridad Informáticas CSIRT, son prácticamente las que se han venido relacionando en cada uno de los capítulos.

7.3.1 Necesidades de infraestructura física. Dentro de las necesidades de infraestructura del CSIRT, se requiere que se adecuen los espacios necesarios, con los ambientes adecuados, para que tanto los equipos de trabajo humano, como todo el hardware que se requiera, cuente con la seguridad, protección y comodidad necesaria para su correcto funcionamiento dentro de la empresa Cibersecurity de Colombia LTDA., de modo que se deben realizar los estudios necesarios para dicha organización de espacios y adecuaciones de lo relacionado.

7.3.2 Necesidades de capacitación. El CSIRT, requiere que se tenga un grupo de especialistas que garanticen la capacitación constante, tanto de los miembros del equipo, como de los mismos usuarios, estos también requieren de conocimientos esenciales, como por ejemplo la manera correcta de realizar el reporte de los incidentes de seguridad.

[118] EMBAJADA DE ESTADOS UNIDOS EN COLOMBIA. Expertos de EE. UU. [Sitio Web] fortalecen capacidades de funcionarios en ciberseguridad y diseño de servicios digitales. 2019. [Consulta: 27 de Abril de 2020] Disponible en: https://co.usembassy.gov/es/expertos-de-ee-uu-fortalecen-capacidades-de-funcionarios-en-ciberseguridad-y-diseno-de-servicios-digitales/

7.3.3 Necesidad de vigilancia. se requiere que el CSIRT cuente con la vigilancia tanto física como de video, las 24 horas los 365 días al año, ya que es de suma importancia mantener el control total de todos los lugares físicos que corresponden al CSIRT.

7.3.4 Necesidades de talento humano. Dentro de los requerimientos de los perfiles necesarios del equipo de funcionarios, para la atención, gestión, desarrollo, y respuesta a incidentes de seguridad de la información, se requiere tener pleno conocimiento de los tipos de incidentes a los que se deberá enfocar el personal de analistas y especialistas, por lo que depende de las necesidades del grupo de clientes a tendidos y los usuarios internos de la empresa Cibersecurity de Colombia LTDA., de esta manera se logrará entender el enfoque que se debe tener para la atención de estos incidentes y así contratar personas humano, con las capacidades, conocimientos y destrezas en la atención según el tipo de incidentes atendidos.

7.3.5 Necesidades de subcontratación. Se requiere la subcontratación de servicios, en caso de que estos sean necesarios, como por ejemplo los servicios Administración de los sistemas de información, con el fin de que haya una completa claridad en los procesos y políticas internas, así como la destrucción de información confidencial, luego de cumplir su siclo de vida.

7.3.6 Necesidades del grupo de clientes atendido. Es importante realizar las verificaciones necesarias que correspondan, en cuanto a las necesidades del grupo de clientes atendidos y los usuarios internos de la empresa Cibersecurity de Colombia LTDA., identificando los factores más importantes a los que se enfrenta el CSIRT, de esta manera se lograra establecer, las necesidades de los clientes, en cuanto a atención de incidentes de seguridad, capacitación, organización, mejoramiento de infraestructura tecnológica interna del cliente, de esta manera se lograran desarrollar las demás necesidades del mismo CSIRT y enfocar so propósito en pro de la función que se requiera, para solventar las necesidades de su grupo de clientes.

7.3.7 Necesidad de la estructura del equipo de trabajo. Para establecer el equipo como estructura, es necesario del talento humano, según el grupo de trabajo, saber cuáles son las necesidades de los clientes, de esta manera se podrá establecer la estructura, sin embargo, se realizará una según los servicios que se ofertaran, para ver la estructura remítase al Capítulo 10.

7.3.8 Necesidad de hardware y software. Para lograr establecerla, se requiere conocer varios puntos en específico los siguientes, las instalaciones, el grupo de talento humano, junto con la cantidad contratada, el enfoque del CSIRT, el grupo de clientes atendidos, las necesidades del grupo de clientes atendidos y el presupuesto con el que cuenta la empresa Cibersecurity de Colombia LTDA., de esta manera se podrá tener un estimado de los requisitos de hardware y software, que se requieren para el funcionamiento del CSIRT, en este proyecto, no se establecerán los detalles de las marcas, cantidades, funciones y demás relacionados para el hardware y software, los cuales se dejaron estipulados en las limitaciones, pero a modo de ejemplo se puede indicar, que se requeriría la cantidad de hardware, según la cantidad de personal contratado y demás necesidades que tenga el CSIRT, así mismo el software, de monitoreo, gestión, protección Etc.

7.3.9 Necesidad de procesos y procedimientos. Con el fin de solventar esta necesidad, es de suma importancia, establecer, políticas, procesos, reglas Etc. Todo con fin de que se maneje un cronograma de aplicación de procesos y estándares dentro de la operación, de esta manera garantizando que se cumpla con lo estipulado en los diferentes manuales de procedimientos y procesos, así como las políticas que se deben establecer, con el fin de evitar fallos al interior.

7.3.10 Necesidades adicionales de otras áreas. Cuando se refiere a otras áreas, es necesario hacer claridad, que se necesita de apoyo adicional, como por ejemplo la parte (Jurídica), siendo de gran importancia y ayuda en la atención y respuesta de incidentes que puedan estar comprometidos con algún aspecto legal luego de su respuesta o solución, este apoyo debe ser permanente, pues muchos de los incidentes pueden terminar en demandas y procesos legales, los cuales deben ser asumidos por la persona de apoyo del área de jurídica.

Es importante mencionar que, en ocasiones se requiere, del apoyo de otra área importante, como puede ser la de comunicaciones o relaciones públicas, muchas veces, por la misma información que se maneja dentro del equipo, puede que sea necesario la presentación de dicha información, en entrevistas o incluso en programas de televisión, donde se debe exponer casos o análisis de los procesos practicados según el caso.

7.3.11 Necesidad de auto evaluación. Dentro de los requerimientos del equipo, también es de suma importancia resaltar que se requiere un auto proceso de mejora, por lo que se debe requerir las auditorías internas, evaluación de incidentes de seguridad en comités de trabajo, mensuales o semanales, investigaciones de procesos de mejora continua en el equipo, como procesos disciplinarios.

7.4 POLÍTICAS DEL CSIRT

7.4.1 Política de clasificación de información. Dando contenido a esta política la empresa Cibersecurity de Colombia LTDA., realizará una política de clasificación de la información para el CSIRT, la cual se basará en cuatro objetivos específicos que le permitirán tener una clasificación adecuada de los datos de información, los objetivos mencionados permitirán que la información tenga un orden especifico, así como un responsable que esté a cargo, así mismo se realizará una clasificación mediante etiquetas que le permitan al consultor buscar en el lugar adecuado, se indican los objetivos a continuación[119].

A. Los activos de información deben ser inventariados.

B. Los activos de información deben tener identificado un propietario.

C. La información debe ser clasificada.

D. La información debe ser etiquetada y debe darse el tratamiento adecuado a dicha clasificación.

7.4.1.1 Los activos de información deben ser inventariados. Con el fin de poder clasificar la información en un inventario, es muy importante disponer de los medios necesarios y conocer de primera mano cuales son los datos de los que se dispone para realizar el respectivo inventario, para este caso se tendrán en cuenta la información en las bases de datos, en los medios electrónicos, en formato de papel o físico, en correos electrónicos, así como en distintos medios de almacenamiento portátiles, P. ej. Memorias USB, discos duros, entre otros, dicho inventario debe estar actualizado y auditado mínimo dos veces al año[120].

7.4.1.2 La información debe tener un propietario. Los propietarios de la información según sea su responsabilidad dentro de la organización, debe tener en cuenta los siguientes aspectos, los cuales debe aplicar de manera correcta, debe clasificar de acuerdo con su grado de sensibilidad (Confidencialidad, integridad, disponibilidad) y criticidad, de la información que este manejando dentro de la organización, siendo el custodio directo de dicha información hasta que se determine lo contrario[121].

[119] CAVANNA Santiago. Política de Clasificación de la información. [Sitio Web] (2019) Argentina. [Consulta: 27 de abril de 2020] Disponible en: http://www.adecuarse.com/
[120] Ibid.
[121] Ibid.

7.4.1.3 La información debe ser clasificada. Cada uno de los datos de la información obtenida será considerada de uso interno, hasta que se dé una nueva reclasificación de esta, como por ejemplo en alguna otra categoría, pudiéndose reclasificar a través del proceso correspondiente, los datos de información, preferentemente deberán ser clasificados antes de su creación, recopilación o adquisición, así como las pautas de clasificación de la información, necesariamente no debe mantenerse invariable por siempre, pues estás pueden cambiar y hasta llegar a tener otro criterio, se debe tener en cuenta que la información puede llegar a ser obsoleta, siendo necesario su eliminación, siempre teniendo claro que la destrucción de cualquier proceso, se debe asegurar la confidencialidad de la información hasta el momento de su eliminación, esta también deberá ser clasificada con los grados de criticidad, es por ellos que todos los documentos tanto físicos y digitales, deben contener una etiqueta que los clasifique, tal como se enumera a continuación, dicha clasificación se debe realizar desde la creación de dicho documento, en su defecto si se trata de un escrito, puede ser realizada por personal de archivo o con el apoyo de software diseñado para tal fin, como puede ser el SoftExpert [122].

A. **Confidencial:** nivel de confidencialidad solo del propietario.

B. **Restringido:** con niveles medios para la confidencialidad.

C. **Uso interno:** con un nivel bajo de confidencialidad.

D. **Público:** Acceso total a la información de cualquier persona.

7.4.1.4 La información debe ser etiquetada y clasificada. Es muy importante poder rotular y etiquetar cada dato de información que se obtenga en el día a día de la operación, sin importar el medio en el que se recolecte, almacene, disponga o trasporte dicha información, se deben tener en cuenta varios aspectos que son importantes para el correcto etiquetado e identificación de cada segmento de información recolectado[123].

A. Código de identificación

B. Tipo de activo

[122] ISOTOOLS. ISO 27001 Cómo se debe realizar la clasificación de la información. (14 septiembre, 2017) [Sitio Web] Blog especializado en Sistemas de Gestión de Seguridad de la Información. [Consulta: 27 de abril de 2020] Disponible en: https://www.pmg-ssi.com/2017/09/iso-27001-clasificacion-de-la-informacion-2/
[123] CAVANNA. Óp. cit.

C. Breve descripción

D. Principales características técnicas

E. Responsable del activo

F. Administrador del activo

De igual forma, se debe indicar que complementando los diferentes métodos de clasificación de los que ya se habló, es importante mencionar una clasificación a la matriz de criticidad de los niveles que tiene un activo de información para “La empresa Cibersecurity de Colombia LTDA.” se le dará, a la información un valor por cada uno de estos criterios de clasificación. En cada una de las siguientes categorías[124].

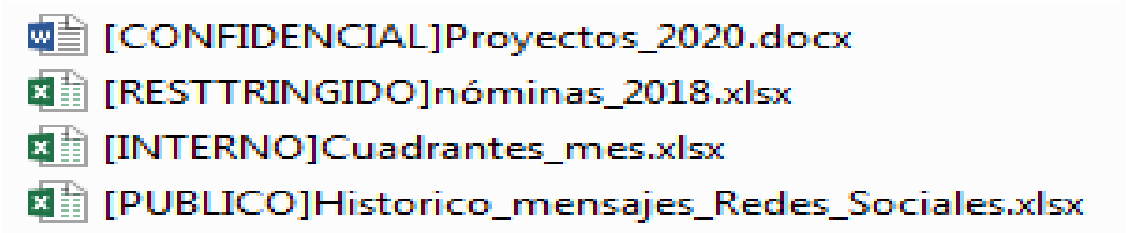
A. **Criticidad BAJA:** ninguno de los valores asignados supera 1.

B. **Criticidad MEDIA:** alguno de los valores asignados es 2.

C. **Criticidad ALTA:** alguno de los valores asignados es 3.

La manera correcta de realizar la etiqueta a los documentos digitales, teniendo en cuenta la clasificación de la información en cuanto al nivel de criticidad, una buena manera de realizar el etiquetado a la hora de crear cualquier producción digital, puede ser un Ejemplo de ellos, como se observa en la Figura 15, dicho proceso se podría realizar mediante la utilización de un software que permita realizar u buen etiquetado y clasificación, una buena herramienta podría ser (Alfresco).

Figura 15 Etiquetado de documentos digitales



Fuente: El autor.

[124] COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. [En Línea] GIT-G-01 guía para la calificación de la información. Bogotá D.C. 2015. [Consulta: 27 de abril del 2020]. P.7-22. Disponible en: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/3.3%20Procesos%20y%20Procedimientos/GIT-G-01_GUIA_PARA_LA_CALIFICACI%C3%93N_DE_LA_INFORMACI%C3%93N_AGN.pdf

7.4.2 Política de protección de datos. Para lograr determinar dicha política, se deben tener claros los actores que participaran en la misma, los clientes y la misma compañía como tal, los cuales estarán en función de los intereses de la Empresa Cibersecurity de Colombia LTDA., al momento de implementar el CSIRT, por lo que se deben establecer, los derechos y deberes de cada una de las partes, los derechos son todos aquellos a los que se tiene como cliente, Acceder, conocer, actualizar y rectificar sus datos personales frente, a la empresa Cibersecurity de Colombia LTDA., en su condición de responsable del tratamiento, entre las dos partes deben firmar una cláusula de tratamiento de datos, la cual servirá como soporte, para las disposiciones y actuaciones generales que se disponga al trascurrir los contratos pactados, por lo que el CSIRT solo podrá utilizará los datos personales del cliente, para el cumplimiento y funciones descriptas en contrato pactado, así como de las finalidades autorizadas expresamente por el cliente final o por las normas vigentes, como la "Ley Estatutaria 1581 de octubre 18 de 2012" [125], de este modo la empresa Cibersecurity de Colombia LTDA., debe solicitar el consentimiento libre, expreso, previo e informado del titular, de los datos para su tratamiento, excepto en los casos expresamente autorizados en la ley[126].

7.4.3 Política de retención de información. Esta será siempre aplicada a los medios en los cuales se pueda guardar, procesar y almacenar datos, como el papel, los medios electrónicos, correos, videos, audio, sistemas de control de accesos, bases de datos, servidores, Etc. La persona encargada del proceso, bajo las normas establecidas y lo dispuesto en la ley, determinara el tiempo por el cual los datos en general, deben ser retenidos mediante el programa de retención de información, Esta política define el tiempo en el cual el CSIRT deberá mantener cada uno de los registros u otra clase de información de la cual disponga, el método de destrucción lo podrá realizar la persona encargada o se podrá contratar una empresa externa especialista en materia de destrucción de información confidencial, pues dependiendo del grado de criticidad se debe aplicar un método de eliminación, p. ej. Para los documentos en papel de criticidad (1) se debe eliminar como residuos confidenciales (triturado de corte transversal e incinerado) en las cortadoras de papel, y los documentos y demás archivos de información electrónica, se deben aplicar el método de eliminación electrónica segura[127].

[125] COLOMBIA, CONGRESO DE LA REPUBLICA. Óp. cit.
[126] UNIVERSIDAD EAFIT. política de tratamiento de protección de datos personales de los titulares. [En Línea] [Consulta: 12 de octubre de 2019] p. 4-7. 14. Disponible en: http://www.eafit.edu.co/institucional/reglamentos/tratamiento-proteccion-datos-personales/Documents/Politica-Universidad-EAFIT-de-tratamiento-de-protecci%C3%B3n-de-datos-personales.pdf
[127] PÉREZ AGUILERA Carlos J. política de retención de datos. [En Línea] Ofiteco Uninc. (08 de mayo del 2018) [Consulta: 12 de octubre de 2019] P. 4-7. 8. Disponible en: https://uning.es/wp-content/uploads/2018/06/Politica-de-retencion-de-datos.pdf

7.4.4 Política de destrucción de información. El fin u objetivo de esta política, es definir la forma como el CSIRT, garantizara que la información, que ya cumplió su ciclo de vida y que no altera las demás políticas, la cual pueda estar almacenada en equipos y soportes digitales, así como los medios físicos y lógicos sea borrada o eliminada de forma segura, los pasos que se pueden aplicar para determinar el ciclo de vida de cualquier producción realizada bien sea en físico o digital, debe cumplir los siguientes requisitos, (Creación, organización y clasificación, colaboración y revisión, verificación y permanencia o eliminación) en Colombia se reglamenta con el "Acuerdo 006 de 2014 del Archivo General de la Nación"[128], del 15 de octubre del 2014, el cual indica las pautas para una mejor clasificación y ciclo de vida de los documentos, físicos y digitales. Garantizando que la información este siempre protegida hasta finalizar su ciclo de vida, igualmente los dispositivos y medios que la contengan también lleguen a su fin, para completar este ciclo de vida de la información, es necesario pasar por el proceso de destrucción de la misma, garantizando un borrado seguro de la información electrónica y física, la cual se debe borrar o eliminar, tanto la información original, como todas sus copias, y los respectivos respaldos existentes de información, en la destrucción de la información se deben tener presente el cumplimiento de dos políticas adicionales "divulgación y acceso". Igualmente se debe tener presente el registro de las operaciones de Borrado, las cuales se describen a continuación[129].

A. **Solicitud:** Solicitud formal dirigida al propietario del activo. indicando los medios o información a destruir, dicha solicitud debe ser inequívoca, al medio o la información que requiere destrucción.

B. **Proceso de destrucción**: se debe generar un reporte de actuación, el cual permitirá identificar, a cada uno de los autores del proceso y la metodología empleada para la destrucción de la información, igualmente se debe colocar las observaciones necesarias a que haya lugar, identificando claramente los procesos realizados.

C. **Persona responsable:** esta persona deberá realizar un análisis con antelación de la destrucción de la información, donde evaluará si corresponde o no la destrucción de dicha información, teniendo siempre presente cada uno de los decretos, leyes y otra normativa vigente.

D. **Destrucción:** siempre se debe realizar de acuerdo con los protocolos y demás políticas que acompañan la presente, como P. ej. La política de "retención

[128] ARCHIVO GENERAL DE LA NACIÓN (Colombia). Repositorio Normativo. Acuerdo No. 006. 15 oct 2014. "Por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI "Conservación de Documentos" de la Ley 594 de 2000" [En Línea] [Consulta: 12 septiembre de 2020] Disponible en: https://normativa.archivogeneral.gov.co/acuerdo-006-de-2014/

[129] CAVANNA Santiago. Política de Destrucción de la información. Óp. cit.

de información", como medida de respaldo, se debe contemplar la posibilidad de que el proceso de destrucción falle, tanto en un medio lógico, como físico, por lo que esta situación deberá quedar plenamente descrita y documentada, resaltando los procesos adicionalmente utilizados para llegar a la adecuada destrucción del medio.

Otro aspecto importante es el relacionado con el traslado de soportes físicos, lógicos y/o información almacenada de manera externa a "al CSIRT" por lo que se deberá asegurar la respectiva cadena de custodia, con el fin de evitar fugas de información. El Csirt, deberá tomar todas las medidas necesarias de verificación y cumplimiento de la presente política, con el fin de que se realice lo estipulado, por lo que se podrán tomar las medidas necesarias que se consideren pertinentes con el fin de llegar a ciclo final de toda la información, sin importar el medio en que se procese, dentro del centro de atención a incidentes de seguridad informática[130].

7.4.5 Política de divulgación de información. Toda información debe ser accesible y puede divulgarse a los interesados con previa autorización, sin que esta, de perjuicio de las restricciones establecidas en las demás políticas, esta política, especifica cómo y cuándo el CSIRT, puede divulgar la información interna o externa, es importante mencionar que ningún tipo de información confidencial estará dispuesta a ser divulgada bajo esta política, solo estará disponible al público la información de criticidad (Baja), la cual no cuenta o está relacionada en ningún nivel de confidencialidad, la información accesible al público se facilitará en la medida de lo posible, esta se tratara de compartir en folletos, revistas, entrevistas, y en lo posible en un sitio web del CSIRT, siendo los mismos lugares donde se podrá consultar, por otra parte se deberá tener presenta la "Ley Estatutaria 1581. de octubre 18 del 2012, para la protección de datos personales" [131], la información se divulgará siempre y cuando esta no ocasione inconvenientes al mismo CSIRT, como a sus clientes, sin embargo existen casos excepcionales en los cuales, se puede tener acceso a la información con algún nivel de confidencialidad bajo el amparo de previa solicitud, así como las expuesta por la ley, donde se ordena a cualquier entidad del estado relevar o colocar a disposición de alguna autoridad competente la información solicitada bajo orden judicial previamente autorizada por un juez de la republica dentro de un proceso penal e investigativo[132].

[130] Ibid.
[131] COLOMBIA, CONGRESO DE LA REPUBLICA. Óp. cit.
[132] ORGANIZACIÓN MUNDIAL DE LA SALUD (Ginebra). [En Línea] Política de divulgación de información 2017. [Consulta: 12 de octubre de 2019] P. 4-12. Disponible en: http://awareness.who.int/suggestions/InfoDisclosurePolicy_es.pdf

7.4.6 Política sobre el acceso a la información. La presente política, establece quien puede acceder y quien no, a la información del CSIRT, teniendo en cuenta tanto el personal interno, como los miembros de la comunidad objetivo, es de aclarar que el acceso a la información se establece en la "Ley 1712 de 2014, de Transparencia y del Derecho de Acceso a la Información Pública"[133], pero también se debe informar que el CSIRT no es una entidad pública del estado, por lo que gran parte de la información no será de acceso público, solo cuando este contemplado dentro de las diferentes políticas que se han relacionado, sin que estas puedan afectar al CSIRT y sus clientes, dicho de otra manera, solo se dará acceso a la información que no esté dentro de ningún nivel de confidencialidad, por lo cual se tendrá presente el decreto presidencial 1081 del 2015, por el cual se reglamenta el acceso a la información pública[134], se debe realizar una validación de la información que no es confidencial y que no tiene un nivel de criticidad, que este permita indicar o indique que no es publica, con el fin de poder determinar, cual información puede ser publicada y cual no[135].

7.4.7 Políticas de uso apropiado de los sistemas del CSIRT. La política permite definir el uso aceptable de los sistemas y recursos con los que cuenta el CSIRT, de esta manera se dará protección a los sistemas, en primer lugar, se debe determinar si es viable que los mismos miembros del equipo sean los administradores de los sistemas del CSIRT, por lo que se puede dar esta responsabilidad a una entidad externa y capacitada para la administración de los mismos, con el fin de que se tenga un responsable en caso de que algún sistema falle o sufra daños por su mala administración, otra medida es el uso de los equipos para fines personales por parte de los miembros del equipo, se deben garantizar que sean estrictamente para uso dentro del manual de funciones de cada miembro del equipo, lo cual garantice el buen uso y responsabilidad, según las medidas a las cuales estén sujetos los miembros, dentro de sus responsabilidades administrativas, legales y disciplinarias[136].

Otro punto importante es el uso de software, ya que solo se podrá instalar y utilizar los programas y herramientas descritas por el CSIRT, el administrador de los sistemas siempre deberá disponer de una copia de seguridad de respaldo de todos los sistemas, se debe establecer una configuración adecuada a cada uno de los sistemas y herramientas, cortafuegos, antivirus, proxy, VPNs, etc. con el fin de que estas cumplan con los niveles de seguridad exigidos por el CSIRT, así evitando

[133] COLOMBIA, CONGRESO DE LA REPUBLICA. Óp. cit.
[134] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Óp. cit.
[135] SABBAGH Ana Paulina. Secretaría de Transparencia. Presidencia de la Republica de Colombia. [En Línea] transparencia y acceso a la información. Bogotá D.C. [Consulta: 02 de mayo de 2020] P. 12-20. Disponible en: https://secretariageneral.gov.co/sites/default/files/jornada_transparencia_-_ley_de_acceso_a_la_informacion_publica.pdf
[136] CENTRO CRIPTOLÓGICO NACIONAL. Óp. cit., p. 19.

daños a los mismos y perdidas de información, es importante restringir el acceso a los sistemas al personal no autorizado, solo los administradores podrán tener acceso a los equipos, servidores y sistemas de seguridad instalados, por lo que se debe contar con un correcto y seguro control de accesos a lugares críticos de la operación y de infraestructura, donde se encuentran las salas de monitoreo, servidores, equipos de seguridad lógica, seguridad física, así como salas de almacenamiento de evidencias y datos, es necesario contar con sistemas de vigilancia las 24 horas, con el fin de tener un control total de los lugares y quienes acceden a ellos, estableciendo niveles de acceso, dejando en custodia los activos más críticos y confidenciales, para el personal más interno y de jerarquía en el CSIRT, garantizando de esta manera un control adecuado de los accesos a los sistemas[137].

7.4.8 Política de eventos y definición de incidentes de seguridad. Esta política permitirá tener los criterios para definición de los eventos e incidentes de seguridad, con el fin de dar una clasificación a cada uno de ellos y la gravedad, mediante establecimiento de un procedimiento de comunicación de eventos de seguridad, acompañado de un procedimiento de respuesta y escalado de los incidentes, determinando la respuesta que debe darse al evento de seguridad recibido.

7.4.8.1 Clasificación. Cuando se recibe por primera vez un evento de seguridad informática, se debe realizar una verificación adecuada del mismo porque, posiblemente, conlleve a una acción leal o penal, lo que podría derivar en la obtención de evidencias que sirvan como prueba, dentro de dicho proceso penal que se inicie, de esta manera se deberá clasificar el incidente de seguridad y así darle el tratamiento adecuado, solicitando apoyo por parte de personal capacitado en la recolección de evidencias y de asuntos jurídicos, en el momento de la recolección de las evidencias o pruebas se debe llevar a cabo la respectiva cadena de custodia[138].

7.4.8.2 Clasificación del equipo de respuesta. El equipo debe tener una estructura, donde se determine los niveles de atención según el evento de seguridad y la criticidad del mismo, como también los niveles de escalamiento, los responsables deben realizar la documentación requerida para el escalamiento, garantizando una respuesta rápida, efectiva y ordenada, frente a los incidentes de seguridad de la información, reportados desde cualquier nivel, en caso de que se requiera realizar el escalamiento de un incidente de seguridad fuera del CSIRT, solo lo podrá realizar la dirección del CSIRT.

[137] Ibid. P 20
[138] ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO. [En Línea] manual de políticas de seguridad y privacidad de la información Bogotá, D.C. 2018 [Consulta: 12 de marzo de 2020]. P. 71-79. Disponible en: https://www.escuelaing.edu.co/escuela/importantDoc/Manual-politica-seguridad-dela-Informacion.pdf

7.4.8.3 Eventos de seguridad. Dando una clasificación a los eventos que se deben reportar, es importante mencionar que se debe establecer una directriz que permita tener un organigrama, de cómo se debe seguir la secuencia del reporte de eventos de seguridad, teniendo en cuenta las siguientes preguntas, ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte? cada evento debe tener un responsable a quien se le debe dirigir, realizando la correcta documentación del incidente, de manera que no se pierda tiempo en la solicitud de ampliación de la información, lo que permitirá por parte del funcionario encargado dar una respuesta pronta y oportuna[139].

7.4.9 Política de gestión de incidentes. En la presente política se deberá definir cómo se lleva a cabo la gestión de los incidentes de seguridad, como también se debe agregar el tipo de incidentes, que el CSIRT atenderá según los servicios descritos en el portafolio comercial, los cuales serán a los que se les dará respuesta, agregando el tiempo de respuesta al incidente, entre otros[140].

A. **Objetivo:** Se deben establecer los lineamientos necesarios para la gestión y atención de incidentes de seguridad informática, con el fin de que se puedan prevenir y mitigar reduciendo el impacto de estos en los sistemas de información y las infraestructuras a proteger.

B. **Alcance:** Cada uno de los funcionarios e integrantes que tengan legítimo acceso a los sistemas y herramientas del CSIRT.

7.4.9.1 Responsabilidades. El director del CSIRT debe ser el responsable por difundir la presente política a todo y cada uno de los funcionarios responsables de implementarla, independiente del cargo que desempeñe. Los funcionarios del CSIRT son los responsables por dar cumplimiento a la presente política, así como reportar todos y cada uno de los eventos de seguridad que detecte durante su turno en operación, los cuales deben ser reportados al responsable de seguridad de la información que este encargado en el momento, siguiendo todos los procedimientos operativos y establecidos dentro de las demás políticas para tal fin. El director de seguridad de la información, de operación debe velar por el cumplimiento de la presente política[141].

[139] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, Elaboración de la política general de seguridad y privacidad de la información. Guía No 1. Op. cit. P.24
[140] CAVANNA. Op. cit.
[141] Ibid.

7.4.9.2 Descripción. Cada uno de los incidentes de seguridad que sean reportados por los usuarios internos o externos, deberán ser registrados, en una bitácora que deberá llevar el CSIRT, adicional deberán realizar las siguientes acciones con relación a los mismos:

A. **Procesos:** Los procesos de la gestión de los incidentes de seguridad se deberán, explicar de manera clara, sin ningún tipo de ambigüedades, por lo que los mecanismos y metodologías para realizar los respectivos reportes de los incidentes, otro aspecto importante es la información mínima y detallada que se debe proporcionar; manteniendo la confidencialidad de la información suministrada por la persona que realice el reporte del incidente inicialmente, así como su anonimato en caso de que sea necesario[142].

B. **Gestión:** El analista o funcionario que reciba el incidente de seguridad, deberá Informar de manera inmediata y con la información detallada y completa sobre el reporte, al Responsable de Seguridad de la información que se encuentre en el momento, de la existencia del potencial incidente de seguridad informática. Así mismo deberá, realizar la respectiva gestión de cada uno de los incidentes reportados al CSIRT, dando cumplimiento a todas las etapas de su ciclo de vida, las cuales serán las siguientes: reporte, asignación, tratamiento, respuesta, cierre y alimentación de la base de conocimiento[143].

C. **Base de Conocimiento:** Realizar una base de conocimiento de las posibles causas, procesos, fallas, antecedentes y mecanismos utilizados, con el fin de consultarlos y ponerlos en práctica, en futuros incidentes de las mismas características ya vistas, así garantizar que el próximo procedimiento sea mucho más rápido y de esta manera se logre dar respuesta eficientemente y oportunamente, ganando tiempo importante tanto para el CSIRT como para el usuario o cliente que reporta, así como poder realizar un escalamiento en caso de que sea necesario, sin la necesidad de perder tiempo buscando un diagnóstico ya realizado en incidentes anteriores, Adoptando las medidas necesarias, de seguridad eficientes para proteger los activos de información[144].

D. **Procesos dependientes:** De la presente política, dependerá el Proceso de Gestión de Incidentes.

[142] Ibid.
[143] Ibid.
[144] Ibid.

7.4.9.3 Cumplimiento. La presente política deberá ser aplicada en el momento que el CSIRT entre en funcionamiento, así mismo el director del CSIRT, como los líderes de las operaciones, deben velar por el estricto cumplimiento, y la verificación de lo estipulado en la presente Política en dicho documento, el incumplimiento de la política será motivo sufriente para realizar y dar apertura a investigaciones a las que haya lugar, desde disciplinarias y hasta penales[145].

7.4.10 Política de cooperación. Esta política será implementada desde antes de colocar en marcha el CSIRT, condicionalmente es muy importante tener alianzas importantes en materia de cooperación en la atención de incidentes de ciberseguridad, teniendo socios estratégicos tanto nacionales como internacionales, debido a los ataques que pueda sufrir la infraestructura propia o la de algún cliente, puede llegar de cualquier lugar del mundo, por lo que se requiere que el CSIRT, cuente con los contactos necesarios en caso de que se requiera una cooperación de manera urgente, en algún caso específico que se presente.

A. **Objetivo:** establecer estrategias de cooperación con los socios nacionales e internacionales, en temas relacionados, con atención de incidentes de seguridad Informática y ciberseguridad.

B. **Alcance:** para los incidentes que se atiendan con origen nacional e internacional, y que no se conozca de su ocurrencia anteriormente, así como de su gravedad, con previa autorización del director del CSIRT.

Durante la ejecución de la operación, el CSIRT, puede Fomentar la cooperación e interactuar con otras organizaciones, nacionales e internacionales, como equipos SOC, CERT o CSIRT, como también, de la comunidad a la que presta servicios, y demás proveedores, analistas y generadores de inteligencia, etc. ejerciendo labores de punto central de sensibilización y comunicación entre los miembros de la comunidad. Dentro del ámbito nacional se han establecido algunos equipos en particular los cuales hacen referencia a los más destacados del país, como lo es (colCERT Grupo de Respuesta a Emergencias Cibernéticas de Colombia)[146], otro de gran importancia (CCP centro cibernético policial)[147], así como él (CSIRT-PONAL Equipo de Respuesta de Seguridad Informática Incidente de la Policía Nacional de Colombia)[148] y para finalizar el (SOC-CCOC Centro de operaciones de seguridad - Comando de operaciones cibernéticas conjuntas)[149]. Siendo los tres

[145] Ibid.
[146] COLCERT. Op. cit.
[147] POLICÍA NACIONAL DE COLOMBIA. Óp. cit.
[148] POLICÍA NACIONAL DE COLOMBIA. Óp. cit.
[149] COMANDO CONJUNTO CIBERNÉTICO Óp. cit.

equipos de referencia más importantes del país, a los que se deberían o deben ser comunicados los incidentes relevantes de seguridad de la información, en relación con lo anterior, fue comunicado por el “Departamento Nacional de Planeación en el documento CONPES Política Nacional de Seguridad Digital” [150].

Limitaciones: Dentro de las limitaciones de la presente política, se pueden destacar las siguientes, las cuales se pueden modificar de acuerdo con las necesidades de cooperación que pueda fortalecer el CSIRT.

A. No compartir de ninguna manera, información confidencial con otros centros, sin un acuerdo y autorización expresa del director del CSIRT.

B. Esta política aplica siempre en todos y cada uno de los supuestos en los que no exista orden superior, como ninguna obligación legal o normativa dentro del territorio nacional, que obligue a compartir la información.

C. Se debe proteger la información personal dándole privacidad. Teniendo en cuenta que esta se encuentra dentro de los parámetros de confidencialidad, por lo que no se compartirán datos personales, y en caso de que fuese necesario solo se podría hacer bajo orden expresa de un juez colombiano, mediante orden judicial, sin que esto deje sin efecto lo expresado en la Ley Estatutaria 1581.

D. No se podrá realizar la publicación o entrega de información personal, en el momento en que el propietario de esta notifique su deseo de no publicación. Solo en un supuesto en que no exista solicitud legal por parte de autoridad competente o normativa superior que obligue a compartirla.

[150] DEPARTAMENTO NACIONAL DE PLANEACIÓN, Documento CONPES 3854, departamento nacional de planeación, [En Línea] política nacional de seguridad digital Colombia: 2016. [Consulta: 12 de octubre de 2019] P. 91. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

8 ESTUDIAR Y APLICAR EL INTERCAMBIO DE MODELOS

Se realizará un análisis de información, referente a los modelos que puedan ser o hayan sido aplicados, en los países, en los cuales se cuente con diversidad de centros de atención a incidentes de seguridad y grupos de ciberseguridad, de los cuales se mencionaran los CERT y CSIRT, por lo que será necesario, realizar una búsqueda en bases de datos de autores que hayan profundizado en temas relacionados y correspondiente a lo que se pretende en el presente capítulo, con el fin de realizar una descripción de cada uno de los modelos consultados, de esta manera poder tener diversas fuentes e ideas, para ser aplicadas en el presente proyecto, bajo la metodología de información documentada y citada, para finalizar el contexto de este capítulo, se establecerá como modelo (DISTRIBUIDO), el cual será aplicado en la empresa Cibersecurity de Colombia LTDA., con el fin de implementar la documentación para el CSIRT. Concluyendo lo anterior, en España existe un CSIRT que maneja un modelo acorde, a lo que se requiere, para el equipo de la empresa Cibersecurity de Colombia LTDA., este equipo sería un modelo que seguir, se trata del Equipo de Respuesta ante Emergencias Informáticas INCIBE.[151].

8.1 CIBERSEGURIDAD Y MODELOS EN PAÍSES VECINOS

8.1.1 Análisis de ciberseguridad en Brasil. Para entrar en contexto de cómo se encuentra el país vecino de Brasil en temas relacionados con ciberseguridad y como los están afrontando, se determina que ha sido el país más atacado en los últimos años en Latinoamérica, en relación a los ataques informáticos, así como también ha ocupado los primeros lugares en el mundo, luego de estados Unidos, es por esto que el país vecino ha tenido que redoblar esfuerzos con el fin de poder hacer frente a dichos ataques, se dice que estos obedecen a diferentes causas, entre las que se resalta, las herramientas jurídicas para afrontar de raíz la problemática, la falta de personal capacitado y la infraestructura tecnológica que el país tiene actualmente, no es que este mal en comparación con los demás países, solo que debido a su crecimiento económico, requiere de mejores herramientas tecnológicas que le permitan estar en competencia con la tecnología moderna del mundo, lo cual, lo hace un blanco vulnerable para los ataques informáticos en la región y el mundo[152].

[151] INCIBE INSTITUTO NACIONAL DE CIBERSEGURIDAD, Óp. cit.
[152] BNAMERICAS ¿Por qué Brasil es tan vulnerable a los ciberataques? 06 enero, 2020 [Sitio Web] Brasil. [Consulta: 12 septiembre de 2020] Disponible en: https://www.bnamericas.com/es/reportajes/por-que-brasil-es-tan-vulnerable-a-los-ciberataques

Es por esta razón que a mediados del 2016 realizaron su propia política de ciberseguridad, con el fin de poder hacer frente a los inconvenientes qua venían presentando, por esta razón dan importancia a la seguridad informática, dado que entienden que es de suma importancia mantener sus sistemas seguros, de esta manera realizan inversiones de suma importancia para mantenerse actualizados y de una otra manera blindarse contra los ataques cibernéticos de los que ya venían siendo víctimas[153], lo anterior teniendo en cuenta el estado actual para el año 2016, en la actualidad no han mejorado mucho, según el estudio realizado por la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo, denominado, Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020, si se tiene en cuenta la Política y Estrategia de Seguridad Cibernética, sigue siendo prácticamente la misma, sin mejoras considerables, así mismo otros aspectos importantes como lo son, (Cultura Cibernética y Sociedad, Formación, Capacitación y Habilidades de Seguridad Cibernética) se ha visto mejoras en, (Marcos Legales y Regulatorios, Estándares, Organizaciones y Tecnologías) tal como se observa en la página 72 del documento[154].

8.1.2 Modelos de los CSIRT en Brasil. Los diferentes móldelos que se pueden encontrar en Brasil, tienen que ver con los más comunes (Coordinador, Centralizado y Campus), dentro de estos modelos se destacan el NIC.br, CERT.br, así como el CEO / RedeRio - RedeRio Security Group.

8.1.2.1 NIC.br. Modelo Coordinador, Es el Centro de Información y Coordinación de Internet en Brasil, así mismo es responsable de coordinar e integrar las iniciativas y servicios de Internet en el país, tiene coordinación de diferentes equipos en los cuales se puede destacar los siguientes[155].

A. **REGISTRO.br:** Encargado del registro, así como el mantenimiento de cada uno de los nombres de dominio ".br", se encarga de ejecutar y distribuir el direccionamiento IPv4 e IPv6, como también los Sistemas Autónomos (ASN) en todo el país.

[153] LUISA Cruz Lobato. URVIO - Revista Latinoamericana de Estudios de Seguridad N.° 20, junio de 2017, pp. 16-30. La política brasileña de ciberseguridad como estrategia de liderazgo regional. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://revistas.flacsoandes.edu.ec/urvio/article/view/2576/2104

[154] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. Op. cit., P. 72.

[155] NIC.br. (Brasil). Centro de Información y Coordinación [Sitio web] Brasil [Consulta: 12 de octubre de 2019] Disponible en: https://www.nic.br/

B. **CERTIC.br**: Es el encargado y responsable sobre el buen uso y acceso a Internet en Brasil, como también realiza el monitoreo de las Tecnologías de la Información y la Comunicación.

C. **CEWEB.br:** su responsabilidad es difundir, así como proveer, el uso de las tecnologías abiertas en la Web, en Brasil.

8.1.2.2 CEO / RedeRio. Modelo Campus, Este equipo es el encargado de la respuesta a incidentes de seguridad, del campus universitario de Brasil, así como de los centros de investigación y de las agencias gubernamentales del país.

8.1.2.3 CERT.br. Modelo centralizado, Es el Centro para el Estudio, de la Respuesta y el Tratamiento de los Incidentes de Seguridad en todo el territorio brasileño, actuando como CSIRT centralizado, el cual debe coordinar con los demás equipos en todo el territorio nacional, sobre los incidentes de mayor impacto o de infraestructura critica.

8.1.3 Análisis de ciberseguridad en Chile. Durante el periodo de 2018, chile tuvo un incremento del 59% en ataques cibernéticos en comparación con el promedio de América Latina que fue de 62% es un porcentaje muy alto para un solo país, tal como lo informó la Agencia EFE[156], por lo que, sus dirigentes o Gobernantes, se han puesto en la tarea de mejorar su infraestructura y las capacidades de respuesta en temas relacionados con ciberseguridad, según la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo, denominado, Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020, chile ha tenido grandes mejoras en ciberseguridad y se ha comprometido en mejoras para el año 2022, como lo es, tener una infraestructura más sólida, garantizar los derechos de las personas en el ciberespacio, promover el desarrollo de una industria de seguridad cibernética, desarrollar una estrategia de seguridad cibernética basada en la educación y las buenas prácticas, entre otras que se relacionan en el documento[157].

[156] AGENCIA EFE. Los ciberataques crecen en Chile 59% en 2018 cerca de la media de América Latina. Santiago de Chile. 5 ene 2019. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.efe.com/efe/america/economia/los-ciberataques-crecen-en-chile-59-2018-cerca-de-la-media-america-latina/20000011-3858841

[157] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. Op. cit., P. 72

8.1.4 Csirt en Chile. Modelos de los Csirt de chile, dentro de los equipos de respuesta a incidentes de seguridad y ciberseguridad informática, se pueden destacar el Csirt nacional y los modelos coordinador, como lo es el Csirt.gob.cl.

8.1.4.1 Csirt.gob.cl. Equipo de Respuesta ante Emergencias Informáticas, este Csirt realiza las veces de coordinador del país, donde los demás coordinan la atención de los incidentes de seguridad informática de relevancia nacional o internacional[158].

El Csirt gob cl, cuenta con un modelo particular de atención a incidentes de seguridad de la información, el cual está clasificado de la siguiente manera, como se observa en el Cuadro 2.

Cuadro 2. Clasificación de incidentes

Matriz de clasificación de Incidentes			
N°	Clase de Incidente	Tipo de Incidente	Descripción
1	Contenido Abusivo	Pornografía Infantil – Sexual – Violencia	Pornografía infantil, glorificación de la violencia, otros.
		Spam	«Correo masivo no solicitado», lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de un grupo masivo de mensajes, todos teniendo un contenido similar
		Difamación	Desacreditación o discriminación de alguien
2	Código Malicioso	Malware, Virus, Gusanos, Troyanos, spyware, Dialler, rootkit	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.
3	Recopilación de Información	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.
		Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).

[158] Csirt gob cl, (Chile) Equipo de Respuesta ante Emergencias Informáticas. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.csirt.gob.cl/matriz-clasificacion-incidentes/

Cuadro 2. (Continuación)

Matriz de clasificación de Incidentes			
N°	Clase de Incidente	Tipo de Incidente	Descripción
		Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
4	Intentos de Intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
		Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el búfer desbordamiento, puerta trasera, secuencias de comandos cruzadas, etc.).
		Nueva Firma de Ataque	Un intento de usar un exploit desconocido.
5	Intrusión	Compromiso de Cuenta Privilegiada	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede han sido causado de forma remota por una vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet.
		Compromiso de Cuenta sin privilegios	
		Compromiso de Aplicación, Bot	
6	Disponibilidad	Ataque de denegación de servicio (DoS / DDoS)	Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla. Algunos ejemplos DoS son ICMP e inundaciones SYN, ataques de teardrop y bombardeos de mail's. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como Ataques de amplificación DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.
		Sabotaje	
		Intercepción de información	

Cuadro 2. (Continuación)

Matriz de clasificación de Incidentes

N°	Clase de Incidente	Tipo de Incidente	Descripción
7	Información de seguridad de contenidos	Acceso no autorizado a la información	Además de un abuso local de datos y sistemas, la seguridad de la información puede ser en peligro por una cuenta exitosa o compromiso de la aplicación. Además, son posibles los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro). El error humano / de configuración / software también puede ser la causa.
		Modificación no autorizada de la información	
8	Fraude	Phishing	Enmascarado como otra entidad para persuadir al usuario a revelar una credencial privada.
		Derechos de Autor	Ofrecer o instalar copias de software comercial sin licencia u otros materiales protegidos por derechos de autor (Warez).
		Uso no autorizado de recursos	Usar recursos para fines no autorizados, incluida la obtención de beneficios empresas (por ejemplo, el uso del correo electrónico para participar en cartas de cadena de ganancias ilegales) o esquemas piramidales).
		Falsificación de registros o identidad	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.
9	Vulnerable	Sistemas y/o softwares Abiertos	Sistemas «Open Resolvers», impresoras abiertas a todo el mundo, vulnerabilidades aparentes detectadas con nessus u otros aplicativos, firmas de virus no actualizadas, etc.
10	Otros	Todos los incidentes que no encajan en alguna de las otras categorías dadas	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.
11	Test	Para pruebas	Producto de pruebas de seguridad controladas e informadas

Fuente; Csirt gob cl, (Chile) Equipo de Respuesta ante Emergencias Informáticas. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.csirt.gob.cl/matriz-clasificacion-incidentes/

8.1.4.2 Herramientas y software. El Csirt gob cl, cuenta con un listado de Herramientas, software y Sistemas, para las distintas actividades que realiza el equipo en operación, como pueden ser las herramientas de monitoreo, el software de análisis de incidentes, y demás que son requeridas para dar respuesta a los incidentes que son atendidos, como se observa en la Figura 16.

Figura 16. Listado de Herramientas y Software

Fuente: Csirt gob cl, (Chile) Equipo de Respuesta ante Emergencias Informáticas. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.csirt.gob.cl/matriz-clasificacion-incidentes/

8.1.4.3 CLCERT. Laboratorio de Criptografía Aplicada y Ciberseguridad, un Csirt, encargado de la atención de incidentes de seguridad informática en el país chileno, el cual cumple el modelo Campus y Centralizado del país, pues aparte de ser un centro de atención a incidentes de seguridad de la universidad de Chile, este presta también los servicios tanto a entidades públicas como privadas, su fin es analizar, monitorear y dar respuesta a los problemas de seguridad de los sistemas computacionales de todo el país, pues la universidad realiza investigación mediante su equipo de respuesta a incidentes de seguridad, tanto a lo computacional, como a la criptografía, así como la educación en temas relacionados con seguridad informática a toda la comunidad, brindando las herramientas necesarias para que el soporte y conocimiento aportado, permita prevenir los ataques, mediante el conocimiento aportado y las diferentes estrategias de acción, permiten hacer frente a cada uno de los incidentes de seguridad computacional y la criptografía aplicada[159].

8.1.5 Análisis de ciberseguridad Ecuador. Ecuador es uno de los países de América latina que aún no cuenta con una política de ciberseguridad, sin embargo, ha tenido avances significativos en materia de ciberseguridad, tal como lo indica, la OEA y BID en su análisis titulado, Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020, donde se observan mejoras de gran valor como lo son, (Política y Estrategia de Seguridad Cibernética, Marcos Legales y Regulatorios y Estándares, Organizaciones y Tecnologías) donde se han realizado esfuerzos importantes para mejorar las condiciones de la ciberseguridad en el Ecuador[160].

8.1.6 Modelos de Csirt en Ecuador. Dentro de los diferentes grupos de atención a incidentes que cuenta el país de Ecuador, se tiene una variedad desde los militares, Comerciales, infraestructura critica, nacionales y de la parte académica o campus, el área que más centros tiene para la atención de incidentes de seguridad es el sector comercial con un total de 12 centros, seguido de la parte académica con 3 centros para la atención de incidentes de seguridad[161].

---

[159] CLCERT (Chile) Universidad de Chile. Laboratorio de criptografía aplicada y ciberseguridad. [Sitio Web] Chile [Consulta: 12 septiembre de 2020] Disponible en: https://www.clcert.cl/

[160] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. Op. cit., P. 72.

[161] GOB.EC. Portal único de tramites ciudadanos. Asesoría para la formación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) [Sitio Web] Ecuador. [Consulta: 12 de abril de 2020] Disponible en: https://www.gob.ec/arcotel/tramites/asesoria-formacion-equipos-respuesta-incidentes-seguridad-informatica-csirt

8.1.6.1 Ecuador ecuCERT. Centro de respuesta a incidentes informáticos del Ecuador, este centro brinda sus servicios a todo el país, enfocándose en operadores de redes de telecomunicaciones, proveedores de servicios e infraestructura crítica del país, este equipo de respuestas a emergencias informáticas, tiene el modelo de coordinador o de infraestructura critica, por lo que funciona como coordinador de los demás, por lo que los demás, deben reportar los incidentes de mayor impacto, con el fin de darles el trámite correspondiente, incluyendo los incidentes de carácter internacional[162].

8.1.6.2 CSIRT CEDIA. Perteneciente a la Comunidad Academia del Ecuador, específicamente a las instituciones que son miembros de CEDIA, revisa actividades y responde los informes. Los cuales les permitan mejorar la calidad del tráfico en las redes de las instituciones y centros de investigación miembros de Red CEDIA, así como la seguridad en las mismas, y disminuyendo los incidentes de seguridad provocados por fallas en la configuración, dentro de los servicios que presta este equipo de respuesta están los preventivos, realizando constantes monitoreos desde y hacia las redes de sus miembros, lo cual le permite mantener seguras las redes y estar enviando las notificaciones a cada uno de sus miembros en tiempo real, este equipo funciona como modelo centralizado de las instituciones educativas y centros de investigación, igualmente mantiene una comunicación constante con los demás CSIRT del país, garantizando una seguridad global dentro del país en coordinación con los demás equipos de respuesta a incidentes de seguridad cibernética. Por otro lado, cuenta con un portafolio de servicios, que ofrece, diferentes paquetes de servicios dirigidos a las universidades, institutos y colegios[163].

A. Portafolio universidades: dentro de las universidades que son miembro del CEDIA, están varias de las más importantes de Ecuador, como para mencionar alguna de ellas, (Universidad Nacional de Loja, Universidad de Cuenca, Universidad de las Fuerzas armadas, Escuela superior politécnica de Chimbarazo, Escuela politécnica Nacional, Universidad estatal de Bolívar, entre otras) dentro de los servicios que se tienen ofertados a las universidades están todos los relacionados, con Conectividad, infraestructura, multimedia, Aplicaciones académicas, proyectos, Colaboración, Capacitación, eventos e innovación y emprendimiento, para mejor detalle del portafolio, se podrá apreciar en la Figura 17[164].

[162] ECUCER. (Ecuador). Centro de Respuesta a Incidentes Informáticos. [Sitio Web] [Consulta: 12 abril 2020] Disponible en: https://www.ecucert.gob.ec/
[163] CEDIA CSIRT. (Ecuador). Equipo de respuesta a incidentes de seguridad. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://csirt.cedia.edu.ec/
[164] CEDIA CSIRT. Paquete de servicio universidades. Op. cit.

Figura 17. Portafolio Universidades.

Fuente: CEDIA CSIRT. Paquete de servicio universidades. Ecuador 2019. [En Línea] [Consulta: 12 septiembre de 2020] Disponible en: https://www.cedia.edu.ec/dmdocuments/PAQUETES%20DE%20SERVICIOS/universidades_servicios2019.pdf

B. Portafolio Instituciones: dentro de las Instituciones que son miembro del CEDIA, están varios de los más importantes de Ecuador, como para mencionar algunos de ellos, (Instituto Superior Tecnológico Bolivariano, Instituto Superior Tecnológico Jose Chirijogo Grijalva, Instituto Superior Tecnológico Vida Nueva, Instituto Superior Tecnológico Espíritu, Tecnológico Sudamericano, entre otros) los servicios que se tienen ofertados a los Institutos están todos los relacionados, con Conectividad, infraestructura, multimedia, Aplicaciones académicas, Investigación, Capacitación, Colaboración y eventos, para mejor detalle del portafolio, se podrá apreciar en la Figura 18[165].

[165] Ibid.

Figura 18. Portafolio institutos

PAQUETES DE PRESTACIONES — INSTITUTOS

	CONECTIVIDAD			INFRAESTRUCTURA				MULTIMEDIA			APLICACIONES ACADÉMICAS						INVESTIGACIÓN		CAPACITACIÓN		COLABORACIÓN	EVENTOS	
	MEJ.	①		②		③	④	NUE.	⑤		⑥	⑦					NUE.		NUE.				
	Red Avanzada (Mbps)	EDUROAM	Web Application Firewall	Videoconferencia multipunto	Grabación eventos Y transmisión en vivo	Seguridad Informática	ervidores virtuales Multiuso	Radio Online	Cartelera Digital	Repositorio Multimedia	Envió de archivos (100Gb)	Repositorio de Objetos de Aprendizaje	Plataforma MOOC	Repositorio de Acceso Abierto (RAAE)	REDI (Repositorio Semántico de investigadores)	Licencias Wolfram	Fondo CEPRA	Incubadora de Proyectos	Capacitación Escuela de Formación Continua (cupos)	Certificación Escuela de Formación Continua (cupos)	Proyecto ECHO	TICEC (Profesores)	Concursos InnovaCEDIA
BÁSICO	60	✓	✓	1	✓	✓	✓	✓	✓	✓	✓	✓	10	✓	✓	60	0	✓	1	0	✓	1	✓
INTERMEDIO	105	✓	✓	1	✓	✓	✓	✓	✓	✓	✓	✓	15	✓	✓	100	0	✓	1	1	✓	1	✓
AVANZADO 1	150	✓	✓	2	✓	✓	✓	✓	✓	✓	✓	✓	20	✓	✓	250	6	✓	2	1	✓	2	✓
AVANZADO 2	195	✓	✓	3	✓	✓	✓	✓	✓	✓	✓	✓	25	✓	✓	350	9	✓	2	1	✓	2	✓
AVANZADO 3	240	✓	✓	4	✓	✓	✓	✓	✓	✓	✓	✓	30	✓	✓	350	11	✓	3	2	✓	3	✓
AVANZADO 4	285	✓	✓	5	✓	✓	✓	✓	✓	✓	✓	✓	35	✓	✓	450	14	✓	4	2	✓	3	✓
Plan Personalizado	V	✓	✓	V	✓	✓	✓	✓	✓	✓	✓	✓	V	✓	✓	V	V	✓	V	V	✓	V	✓

Fuente: CEDIA CSIRT. Paquete de servicio universidades. Ecuador 2019. [En Línea] [Consulta: 12 septiembre de 2020] Disponible en: https://www.cedia.edu.ec/dmdocuments/PAQUETES%20DE%20SERVICIOS/universidades_servicios2019.pdf

C. Portafolio Colegios: dentro de los colegios que son miembro del CEDIA, están los más importantes de Ecuador, algunos de ellos, (Unidad educativa particular Borja, Fundación colegio americano de Quito, Liceo internacional, Unidad educativa particular cristo rey, entre otras) dentro de los servicios que son ofertados a los colegios, están todos los relacionados, con Conectividad, infraestructura, multimedia, desarrollo académico, Capacitación y eventos, para mejor detalle del portafolio, se podrá apreciar en la Figura 19[166]

[166] CEDIA CSIRT. Paquete de servicio Colegios. Ecuador 2019. [En Línea] [Citado en 12 septiembre de 2020] Disponible en: https://www.cedia.edu.ec/dmdocuments/PAQUETES%20DE%20SERVICIOS/colegios_servicios2019.pdf

Figura 19. Portafolio Colegios

PAQUETES DE PRESTACIONES — COLEGIOS

	CONECTIVIDAD			INFRAESTRUCTURA				MULTIMEDIA		DESARROLLO ACADÉMICO						CAPACITACIÓN	EVENTOS
		①		②		③	④							NUE. ⑤	NUE. ⑥	MEJ.	
	Red Avanzada (Mbps)	EDUROAM	Web Application Firewall	Videoconferencia multipunto	Grabación eventos y Transmisión en vivo	Seguridad Informática	Servidores virtuales Multiuso	Radio Online	Repositorio Multimedia	Envío de archivos (100Gb)	Repositorio de Objetos de Aprendizaje	Plataforma MOOC	Licencias Wolfram	Enciclopedia Britannica CloudLabs	Trofeo Colegial: (Fondos) - ecología - mate - química - robo - oratoria - literatura - ortografía - onu - gestion social / comunitaria	Capacitación EFC (cupos)	TICEC (profesores)
Plan Colegio Básico	60	✓	✓	1	✓	✓	✓	✓	✓	✓	✓	10	60	0	$941,02	0	1
Plan Colegio Intermedio	105	✓	✓	1	✓	✓	✓	✓	✓	✓	✓	15	100	1	$1.459,17	0	1
Plan Colegio Avanzado 1	150	✓	✓	2	✓	✓	✓	✓	✓	✓	✓	20	120	1	$1.977,33	1	2
Plan Colegio Avanzado 2	195	✓	✓	3	✓	✓	✓	✓	✓	✓	✓	25	150	1	$2.495,49	1	2
Plan Colegio Avanzado 3	240	✓	✓	4	✓	✓	✓	✓	✓	✓	✓	30	200	2	$3.013,65	3	3
Plan Colegio Personalizado	V	✓	✓	V	✓	✓	✓	✓	✓	✓	✓	V	V	V	✓	V	V

Fuente: CEDIA CSIRT. Paquete de servicio universidades. Ecuador 2019. [En Línea] [Consulta: 12 septiembre de 2020] Disponible en: https://www.cedia.edu.ec/dmdocuments/PAQUETES%20DE%20SERVICIOS/universidades_servicios2019.pdf

8.2 MODELO EN BASE A LA METODOLOGÍAS COHERENTES

8.2.1 Análisis del modelo. Luego de realizar la consulta de los diferentes modelos que se encuentran estructurados en los Grupos o centros de atención a incidentes de seguridad cibernética de la región de América latina, se toman modelos que pueden aportar al CSIRT de la empresa Cibersecurity de Colombia LTDA., donde se resalta la importancia de algunos, como lo son el modelo, Centralizado e Incrustado, siendo los más adecuados a implementar de manera documentada, viendo la necesidad del cliente al que va dirigidos los servicios de la empresa Cibersecurity de Colombia LTDA., el modelo centralizado permite tener un grupo de clientes de un mismo segmento, pues el CSIRT podría prestar los servicios a las Pymes del país, dado que es un sector bastante extenso, lo cual daría un gran crecimiento al CSIRT si se tiene en cuenta la cantidad de servicios solicitados.

El modelo centralizado, es utilizado en gran medida por los CSIRT que tienen un grupo de clientes dentro de un mismo país, como lo son los CSIRT, de Chile CLCERT y Brasil CERT.br, estos dos equipos prestan sus servicios a diferentes entidades en todo el territorio nacional, así mismo coordinan con los demás CSIRT del país, los incidentes de seguridad que deben ser de conocimiento del CSIRT coordinador en cada uno de sus países, es por esta razón que este modelo sería

el adecuado para el CSIRT de la empresa Cibersecurity de Colombia LTDA., pues atiende todos los servicios de la misma empresa y adicional podría centralizar los servicios o incidentes de todas las Pymes del país que estuvieran interesadas en adquirir servicios de defensa y monitoreo de ataques cibernéticos.

9 ATENCIÓN Y SEGUIMIENTO A INCIDENTES DE SEGURIDAD

9.1 DETECCIÓN DE INCIDENTES DE SEGURIDAD

9.1.1 Medios de detección. Dentro del medio para la detección de los incidentes de seguridad, la empresa Cibersecurity de Colombia LTDA., deberá establecer cuáles serán las herramientas tecnológicas o los medios que utilizara para la identificación de los incidentes de seguridad informática, con el fin de que puedan ser reportados o informados, a continuación, se listarán los que inicialmente utilizará.

9.1.1.1 Reporte de usuarios. Teniendo en cuenta que se trata de servicios que se ofrecerán tanto internamente a la empresa como a los clientes externos, la primera línea de reporte serán los usuarios, quienes deberán realizar dichos reportes al área de ciberseguridad, mediante los medios que establezca el CSIRT.

9.1.1.2 Monitoreo de sistemas de información. El CSIRT, deberá contar con las herramientas de protección y detección de incidentes necesarias, con el fin de que en la realización de monitoreo de la infraestructura de la empresa Cibersecurity de Colombia LTDA., así como en los clientes externos, estas permitan la visualización, detección y registro de los eventos de seguridad que no pueden ser detectados por los usuarios, con el fin de que se garantice la seguridad de la infraestructura.

9.1.1.3 Alertas de seguridad. Dentro las alertaras se pueden establecer los fallos de los servidores o caídas de servicio, las aplicaciones y demás herramientas de protección que se manejen, indicar que también se podría realizar una verificación de los logs de eventos de los sistemas de protección como antivirus, con el fin de ser analizados y posteriormente identificar posibles incidentes de seguridad.

9.2 REPORTE DE INCIDENTES

Dentro de la atención a los incidentes de seguridad de la información, es de suma importancia tener claro el proceso, tanto del equipo de especialistas y analistas del CSIRT, como de los usuarios quienes son las primeras personas en tener el contacto con el incidente de seguridad, cuando son reportados. En caso de que

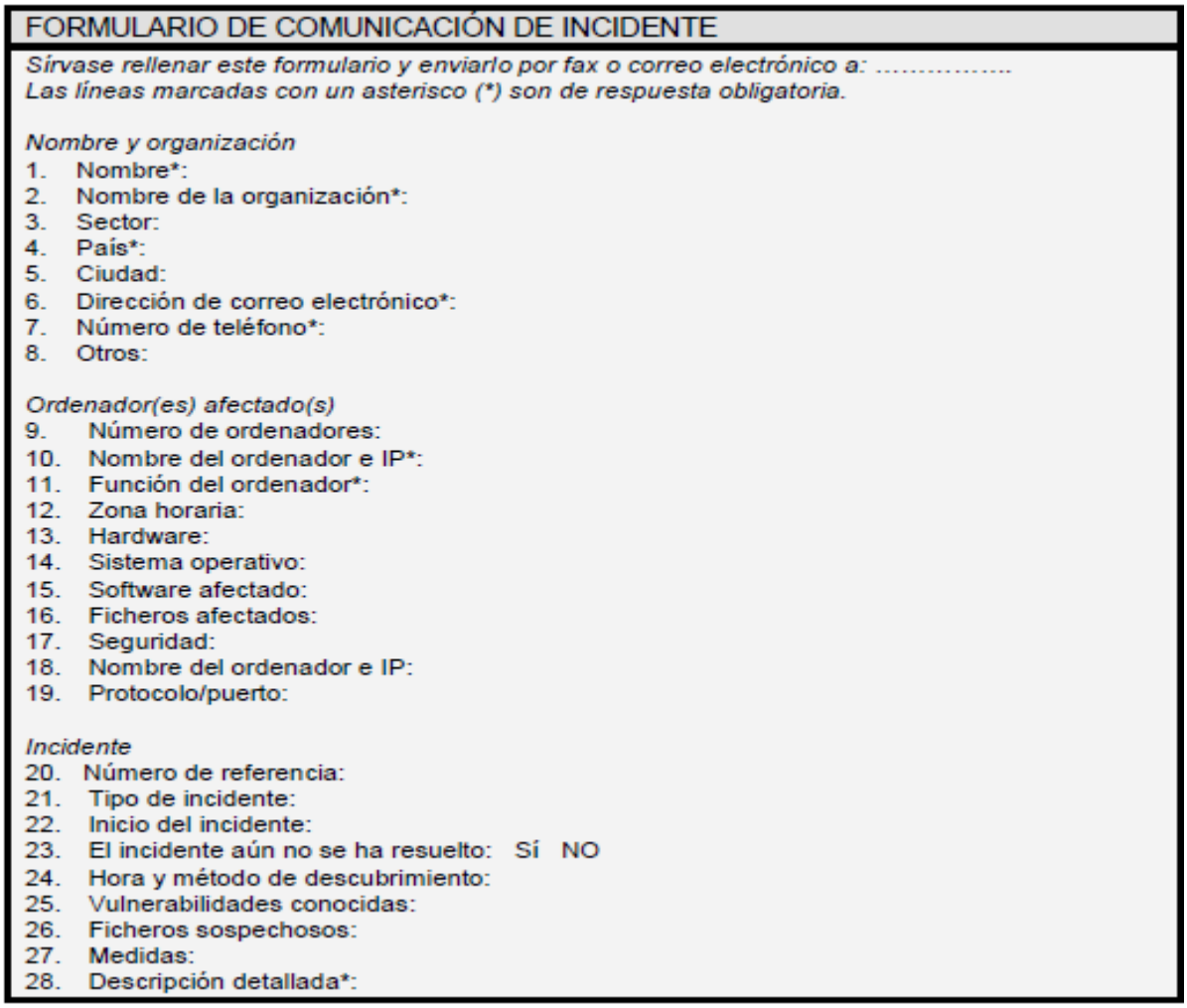
estos sean detectados por las herramientas o software de monitoreo y prevención, tendrían el primer contacto directamente los miembros del equipo, con el fin de que se garanticen el proceso y las políticas en la atención de incidentes, es importante que los usuarios o grupo de clientes, tengan pleno conocimiento del reporte de estos incidentes, pues la primera medida debería ser la capacitación de los usuarios, con el fin de que conozcan el proceso correcto de reporte de estos incidentes de seguridad, el cual se realizara inicialmente con un formato, donde se especifique la mayor cantidad de información posible para que el analista tenga herramientas de información suficientes para iniciar con el proceso de atención al reporte[167].

9.2.1 Medios de reporte. Los medios utilizados para el reporte de los incidentes de seguridad, inicialmente se realizará el reporte por correo electrónico y llamada telefónica para el caso de los incidentes de seguridad críticos, dentro del reporte por correo electrónico el usuario deberá tener el formato estipulado para realizar dicho reporte, con el fin de que se garantice la mayor cantidad de información posible y la claridad de la misma, ya si el analista que tenga asignado el incidente requiere de mayor información deberá tener contacto con el usuario que realiza el reporte, para el reporte de incidentes críticos, se realizara por medio de llamada telefónica, los usuarios deberán tener claro en la capacitación previamente indicada por el equipo del CSIRT, cuáles son las pautas para identificar un incidente categorizado como crítico, por lo que deberán llamar de inmediato al Equipo de Respuesta ante Incidencias de Seguridad Informáticas, donde el funcionario que atienda la llamada, deberá tener a la mano el formato, con el fin de realizar las preguntas adecuadas al usuario y así recolectar la mayor cantidad de información posible para iniciar el proceso de atención del reporte.

9.2.2 Formato de reporte. Con el fin de recolectar la mayor cantidad de información necesaria del incidente de seguridad de la información, es muy importante que se realice un reporte adecuado, tanto por parte de los usuarios como de los mismos miembros del equipo, el formato relaciona información importante que permite identificar el tipo de incidente, así como la categorización, el medio en el que se presentó, el daño que puede causar o está causando, así como los datos personales del usuario que realiza el reporte, área a la que pertenece, funciones, identificación del equipo de trabajo o dispositivo donde se presentó el incidente, dirección IP, hora y fecha. Etc. Todo con el fin de que se tenga la mayor fuente de información, tal como se observa en la Figura 20.

[167] SUPER INTENDENCIA DE SOCIEDADES. (Colombia) Guía Para la Gestión de Incidentes. [En línea] 2017 Colombia: [Consulta: 12-octubre-2019] P.11-18 Disponible en: https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Infraestructura%20Tecnologica/Documentos/GINT-G-006%20Gu%EDa%20Gestion%20de%20Incidentes.pdf

Figura 20. Contenido del reporte de incidente de seguridad.



FORMULARIO DE COMUNICACIÓN DE INCIDENTE

Sírvase rellenar este formulario y enviarlo por fax o correo electrónico a: ……..
Las líneas marcadas con un asterisco (*) son de respuesta obligatoria.

Nombre y organización
1. Nombre*:
2. Nombre de la organización*:
3. Sector:
4. País*:
5. Ciudad:
6. Dirección de correo electrónico*:
7. Número de teléfono*:
8. Otros:

Ordenador(es) afectado(s)
9. Número de ordenadores:
10. Nombre del ordenador e IP*:
11. Función del ordenador*:
12. Zona horaria:
13. Hardware:
14. Sistema operativo:
15. Software afectado:
16. Ficheros afectados:
17. Seguridad:
18. Nombre del ordenador e IP:
19. Protocolo/puerto:

Incidente
20. Número de referencia:
21. Tipo de incidente:
22. Inicio del incidente:
23. El incidente aún no se ha resuelto: Sí NO
24. Hora y método de descubrimiento:
25. Vulnerabilidades conocidas:
26. Ficheros sospechosos:
27. Medidas:
28. Descripción detallada*:

Fuente: AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. (Grecia). ENISA. Cómo crear un CSIRT paso a paso [En Línea] Producto WP2006/5.1(CERT-D1/D2) [Consulta: 12 abril de 2020]. P. 50. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

9.2.3 Creación del incidente. El incidente de seguridad deberá ser creado tan pronto se reporta, con el fin de que sea atendido en el menor tiempo posible, dependiendo de su nivel de criticidad, se le dará una clasificación, para que, a la hora de la asignación se dé prioridad a los más críticos, se podrán utilizar métodos como él (Triage), luego de la creación del incidente se llevara un registro en herramientas de información, que permitan realizar el seguimiento adecuado a cada uno de los incidentes asignados.

9.2.4 Registro de incidentes. dentro de esta etapa del registro es muy importante contar con la capacitación adecuada y así realizar un registro adecuado, para llevar este registro o base de datos, el CSIRT, deberá contar inicialmente con un sistema manual que le permita la automatización de los datos de registros, como también podría ser una bitácora o base de datos, bien sea mediante aplicativo o web, que le permita al funcionario, que recibe dicho incidente, poder registrarlo y así posteriormente el jefe de ciberseguridad quien lo recibiría, poder asignarlo a un especialista o analista dependiendo de la evaluación del impacto de este. Dentro del registro que se llevara, se deberá relacionar la mayor cantidad de información posible, con el fin de poder tener una base de datos completa, que luego sea de gran utilidad para la toma de decisiones y la misma gestión del incidente, conocida como base de conocimiento, dentro del registro que se debe realizar, se encontraran datos como[168]:

A. **Fecha y hora:** es de suma importancia poder tener establecidos los momentos exactos de la ocurrencia del evento presentado, lo cual será de gran ayuda para la gestión pues se deben establecer las medidas de protección lo antes posible.

B. **Resumen del reporte:** se deben establecer una serie de datos, como hardware, software, funcionarios, datos, lugares, procesos, etc. que permitan indicios de lo que sucedió y lo que pudo haber sucedido, con el fin de que el especialista o analista, tenga información suficiente para poder realizar una gestión adecuada.

C. **Datos de quien reporta:** se debe relacionar toda la información del usuario que realiza el reporte, así como el área donde se encuentra laborando, las funciones, puesto de trabajo, equipo de cómputo o dispositivo, en el cual se presentó el incidente de seguridad.

D. **Quien registra:** se debe llevar una secuencia lógica del incidente, donde cada uno de los especialistas o analistas que tiene contacto con el incidente, tenga que registrase con el fin de llevar la cadena de custodia del incidente hasta su finalización o cierre.

E. **Acciones realizadas:** se deben establecer todas las actividades desde el inicio al cierre de lo correspondiente con la gestión del incidente, con el fin de que mediante esta documentación se relacione el paso a paso, hasta su finalización.

[168] Ibid. P. 12

9.2.5 Asignación. La asignación de los incidentes de seguridad depende del jefe de ciberseguridad o los especialistas del área, los cuales tienen asignados unos grupos de analistas, siendo los actores principales en la atención de los incidentes, dicha selección se realizará de manera sistemática, solo será modificada en el caso de que se requiera asignar incidentes a especialistas por su nivel de impacto.

9.3 EVALUACIÓN

La atención de los incidentes de seguridad es muy importante, pues permite tener una correcta evaluación y análisis, lo que garantiza que el proceso de gestión de incidentes de seguridad sea el correcto y así mismo los resultados sean los esperados por el equipo de trabajo. De modo que mediante estas acciones necesarias se permitirá garantizar, los principios fundamentales de la seguridad de la información, la disponibilidad, integridad y confidencialidad de la información.

9.3.1 Evaluación. Con el fin de poder llevar a cabo una evaluación eficiente de un incidente de seguridad, es de suma importancia, poder tener presente los niveles de impacto que este genera o puede generar, sobre los servicios y procesos, así mismo se debe considerar los grados de seguridad que se tienen, según sea el tipo de incidente, ya que mediante esta evaluación, se podrán categorizar dichos incidentes de seguridad, lo cual permite que se realicen acciones diferentes en la solución de los mismos, los diferentes niveles de impacto en los incidentes se podrán observar en la Figura 21.

Figura 21. Nivel de impacto en los incidentes de seguridad

Fuente: Elaboración Propia.

9.3.1.1 Impacto crítico. Dentro de este nivel de impacto, podemos encontrar incidentes de seguridad, los cuales se generan, en ataques dirigidos como los APT, así mismo se pueden relacionar otros como los de ciberterrorismo, los de ataque a infraestructuras críticas, como lo de tipo, daños informáticos PIC.

A. **APT:** este tipo de ataques se consideran como los más perjudiciales para cualquier víctima, su impacto es muy alto, si se tiene en cuenta que dichos ataques siempre llevan un tiempo de preparación y organización, pueden ser planeados por una o más personas, este tipo de ataques se realizan para generar un gran impacto en el medio, buscando que sea de connotación nacional, las principales víctimas de estos ataques son las organizaciones militares, de gobierno, compañías de alto valor. Etc.

A. **Ciberterrorismo:** este tipo de ataque está dirigido a diferentes sectores, como Gobiernos, con el fin de ser desestabilizados, organizaciones militares, con el fin de propiciar guerras, elecciones presidenciales, con el fin de saborear dichos procesos, otro ejemplo podría ser los ataques propiciados a organizaciones como la NASA, EFBI, CIA. etc.

B. **Daños informáticos PIC:** los ataques PCI, son ataques a la infraestructura crítica de un país, ejemplo el borrado de una base de datos de la registraduría nacional, corrupción de información importante como el censo nacional, entre otro tipo de ataques que logran establecer medidas drásticas para su solución y recuperación.

9.3.1.2 Impacto alto. Dentro del impacto alto de incidentes de seguridad de la información, se establecen ataques, como los que pueden afectar seriamente un sistema de información, desde la destrucción de la información, como también los ataques que buscan la lectura de puertos abiertos en una red, entre otros que puedan afectar a los sistemas de una organización, logrando detener su funcionamiento o producción.

Phishing: envío de correos electrónicos con un único fin, realizar una suplantación de identidad y que la víctima envíe información confidencial o personal, como datos de la compañía, información de interés personal, la cual pueda ser utilizada para cometer otros delitos informáticos o penales.

DDoS: ataque de denegación de servicio, este tipo de ataques están bien preparados con un único fin, atacar infraestructuras tecnológicas o sistemas, así como redes de información, estos ataques pueden utilizar paquetes SYN, así como servicios basados en UDP, con el fin de poder detener los procesos y servicios.

Ingeniería social: se caracteriza por la consulta o adquisición de información, mediante estrategia, para que la víctima no se entere, que es ella misma quien está proporcionando la información, sin darse por enterada, una forma puede ser las llamadas telefónicas, las observaciones, la recolección de documentos desechados entre otros.

Sniffing: análisis de las redes de comunicación, con el fin de obtener información que se trasmite por estas.

Scanning: este ataque se caracteriza por el escaneo de puertos en las redes de comunicación, con el fin de poder dirigir ataques por las vulnerabilidades descubiertas mediante este tipo de ataques.

9.3.1.3 Impacto medio. Los ataques que se pueden clasificar en este nivel son los que corresponden a interrupción de actividades, pérdida de datos, como la propagación de virus Troyanos, virus que reproducen contenido sexual, pornografía infantil, los cuales se reproducen al momento de abrir los navegadores.

Troyanos: virus, que pueden detener procesos, brinda información falsa al usuario, indicando que su equipo está infectado por muchos virus y que es necesario que se descarguen otros programas para limpiarlo, para luego descargar otros virus, que los pueden hacer pasar como programas oficiales o legítimos.

Malware: este tipo de virus ocasiona fallas en los sistemas, duplica procesos e información, altera el funcionamiento de los equipos de cómputo, secuestra datos que considera importantes, en ocasiones toma el control del sistema operativo.

9.3.1.4 Impacto bajo. Los incidentes de seguridad, clasificados con impacto bajo, se pueden mencionar algunos que no generan algún tipo de alerta grave y que no causan daños a las infraestructuras de los clientes, tampoco afectan los principios básicos de la seguridad de la información, (disponibilidad, integridad y Confidencialidad) uno de los ejemplos de estos ataques son los siguientes.

Spam: un sistema de información infectado por virus, como también un sistema operativo o aplicaciones que fueron infectadas por virus, los cuales ralentiza los procesos, pero no causan mayor daño. Pueden ser los correos electrónicos masivos, que buscan instalar algún tipo de virus para publicidad comercial.

9.3.1.5 Valor del Impacto. En el Cuadro 3 se observa el nivel de criticidad de los impactos, así como el valor numérico que se puede dar a cada uno de los niveles, dependiendo de los factores del incidente que se atiende, de esta manera se podrá implementar procesos de avaluación como él TRIAGE.

Cuadro 3. Valores de criticidad de los impactos

Impacto	Bajo	Medio	Alto	Critico
Bajo			5	5
		5		
	5			4
Medio			4	
		4		
	4			3
Alto			3	2
		3	2	2
	3	2	2	1
Critico	2	2	1	1
	1	1	1	1

Fuente: Elaboración propia

9.3.2 Tiempos de respuesta. Este término es muy importante, pues se debe establecer unos tiempos de terminados de respuesta a cada uno de los incidentes que se reporten, de esta manera se cumplirán las políticas de respuesta a incidentes de seguridad y los procesos establecidos por el CSIRT, así mismo el analista que esté a cargo de dicho incidente, tendrá un control de este, pues debe saber el tiempo que tiene para la respuesta de determinado incidente, según la cantidad que tenga asignada, en el cuadro 4. Se verán los estos tiempos según el impacto de cada incidente de seguridad.

Cuadro 4. Tiempo de respuesta

Impacto	Valor Numérico	Tiempo
Bajo	5	24. Horas
Medio	4	10. Horas
Alto	3	7. Horas
Critico	2	4. Horas
	1	2. Horas

Fuente: Elaboración Propia.

9.4 GESTIÓN DE INCIDENTES

9.4.1 Preparación del incidente. Para la respectiva gestión de un incidente de seguridad se debe, dar preparación al mismo, desde el momento en que se recibe, se asigna, la evaluación que se realiza, la categorización según el nivel de impacto, entre otras actividades que se deben tener en cuenta para lograr iniciar con la gestión correspondiente de atención y solución.

9.4.2 Identificación. Es preciso realizar una identificación del incidente, con el fin de poder entenderlo y solucionarlo, dentro de los aspectos para tener en cuenta se debe tener la mayor cantidad de información, así lograr identificar su posible solución, se debe realizar una observación profunda de las evidencias recolectadas durante la evaluación y análisis, con el fin de que se apliquen las herramientas necesarias para su proceso de verificación y respuesta.

9.4.3 Contención. Esta es una de las etapas más críticas de la gestión del incidente, ya que se debe mitigar y contener el ataque, por lo que se deben poner en funcionamiento y en actividad todas las herramientas disponibles para la pronta contención de los daños que se estén causando a los sistemas atacados, con el fin de evitar que estos puedan afectar a otros, así mismo es de suma importancia que se solicite el apoyo correspondiente a otros integrantes del grupo, con el fin de evaluar daños y reducir el impacto.

9.4.4 Mitigación. Dentro de la fase de mitigación, se deben tomar medidas rápidamente, pues si hablamos de un ataque de denegación, este podría causar daños irreversibles, ejemplo el borrado de información, de manera que se debe actuar rápidamente, contar con el apoyo de personal especializado para tomar las medidas necesarias y perder eliminar el ataque, se debe tratar en lo posible de contar inicialmente o prioritariamente con una copia de seguridad de los sistemas atacados, dicha copia de seguridad en lo posible debe ser limpia, otra medida importante para tomar es la de eliminación del software el cual está siendo o fue utilizado por el atacante.

9.4.5 Recuperación. El estado de recuperación debe ser cuidadoso, por lo que no se deben realizar acciones o tomar decisiones precipitadamente, se debe establecer medidas que garanticen que los sistemas afectados puedan estar limpios y que no estén vulnerables aun, se debe dar recuperación a la operación en su estado normal, garantizando que las áreas afectadas puedan operar nuevamente sin la incertidumbre de que puedan ser atacados doblemente, es necesario realizar un monitoreo a los sistemas que fueron atacados por un tiempo prudencial.

9.4.6 Post incidente. Para finalizar se deben llevar a cabo las respectivas evaluaciones de los daños y las perdidas, tanto de información como de tiempos de operación, detallando y documentando el incidente de manera cronológica desde que se inició la gestión hasta que se realiza la respectiva recuperación de los sistemas, adicional se deben establecer con el equipo de trabajo las lecciones aprendidas del incidente, dejan historial en la base de conocimiento, así mismo realizar el respectivo informe de la respuesta del incidente, con el fin de que el jefe atienda los requerimientos a que haya lugar en caso de que se tengan daños de consideración.

En la Figura 22. Se observa esquema de relación, de cada una de las fases de atención a incidentes de seguridad de la información, la cual será establecida por el CSIRT, en la empresa Cibersecurity de Colombia LTDA.

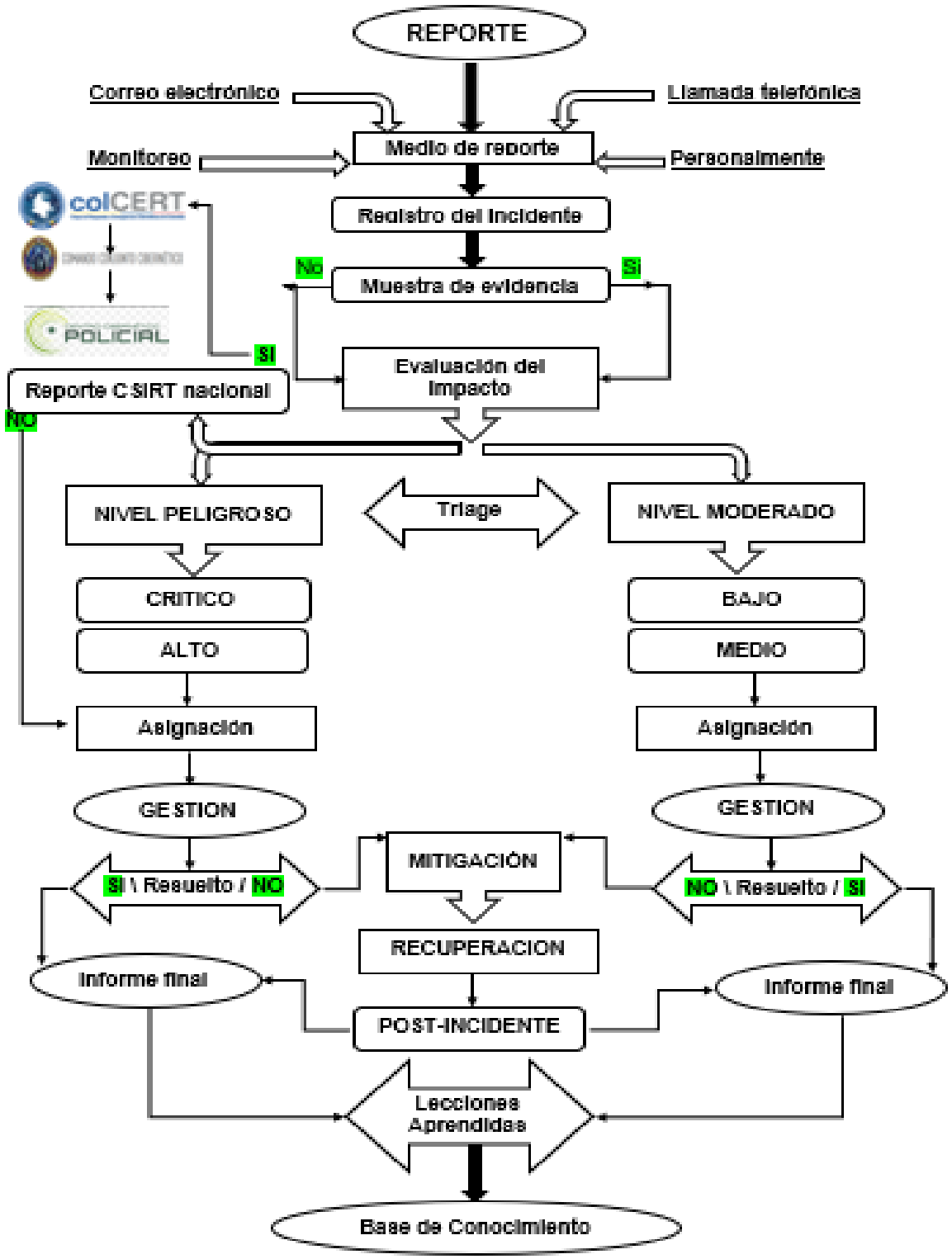
Figura 22. Fases de la gestión de un incidente de seguridad

Fuente: Consejo Nacional de Ciberseguridad. [Ren Línea] Guía nacional de notificación y gestión de ciber incidentes.: España. [Consulta: 12 de octubre de 2019] P. 29-55 Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

9.4.7 Modelo de atención a incidentes. Como se ha venido desarrollando el presente proyecto, es muy importante realizar un modelo de atención a incidentes de seguridad informática, donde se determine el ciclo de vida de cada uno de los incidentes de seguridad de la información, tal como se ha indicado en el presente capitulo, donde se manifestó desde el inicio de la atención, registro y asignación, de los incidentes de seguridad hasta la respuesta al mismo con el respectivo informe.

En la Figura 23. Se observa el modelo de atención a incidentes que se implementará en el CSIRT, lo que abarca todos los puntos de vista de la atención y evaluación del incidente hasta su finalización, así como las lesiones aprendidas las cuales sirven para la base de conocimiento, entendiendo que se cuenta con esta experiencia y es fundamental para los nuevos reportes que se realicen y poder evitar futuros incidentes reportados por los usuarios y solucionarlos de una manera más eficiente, donde se identifican con características similares.

Figura 23. Modelo de atención a incidentes de seguridad



Fuente: Elaboración Propia.

10 DEFINICIÓN DE PERFILES Y ORGANIGRAMA DEL CSIRT

En el presente capítulo se establecerán puntos importantes que se requieren en la estructuración del CSIRT, se debe establecer un esquema que le permita al CSIRT, poder darse a conocer, un punto importante es el desarrollo de su Misión y Visión, donde se dará una orientación del CSIRT al futuro, así mismo se establecerá un organigrama donde se podrá evidenciar la estructura interna que tiene la empresa Cibersecurity de Colombia LTDA., se especificarán todos los perfiles que debe tener el CSIRT, como las funciones de cada uno, los roles que deben cumplir dentro del área que se encuentran asignados, la experiencia que se debe requerir para asumir el cargo, los diferentes aspectos educativos con los que debe contar el candidato a la hora de ser perfilado para el cargo, entre otra importante información que el perfil del candidato debe reunir con el fin de poder hacer parte del CSIRT de empresa Cibersecurity de Colombia LTDA.

10.1 MISIÓN Y VISIÓN DEL CSIRT

Es importante el diseño de la Visión y Misión del CSIRT, de manera que, mediante esta se pueden realizar los procesos a los cuales le apunta el CSIRT, en conjunto con los objetivos es importante conocer, cual es la proyección del centro de respuesta a incidentes informáticos, siendo la carta de presentación ante sus clientes y demás consultores o visitantes, de acá la importancia de poder estructurar la Visión y Misión, de una manera coherente, según los servicios y la orientación que se pretenda dar, así como también una manera eficaz que permita identificar cada aspecto a tener en cuenta, de la proyección a la que se debe apuntar, pues, al comunicar la Visión y Visión, esto permite que las empresas conozcan más de fondo el negocio, permitiéndoles tener una pequeña introducción del CSIRT y así se interesen por los servicios que se ofertan, igualmente ayudara a la identificación de problemas internos, dado que serán identificados antes de su implementación, pues con la Visión y Visión, se da una ruta que permitirá fijar ciertos criterios, que ayudaran a la orientación y proyección del CSIRT, siendo la manera para empezar a promocionar el centro de atención a incidentes, por parte de la empresa Cibersecurity de Colombia LTDA.

10.1.1 Misión. Garantizar las condiciones necesarias para el aseguramiento de las plataformas tecnológicas de la empresa Cibersecurity de Colombia LTDA y demás clientes., como apoyo y centro de referencia en seguridad de la información, en las nuevas tecnologías para las pymes en Colombia, en la atención, prevención y respuesta a incidentes de seguridad informática.

10.1.2 Visión. Para el año 2025. Ser reconocida a nivel nacional, como una de las cinco mejores compañías de ciberseguridad en la prevención y protección en materia de delitos informáticos.

10.2 DEFINICIÓN DE ROLES Y PERFILES

La perfilación del equipo es de suma importancia, teniendo en cuenta que se debe garantizar una contratación de personal capacitado y capaz, de llevar a cabo las funciones que le serán encomendadas en las actividades diarias dentro de sus funciones asignadas, por lo que se debe elaborar un perfil que cumpla con todas y cada una de las condiciones necesarias para que se pueda afianzar en dicho lugar de trabajo, así como para que aporte todo su conocimiento y experiencia al Equipo de Respuesta ante Incidencias de Seguridad Informáticas CSIRT, en la atención y solución de incidentes de seguridad y ciberseguridad informática. Se realizará un perfilamiento de cada uno de los perfiles requeridos dentro de la operación del CSIRT, donde se destacarán los requerimientos del talento humano necesario, así como la especificación técnica de cada uno de los perfiles que conforman el grupo, en sus diferentes áreas, así mismo los requerimientos educativos y capacidades que cada uno de ellos debe tener para formar parte del Equipo de Respuesta ante Incidencias de Seguridad Informáticas.

10.2.1 Dirección de Tecnología. Es el encargo de la dirección con más jerarquía y responsabilidad, quien toma las decisiones que puedan afectar o mejorar las condiciones del CSIRT, así mismo establece total compromiso y lleva a cabo la planificación estratégica de cara a la operación, así como, ante los clientes y los medios, por lo que debe tener claros los procesos y actividades que desarrolla el CSIRT, También establece acuerdos de cooperación con otras organizaciones y sirve de enlace con el Comité Directivo de los demás CSIRT nacionales e internacionales. El director del CSIRT también actúa como portavoz dentro de la empresa Cibersecurity de Colombia LTDA.

10.2.1.1 Perfil. Debe ser una persona con liderazgo, igualmente es muy importante que cuente tanto con los conocimientos, tanto administrativos, políticos, manejo de personal, de ciberseguridad y técnicos requeridos para este cargo, debe ser un perfil en lo posible muy completo, con una experiencia certificable y con una recomendación de peso por una institución o persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.1.2 Formación académica. Los requisitos académicos que este cargo requiere se establecerán de la siguiente manera:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Maestría o Doctorado en seguridad de la información o seguridad Informática.
Certificaciones en Seguridad (CISSP, ISO 27001, CISM, CISA o similar).

B. Se valorará:
Postgrado en Gerencia de proyectos o similares.
Cursos o seminarios internacionales en Ciberseguridad.

10.2.1.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como director o jefe de alguna compañía reconocida, en relación con el perfil y cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado director.
Más de 12 años de experiencia en áreas técnicas en TI o Seguridad de la información.
Más de 6 años en gerencia de TI.
Haber desarrollado o liderado un proyecto de seguridad.
Manejo de personal por más de 10 años.
Soporte técnico en temas de seguridad por más de 8 años.

B. Se valorará:
Experiencia en posiciones similares.

10.2.2 Jefe de operaciones. Es el cargo de más jerarquía en cuanto a la operación del CSIRT, depende del director de tecnología, es quien toma las decisiones referentes a la operación del CSIRT, así mismo establece la planificación estratégica, de cara a la operación y los clientes, debe tener claros los procesos y actividades que desarrolla el CSIRT, así como el escalamiento de los incidentes de seguridad de infraestructura crítica y de gran impacto, con el fin de que sean notificados al director de tecnología y este los escale con el (colCERT). También establece coordinaciones con otras organizaciones externas en materia. Así como debe ser el coordinador de las solicitudes de apoyo por parte de los Coordinadores, en cuanto a las demás direcciones y áreas de la empresa, como (Jurídica y Recursos Humanos), la primera con el fin de que apoye los temas legales de los incidentes de seguridad que se requieran y la segunda en temas de contratación con los perfiles necesarios para la operación, Es el directo responsable de la operación de incidentes de seguridad e infraestructura, las 24 horas al día, los 365 días al año, dentro de la empresa Cibersecurity de Colombia LTDA.

10.2.2.1 Perfil. Debe ser una persona con liderazgo, igualmente es muy importante que cuente tanto con los conocimientos técnicos, administrativos y manejo de personal, para este cargo debe ser un perfil, en lo posible muy completo, con una experiencia certificable en seguridad de la información, tanto técnica como administrativa, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.2.2 Formación académica. Los requisitos académicos de este cargo, deben ser técnicos y administrativos, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Especialización o maestría en seguridad de la información o seguridad informática.
Certificaciones en Seguridad (ISO 27001, CISM, CISA, VMware, CCNP).

B. Se valorará:
Postgrado en Gerencia de proyectos o similares.

10.2.2.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Coordinador o jefe de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Coordinador o jefe de sistemas.
Más de 8 años de experiencia en áreas técnicas en TI o Seguridad de la información.
Más de 5 años en gerencia de TI.
Haber liderado un proyecto de seguridad.
Manejo de personal por más de 8 años.
Soporte técnico en temas de seguridad por más de 8 años.

B. Se valorará:
Experiencia en posiciones similares.

10.2.3 Coordinador de infraestructura. Cargo coordinación de operación del área de infraestructura, depende del jefe operativo, es quien toma las decisiones referentes a los incidentes internos de seguridad de la información y el soporte a la infraestructura tecnológica de la empresa Cibersecurity de Colombia LTDA, dentro de la operación cuenta con un grupo de especialistas, analistas de TI y técnicos, así mismo establece la planificación estratégica, de cara a la operación del área de infraestructura, informa al Jefe de Operación, las necesidades de coordinar apoyo de otras áreas de la empresa, debe tener claros los procesos y actividades que desarrolla el CSIRT dentro de su área, También establece coordinaciones con el Área de ciberseguridad para el escalamiento de incidentes de mayor impacto. Es el directo responsable de la operación, las 24 horas al día, los 365 días al año, de la infraestructura tecnológica, de la empresa Cibersecurity de Colombia LTDA.

10.2.3.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos y manejo de personal, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información e infraestructura, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.3.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas, debido a que se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Especialización en seguridad de la información o seguridad informática.
Certificaciones en Seguridad (ISO 27001, ITIL, VMware, CCNP. RED HAT)

B. Se valorará:
Postgrado en Gerencia de proyectos o similares.

10.2.3.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Especialista o Coordinador de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Especialista o Coordinador.
Más de 5 años de experiencia en áreas técnicas en TI y Seguridad de la información.

Más de 3 años en gerencia de TI.
Manejo de personal por más de 4 años.
Soporte técnico en temas de seguridad por más de 5 años

B. Se valorará:
Experiencia en posiciones similares.

10.2.4 Coordinador de ciberseguridad. Cargo Coordinación de operación del área de ciberseguridad, depende del jefe operativo, es quien toma las decisiones referentes a los incidentes internos y externos de seguridad de la información, así como los relacionados con Informática Forense, dentro de la operación cuenta con un grupo de especialistas, analistas y técnicos de ciberseguridad, así mismo establece la planificación y coordinación estratégica, de cara a la operación del área de ciberseguridad, informara al jefe de operación, las solicitudes de apoyo de áreas como (Jurídica y Recursos humanos), así como el escalamiento de los incidentes de seguridad de infraestructura crítica y de gran impacto. Debe tener claros los procesos y actividades que desarrolla el CSIRT dentro de la empresa Cibersecurity de Colombia LTDA., También establece coordinaciones con el área de infraestructura cuando lo requiera según las necesidades de la operación. Es el directo responsable de la operación, las 24 horas al día, los 365 días al año, de todos los incidentes de seguridad de la información, internos y externos del CSIRT.

10.2.4.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos y manejo de personal, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.4.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas ya que se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Especialización en seguridad de la información o seguridad Informática.
Certificaciones en Seguridad (ISO 27001, CISM, CISA, CCNP. RED HAT, NIST, HIPPA, GDPR).

B. Se valorará:
Postgrado en Gerencia de proyectos o similares.

10.2.4.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Especialista o Coordinador de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Especialista o Coordinador.
Más de 5 años de experiencia en áreas técnicas en Seguridad de la información.
Más de 1 año en gerencia de seguridad de la información.
Manejo de personal por más de 3 años.
Soporte técnico en temas de seguridad por más de 6 años.

B. Se valorará:
Experiencia en posiciones similares.

10.2.5 Especialista en Ciberseguridad. Cargo Especialista en Ciberseguridad de operación, depende del Coordinador de Ciberseguridad, es quien apoya en las decisiones referentes a los incidentes internos y externos de seguridad de la información, Encargado de todo los incidentes de ciberseguridad de los clientes internos y externos de la empresa Cibersecurity de Colombia LTDA., dentro de la operación cuenta con un grupo de analistas de ciberseguridad, que son la primera línea de atención a los incidentes, así mismo establece la planificación estratégica, de cara a la operación del área de ciberseguridad, solicita al jefe de Ciberseguridad el apoyo de otras áreas, y escala los incidentes de infraestructura crítica y de alto impacto. Debe tener claros los procesos y actividades que desarrolla el CSIRT dentro de la empresa Cibersecurity de Colombia LTDA., deben ser el apoyo al área de infraestructura cuando lo requiera según las necesidades de la operación, en caso de que se requiera, todos los incidentes de alto impacto o importancia deben pasar por el área de ciberseguridad, donde se determinara el tiramiento y ciclo de vida del incidente. Es el directo responsable de la operación, las 24 horas al día, los 365 días al año, de todos los incidentes de seguridad de la información, internos y externos del CSIRT.

10.2.5.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos y manejo de personal, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.5.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas, pues se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Especialización en seguridad de la información o seguridad Informática.
Certificaciones en Seguridad (ISO 27001, CISM, CCNP).

B. Se valorará:
Postgrado en Gerencia de proyectos o similares.
Certificaciones en Seguridad (RED TAH, CISA).

10.2.5.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Analista de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Analista.
Más de 5 años de experiencia en áreas técnicas en Seguridad de la información.
Manejo de personal por más de 2 años.
Soporte técnico en temas de seguridad por más de 5 años.

B. Se valorará:
Experiencia en posiciones similares.
Más de 1 año en gerencia de seguridad de la información.

10.2.6 Especialista en Informática Forense. Cargo Especialista de informática Forense del área de ciberseguridad, depende del Coordinador de Ciberseguridad, Encargado de la atención de todos los incidentes de Informática forense de los clientes internos y externos de la empresa Cibersecurity de Colombia LTDA., dentro de la operación cuenta con el apoyo del Coordinador de Ciberseguridad y el Analista de Informática forense, así como del personal designado del área de Jurídica en todos los temas relacionados con evidencias, cadena de custodia y procesos judiciales y penales que se deriven de la atención de estos incidentes, así mismo establece la planificación en respuesta de los incidentes de Informática forense, debe tener claros los procesos y actividades que desarrolla en el CSIRT, en lo referente a la atención de incidentes de Informática forense, dentro de la empresa Cibersecurity de Colombia LTDA., debe escalar los incidentes o casos de relevancia al jefe de Ciberseguridad, será el apoyo, de los especialistas del área de infraestructura cuando lo requiera según necesidades del servicio, Es el directo responsable, las 24 horas al día, los 365 días al año, de todos los incidentes de Informática forense, internos y externos que le sean asignados a su grupo de trabajo.

10.2.6.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.6.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas, pues se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:

Profesional en cualquier área de sistemas de la información.
Especialización en seguridad de la información o seguridad Informática.
Diplomado certificado de análisis forense.
Certificación en Informática forense.
Certificaciones en Seguridad (ISO 27001, NIAs, CHFI, CCFP).

B. Se valorará:

Postgrado en Gerencia de proyectos o similares.

10.2.6.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Analista de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Analista.
Más de 6 años de experiencia en áreas técnicas en Seguridad de la información e Informática forense.
Manejo de personal por más de 2 años.
Soporte técnico en temas de seguridad por más de 5 años.

B. Se valorará:
Experiencia en posiciones similares.
Más de 1 año en gerencia de seguridad de la información.

10.2.7 Especialista Voz IP y Telefonía Móvil. Cargo Especialista, depende del Coordinador de Infraestructura, es quien se encarga del soporte de telefonía móvil y Voz IP, de la empresa Cibersecurity de Colombia LTDA., con el apoyo de los analistas que le sean asignados, realizando la verificación de seguridad en los equipos de telefonía móvil de la compañía, que a su vez son asignados a los empleados, dentro de la operación y que también sufren ataques informáticos, generando incidentes de seguridad, por lo que se requiere de todo el soporte en general, así mismo debe establecer la planificación estratégica, de cara a la operación del área de infraestructura, referente a su cargo y funciones, debe tener claros los procesos y actividades que desarrolla dentro del CSIRT, Establecerá coordinaciones con los especialistas del área ciberseguridad y escalara los incidentes de alto impacto. Es el directo responsable del soporte y atención de los incidentes de seguridad de Telefonía Móvil y Voz IP de la operación, las 24 horas al día, los 365 días al año, de la empresa Cibersecurity de Colombia LTDA.

10.2.7.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos y manejo de personal, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información y Telefonía Móvil y Voz IP, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.7.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas ya que se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Especialización en seguridad de la información o seguridad Informática.
Certificaciones en Seguridad (ISO 27001, GRANDSTREAM, CCNA, CCNP).

B. Se valorará:
Diplomados en manejo de equipos móviles.
Certificaciones de seguridad digital.

10.2.7.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Especialista de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado especialista.
Soporte técnico en temas de seguridad, Telefonía Móvil y Voz IP, por más de 5 años.
Manejo de personal por más de 2 años.

B. Se valorará:
Experiencia en áreas técnicas en TI o Seguridad de la información.
Experiencia en posiciones similares.

10.2.8 Especialista Infraestructura y Redes. Cargo Especialista en redes, depende del Coordinador de Infraestructura, es quien se encarga del soporte de infraestructura y redes, de la empresa Cibersecurity de Colombia LTDA., atiende los incidentes de seguridad Informática internos, de las redes y la infraestructura tecnológica de la compañía, con el apoyo de los analistas que le sean asignados, así mismo debe establecer la planificación estratégica, de cara a la operación del área de infraestructura, referente a su cargo y funciones, debe tener claros los procesos y actividades que desarrolla dentro del CSIRT. Establecerá coordinaciones de apoyo a los especialistas del área ciberseguridad y escalará los incidentes de alto impacto. Es el directo responsable del soporte y atención de los incidentes de seguridad de redes y la infraestructura tecnológica de la operación, las 24 horas al día, los 365 días al año, de la empresa Cibersecurity de Colombia LTDA.

10.2.8.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos y manejo de personal, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información, redes e infraestructura tecnológica, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.8.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas ya que se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Especialización en seguridad de la información o seguridad Informática.
Certificaciones (ISO 27001, CCNA, CCNP).

B. Se valorará:
Certificaciones en Seguridad similares.

10.2.8.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Especialista de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado especialista.
Soporte técnico en temas de seguridad, redes e infraestructura tecnológica, por más de 6 años.
Manejo de personal por más de 2 años.
Experiencia en áreas técnicas en TI, Redes o Seguridad de la información más de 5 años.

B. Se valorará:
Experiencia en posiciones similares.

10.2.9 Especialista SO - Linux - UNIX - Windows. Cargo Especialista Sistemas Operativos, depende del Coordinador de Infraestructura, es quien se encargan del soporte de los sistemas operativos Linux - UNIX – Windows - iOS, de la empresa Cibersecurity de Colombia LTDA., atiende los incidentes de seguridad Informática internos, en lo referente a todos los sistemas operativos instalados en los equipos de trabajo de la compañía, con el apoyo de los analistas que le sean asignados, así mismo debe establecer la planificación estratégica, de cara a la operación del área de infraestructura, referente a su cargo y funciones, debe tener claros los procesos y actividades que desarrolla dentro del CSIRT, Establecerá coordinaciones de apoyo a los especialistas del área ciberseguridad y escalara los incidentes de alto impacto. Es el directo responsable del soporte y atención de los incidentes de seguridad de SO - Linux - UNIX - Windows de la operación, las 24 horas al día, los 365 días al año, de la empresa Cibersecurity de Colombia LTDA.

10.2.9.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos y manejo de personal, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información, SO - Linux - UNIX – Windows, iOS, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.9.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas, pues se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Especialización en seguridad de la información o seguridad Informática.
Manejo de Sistemas operativos Linux - UNIX – Windows - iOS, así como servidores.
Certificaciones (ISO 27001, RED HAT, MCSA).

B. Se valorará:
Certificaciones en Seguridad informática.

10.2.9.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Especialista de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado especialista.
Soporte técnico en temas de seguridad, Sistemas operativos Linux - UNIX – Windows, por más de 6 años.

Manejo de personal por más de 2 años.
Experiencia en áreas técnicas en TI, Redes o Seguridad de la información por más de 4 años.

B. Se valorará:
Experiencia en posiciones similares.

10.2.10 Analista en Ciberseguridad. Cargo Analista de operación del área de ciberseguridad, depende del Coordinador y Especialista de Ciberseguridad, Encargado en la atención de todos los incidentes de ciberseguridad de los clientes internos y externos de la empresa Cibersecurity de Colombia LTDA., dentro de la operación cuenta con el apoyo del Especialista de ciberseguridad, así mismo establece la planificación en respuesta de los incidentes del área de ciberseguridad, debe tener claros los procesos y actividades que desarrolla el CSIRT en lo referente a la atención de incidentes de seguridad de la información, dentro de la empresa Cibersecurity de Colombia LTDA., debe informar los incidentes de alto impacto, deben ser el apoyo de los analistas del área de infraestructura cuando lo requiera según las necesidades, Es el directo responsable, las 24 horas al día, los 365 días al año, de todos los incidentes de seguridad de la información, internos y externos que le sean asignados.

10.2.10.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.10.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas, pues se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en cualquier área de sistemas de la información.
Certificaciones en Seguridad (ISO 27001, CISA).

B. Se valorará:
Especialización en seguridad de la información o seguridad Informática.

10.2.10.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Analista de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Analista.
Más de 3 años de experiencia en áreas técnicas en Seguridad de la información.
Más de 2 año en respuesta a incidentes de seguridad de la información.

B. Se valorará:
Experiencia en posiciones similares.

10.2.11 Analista en Informática Forense. Cargo Analista de informática Forense del área de ciberseguridad, depende del Coordinador y Especialista de Informática forense de Ciberseguridad, Encargado en la atención de todos los incidentes de ciberseguridad de Informática forense de los clientes internos y externos de la empresa Cibersecurity de Colombia LTDA., dentro de la operación cuenta con el apoyo del Especialista de Informática forense, así mismo establece la planificación en respuesta de los incidentes de informática forense, debe tener claros los procesos y actividades que desarrolla en el CSIRT, en lo referente a la atención de incidentes de informática forense, dentro de la empresa Cibersecurity de Colombia LTDA., informara de todos los incidentes de impacto alto y solicitara el apoyo del analista de jurídica, deben ser el apoyo de los analistas del área de infraestructura cuando lo requiera según las necesidades, Es el directo responsable, las 24 horas al día, los 365 días al año, de todos los incidentes de informática forense, internos y externos que le sean asignados.

10.2.11.1 Perfil. Debe ser una persona con liderazgo, es muy importante que cuente con los conocimientos técnicos requeridos, para este cargo debe ser un perfil, competitivo, con una experiencia certificable en seguridad de la información, debe ser una persona destacada en el medio, que cumpla con las necesidades del cargo.

10.2.11.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas, pues se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en el en cualquier área de sistemas de la información.
Diplomado en informática Forense.
Certificaciones en Seguridad (ISO 27001, NIAs, CHFI, CCFP).

B. Se valorará:
Especialización en seguridad de la información o seguridad informática.

10.2.11.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Analista de alguna compañía o área importante de la misma, con relación al cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Analista.
Más de 3 años de experiencia en áreas técnicas en Seguridad de la información.
Más de 2 año en respuesta a incidentes de informática forense.

B. Se valorará:
Experiencia en posiciones similares.

10.2.12 Analista de Infraestructura. Cargo Analista, depende de los especialistas de Infraestructura, son quienes se encargaran del soporte de toda la infraestructura tecnológica de la empresa Cibersecurity de Colombia LTDA., cubriendo todos los servicios de (Telefonía Móvil - Voz IP, Infraestructura - Redes y SO - Linux - UNIX - Windows) con el apoyo de los especialistas del área, realizando la verificación y respuesta de todos y cada uno de los incidentes de seguridad de la información, que se reporten de los usuarios internos, así mismo se debe atender todo el soporte en general, se debe establecer la planificación estratégica, de cara a la operación del área de infraestructura, referente a su cargo y funciones, deben tener claros los procesos y actividades que desarrollan dentro del CSIRT, Establecerán coordinaciones con los especialistas y Analistas del área ciberseguridad, escalando los casos de alto impacto, como de los apoyos que estos requieran de los servicios de Infraestructura. Son los directos responsables del soporte y atención de los incidentes de seguridad internos de la operación, las 24 horas al día, los 365 días al año, de la empresa Cibersecurity de Colombia LTDA.

10.2.12.1 Perfil. Deben ser personas con liderazgo, es muy importante que cuenten con los conocimientos técnicos requeridos para este cargo, deben poseer un perfil, competitivo, con una experiencia certificable en seguridad de la información e Infraestructura de manera completa, deben ser personas destacadas en el medio, que cumplan con las necesidades del cargo.

10.2.12.2 Formación académica. Los requisitos académicos de este cargo deben ser de grandes capacidades técnicas ya que se requieren para el apoyo de la operación, tal como se indica a continuación:

A. Requerido:
Profesional en el en cualquier área de sistemas de la información.
Certificaciones en Seguridad (ISO 27001, ITIL, CCNA).

B. Se valorará:
Especialización en seguridad de la información o seguridad informática.

10.2.12.3 Experiencia. Dentro de la experiencia para este cargo se deben haber desempeñado como Analistas de alguna compañía o área importante en relación con la misma y con el cargo requerido, entre otros requisitos que se indicaran a continuación:

A. Requerido:
Ultimo cargo desempeñado Analista.
Soporte técnico en temas de seguridad e Infraestructura, por más de 4 años.
Experiencia en áreas técnicas en TI o Seguridad de la información.

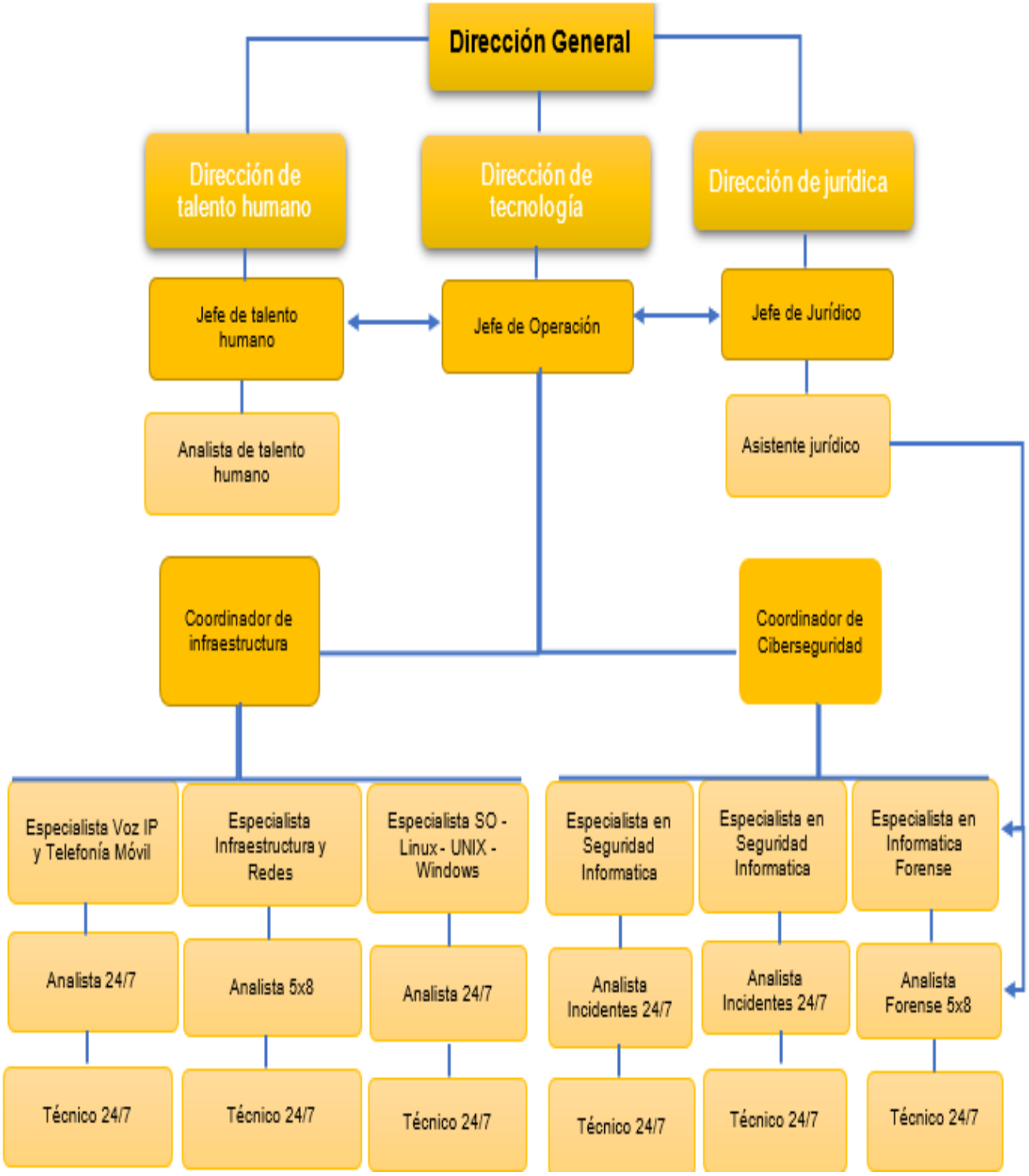
B. Se valorará:
Experiencia en posiciones similares.

10.3 ORGANIGRAMA DE CIBERSECURITY DE COLOMBIA LTDA.

Se establecerá un organigrama y descripción de cómo se encuentra estructurado el CSIRT internamente, así como la forma en que este opera, según las especificaciones ya realizadas y las funciones de las diferentes áreas establecidas en este, así como las cooperaciones entre sí, los horarios por los empleados y demás. Dentro de la organización se tienen varias direcciones o áreas desglosadas después de la dirección general, el área de jurídica, el área de recursos humanos, el área financiera y por su puesto el área de tecnología, cada una de ellas maneja una dirección y se desprende de manera jerárquica, hasta llegar a los analistas o técnicos, la dirección de tecnología está dividida en dos escenarios, infraestructura y ciberseguridad, las cuales se complementan para el soporte al cliente interno y también serán importantes para los clientes externos, adicional al complemento de estas dos áreas de la dirección de tecnología, también se podría indicar que la dirección de jurídica, hace parte fundamental, así como el apoyo necesario al área de tecnología, este apoyo es muy importante en caso de que se requiera en la atención de incidentes de seguridad con implicaciones legales, las demás áreas serian complementos en los casos de contratación de talento humano y la dirección

financiera en cobros, presupuestos y estadísticas de los servicios prestados por el CSIRT. Se observará lo anteriormente indicado en la Figura 24.

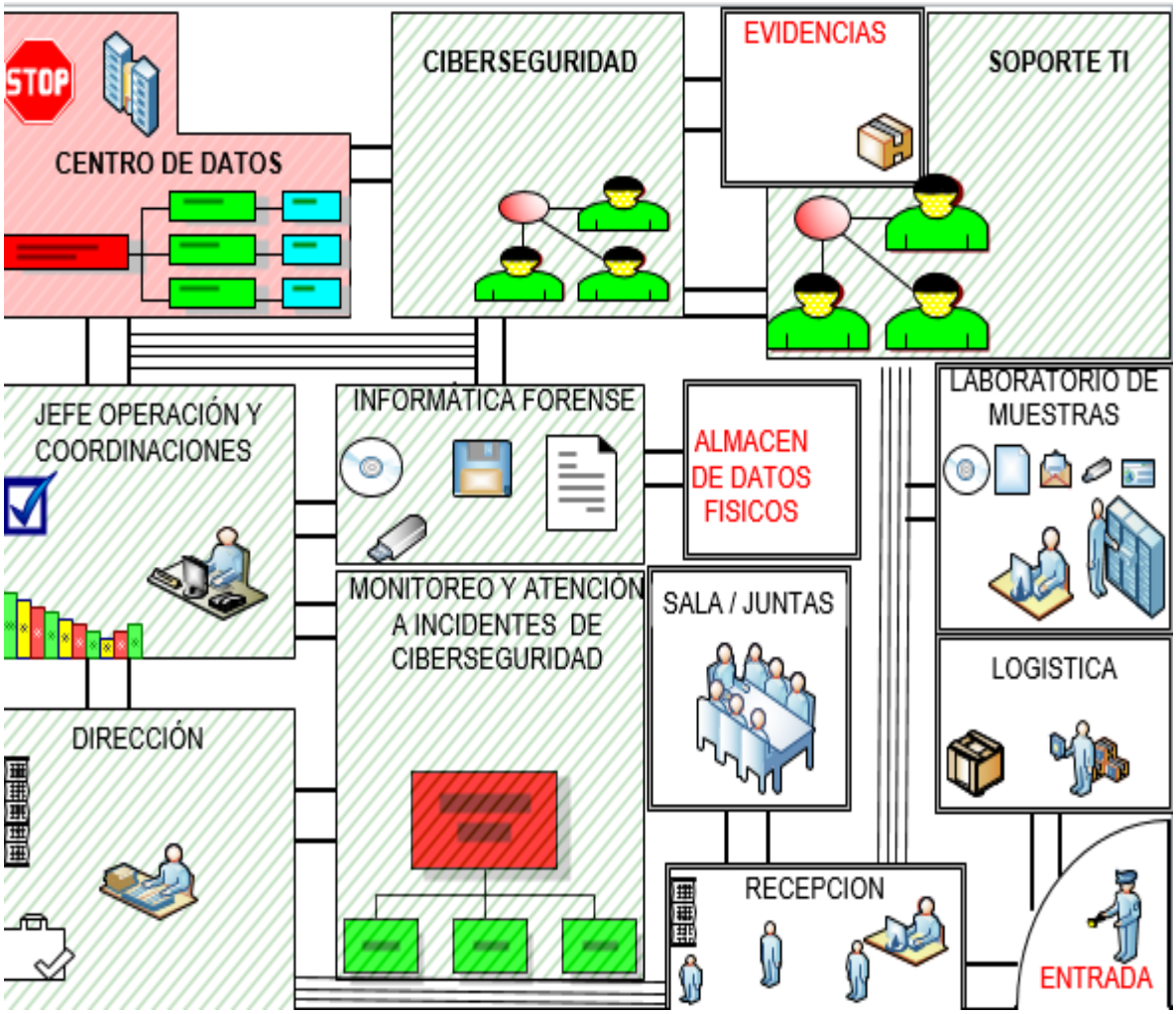
Figura 24. Organigrama Interno de Cibersecurity de Colombia LTDA.



Fuente: Elaboración propia.

10.3.1 Estructura interna CSIRT Cibersecurity de Colombia LTDA. Dentro de la estructura que se utilizará para este Csirt, se adecuaron espacios como, cuarto de evidencias, laboratorio de muestras, evidencias, informática forense, Monitoreo y atención de incidentes de ciberseguridad, entre otros que se pueden observar en la Figura 25.

Figura 25. Estructura CSIRT Empresa Cibersecurity de Colombia LTDA



Fuente: Elaboración propia.

11 CONCLUSIONES

El presente proyecto, es de suma importancia no solo para la empresa Cibersecurity de Colombia LTDA., a la cual fue dirigido, si no para cualquier organización que desee poner en marcha un CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas), dado que la seguridad de la información o seguridad informática, puede considerarse como una de las temáticas más complejas, especialmente por las malas conductas implementadas por los usuarios dentro de una compañía, por lo cual es importante capacitar con estudios que les permitan saber más del tema y algunos más en específico, los lineamientos de seguridad, se consolidan como herramientas muy útiles, para la determinación de los riesgos a los que puedan estar expuestos los sistemas y en segundo lugar para culturizar a las personas, en especial los usuarios de internet, los cuales deben prestar atención a la rigurosa exposición a la que están día a día con los delincuentes informáticos, también conocidos como piratas informáticos.

El objetivo uno, que está representado en el capítulo 7, del presente proyecto, representa un enfoque importante al documento, puesto que permite identificar, partes esenciales como el plan comercial, el cual es de suma importancia, pues todo equipo de respuesta a incidentes de seguridad informática, debe elaborar su plan de servicios, permitiendo que se dé forma a su plan estratégico, puesto que este le permitirá ser reconocido no solo a nivel nacional sino internacional, siendo que mediante sus estrategias de mercado y servicio, podrá conocer varios equipos que le servirán de instrumento en su proyección. Dentro de este mismo capito se evidencian aspectos de suma importancia como las necesidades que debe satisfacer el CSIRT, así como las políticas y procesos que se deben implementar al interior del equipo, puesto que esto les garantizara que se cumplan con los objetivos propuestos y trazados por la empresa.

El objetivo dos, está representado por el capítulo 8, del presente proyecto, este se concluye sobre los diferentes modelos que actualmente se pueden implementar en cualquier equipo de respuesta a incidentes de seguridad de la información, siempre y cuando se tenga establecido los servicios y la población a la cual van dirigidos estos servicios, el presente proyecto se enfocó en el modelo (Distribuido) si bien este le permite ser implementado dentro de la misma empresa a la cual se enfocaran sus servicios, por lo que esta le suministrara el payo tecnológico y recursos humanos para su funcionamiento y puesta en marcha, lo que garantizara que este proyecto tenga viabilidad y proyección.

El objetivo tres, está representado por el capítulo 9 del presente proyecto, es un capítulo muy importante durante el presente proyecto, pues en él se evidencia toda la información referente a la atención de los incidentes de seguridad de la información, permite evidenciar el modelo de atención desarrollado, el cual expresa al lector información visual muy valiosa, desde el inicio de reporte del incidente, pasando por el registro en el sistema que se elige para dicho fin, así como la evaluación del reporte, permitiendo determinar si es necesario realzar ciertas actividades, como también decidir si este debe ser reportado a las autoridades máximas en su entorno, las cuales determinen el conocimiento de dicha ocurrencia, colaborando en la solución de esta, siendo así que se puede determinar en qué momento se finaliza el mismo, para poder finiquitar su peligrosidad en los sistemas, dejando consigo unas lecciones y experiencias que les permitirán poder colocar en práctica en futuros incidentes de las mismas características, mediante la base de conocimiento que se debe implementar.

El objetivo cuatro, está representado por el capítulo 10 del presente proyecto, a simple vista se podría concluir que es uno de los capítulos más interesantes y fáciles de entender, pues en él, se puede evidenciar todo lo relacionado con lo que se ve desde la distancia a cualquier compañía o incluso algo que tenga forma, ya que, se observa el exterior de esta, como la estructura que se dio, al equipo, donde se indica cada uno de sus perfiles y funciones, datos de suma importancia para el equipo como tal, puesto que su misión y visión, los conducen a que se cumplan varios requisitos, entre los cuales se destaca la contratación idónea de perfiles que le garanticen estabilidad al CSIRT cumplimiento de funciones establecidas por cada uno de ellos, dentro de los servicios ofertados y adquiridos por los clientes, la información suministrada permite manifestar que se debe realizar un proceso pues todos los integrantes que se contratan deben cumplir con una suma de características, en cuanto a conocimientos y estudios, que los hace muy interesantes para el equipo, puesto que reúnen una serie de capacidades y experiencias que los caracteriza por ser personas que se han preparado y capacitado para lograr pertenecer a un equipo como el CSIRT de empresa Cibersecurity de Colombia LTDA.

12 RECOMENDACIONES

Prestar un servicio de calidad con el fin de que dichos servicios se den a conocer, así como la atención por parte del personal especializado debe ser muy respetuosa y profesional, garantizando el reconocimiento por parte de los sectores atendidos dentro y fuera de la empresa Cibersecurity de Colombia LTDA.

Promover los servicios del CSIRT, con el fin de que estos tengan una importante acogida y solicitud de adquisición por los clientes potenciales a los cuales están enfocados, garantizando el crecimiento esperado por la compañía, así como la proyección de su visión.

Garantizar la correcta capacitación a los sectores de usuarios que se pretende atender, lo que permitirá que se garantice que los mismos se encuentren satisfechos con los servicios prestados, de esta manera se podrá tener mejores resultados y calidad de los servicios, así como la calificación que se recibirá por parte de ellos.

Informar a las diferentes autoridades de la puesta en marcha de los presentes servicios, con el fin de que se tenga conocimiento y aceptación por parte de la comunidad, los cuales pueden ser aliados muy importantes en la cooperación nacional e internacional, puesto que siempre se puede estar expuesto a ataques que traspasan las fronteras.

13 ANEXOS

13.1 ANEXO 1:

13.1.1 Reporte incidentes de seguridad de la información.

BIBLIOGRAFÍA

A Wilson y PRIETO h. Mindefensa colCER. Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT. La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio" [En Línea] Colombia 2019. [Consulta: 12 de octubre de 2019] P. 18-24 Disponible en: https://web.certicamara.com/files/eventos/CiberseguridadCiberdefensaColombia.pdf

ACOSTA UBAQUE Nubia Esperanza y LEÓN PATIÑO Tania Kruskaya. diseño del sistema de gestión de seguridad de la información (s.g.s.i.) para el centro de datos de la personería de Bogotá d.c. bajo las normas ntc-iso-iec 27001:2013 y ntc-iso-iec 27002:2013. UNAD. [En línea] Escuela de Ciencias Básicas, Tecnología e Ingeniería 2017. [Consulta: 12 abril de 2020] P. 21-219 Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11940/35508879.pdf?sequence=1&isAllowed=y

ADR Formación. Día de Internet 2020: la importancia de la tecnología durante la crisis sanitaria. Mayo de 2020. Blog. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.adrformacion.com/blog/dia_de_internet_2020_la_importancia_de_la_tecnologia_durante_la_crisis_sanitaria.html

AGENCIA EFE. Los ciberataques crecen en Chile 59% en 2018 cerca de la media de América Latina. Santiago de Chile. 5 ene 2019. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.efe.com/efe/america/economia/los-ciberataques-crecen-en-chile-59-2018-cerca-de-la-media-america-latina/20000011-3858841

AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. (Grecia). ENISA. cómo crear un CSIRT paso a paso. Producto WP2006/5.1(CERT-D1/D2) [Consulta: 12 abril 2020]. P. 12-90 Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

ARCHIVO GENERAL DE LA NACIÓN (Colombia). Repositorio Normativo. Acuerdo No. 006. 15 oct 2014. "Por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI "Conservación de Documentos" de la Ley 594 de 2000" [En Línea] [Consulta: 12 septiembre de 2020] Disponible en: https://normativa.archivogeneral.gov.co/acuerdo-006-de-2014/

ASOBANCARIA (Colombia). Riesgo cibernético y el futuro de la estabilidad financiera. Semana económica 2019. Edición 1178. 26 de marzo de 2019. [Citado el 12 abril de 2020] p. 8-12 Disponible en: https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1178.pdf

ASOBANCARIA. Csirt Financiero un Enfoque Colaborativo a la Ciberseguridad. [Sitio Web Colombia: [Consulta: 12 octubre de 2019] Disponible en: https://www.asobancaria.com/csirt/

BARZANALLANA Rafael. Gestión de la Seguridad en Sistemas de Información. Introducción a la Seguridad Informática. [En Línea]. España. UMU. [Consulta: 12 abril 2020] P.18-65 Disponible en: https://www.um.es/docencia/barzana/GESESI/GESESI-Introduccion-a-la-seguridad.pdf

BÉLGICA UNIÓN EUROPEA. directiva (UE) 2016/1148 del parlamento europeo y del consejo. Diario Oficial de la Unión Europea. [En Línea] de 6 de julio de 2016. [Consulta: 12 de octubre de 2019] P. 1-30. Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf

BÉLGICA. UNIÓN EUROPEA. Reglamento europeo sobre la Ciberseguridad 2019/881. Diario Oficial de la Unión Europea. [En Línea] 27 de junio de 2019. [Citado el 12 de octubre de 2019] P. 1-55. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN

BNAMERICAS ¿Por qué Brasil es tan vulnerable a los ciberataques? 06 enero, 2020 [Sitio Web] Brasil. [Consulta: 12 septiembre de 2020] Disponible en: https://www.bnamericas.com/es/reportajes/por-que-brasil-es-tan-vulnerable-a-los-ciberataques

B-SECURE (Colombia). Pasión por la seguridad. [En Línea] [Consulta: 12 abril de 2020] Disponible en: https://www.b-secure.co/

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES, POLICÍA NACIONAL DE COLOMBIA Y IMPACTOTIC, [En línea] Tendencias de Cibercrimen en Colombia 2019-2020, octubre 2019. [Consulta: 12 diciembre 2019] P. 7-36 Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. (Colombia). [Sitio Web] [Consulta: 12 abril 2020] Disponible en: http://www.csirt-ccit.org.co/

CAROZO Eduardo. *Et al*. Análisis del Desarrollo de un Centro de Respuesta Nacional para la República Oriental del Uruguay. [En Línea] Universidad de Montevideo [Consulta: 12 de octubre 2019] P. 1-23. Disponible en: http://www.um.edu.uy/_upload/_descarga/web_descarga_25_Memoria_6_CentrodeRespuesta.pdf

CAROZO Eduardo: MARTÍNEZ Carlos y VIDAL Leonardo. CERTuy: Hacia un CSIRT Nacional. CSIRT – ANTEL. Grupo de Seguridad Informática, Facultad de Ingeniería, Universidad de la República de Uruguay. [En línea] [Consulta: 12 octubre 2019] P. 18. Disponible en: https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

CAVANNA Santiago. Política de Clasificación de la información. [Sitio Web] (2019) Argentina. [Consulta: 27 de abril de 2020] Disponible en: http://www.adecuarse.com/

CEDIA CSIRT. (Ecuador). Equipo de respuesta a incidentes de seguridad. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://csirt.cedia.edu.ec/

CEDIA CSIRT. Paquete de servicio universidades. Ecuador 2019. [En Línea] [Consulta: 12 septiembre de 2020] Disponible en:

https://www.cedia.edu.ec/dmdocuments/PAQUETES%20DE%20SERVICIOS/universidades_servicios2019.pdf
CELSIA. Políticas con sus respectivos estándares. [En Línea] [Consulta: 12 marzo de 2020] P. 17-24. Disponible en: https://www.celsia.com/Portals/0/contenidos-celsia/nuestra-empresa/politicas-y-adhesiones/politicas/politica-seguridad-de-la-informacion.pdf
CENTRO CRIPTOLÓGICO NACIONAL. (España). Principios y recomendaciones básicas en Ciberseguridad [En línea] (CCN-CERT BP/01) octubre 2017, [Consultado: 12 diciembre de 2019] P. 6-28 Disponible en: https://www.ucm.es/data/cont/media/www/pag-114974/CCN-CERT_BP_01.pdf
CERT.BR. Equipo Nacional de Respuesta a Emergencias Informáticas de Brasil. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en: httxps://www.cert.br/
CERTUY (Uruguay). Centro Nacional de Respuesta a Incidentes de Seguridad Informática. [Sitio Web] [consulta: 12 de abril 2020] Disponible en Internet: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/
CIBERSEGURIDAD INDUSTRIAL BY LOGITEK. ¿Qué es un firewall industrial DPI (Deep Packet Inspection)? [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.ciberseguridadlogitek.com/que-es-un-firewall-industrial-dpi-deep-packet-inspection/
Ciberseguridad. Noticias relevantes sobre este sector en auge. Software de seguridad informática. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://ciberseguridad.com/herramientas/software/
CLARO Colombia. Centro de Operaciones de Seguridad Equipo Claro. SOC. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: http://www.claro.com.co
CLCERT (Chile) Universidad de Chile. Laboratorio de criptografía aplicada y ciberseguridad. [Sitio Web] Chile [Consulta: 12 septiembre de 2020] Disponible en: https://www.clcert.cl/
COELHO Fabián Significado de Planteamiento del problema, Ciencia y Salud, Universidad de los Andes, Bogotá D.C. [Sitio Web] Blog Significados.com [Consulta: 12 abril 2020] Disponible en: https://www.significados.com/planteamiento-del-problema/
colCERT. (Colombia). Grupo de Respuesta a Emergencias Cibernéticas. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en Internet: http://www.colcert.gov.co/
COLOMBIA, CONGRESO DE LA REPUBLICA, LEY 527 de 1999. comercio electrónico y de las firmas digitales. (21 de agosto de 1999) Diario Oficial No. 43.673. [En Línea] [Consulta: 12 de octubre de 2019] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html
COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. [En Linea] Guia No 21. V 1-2. Bogotá: 2016. [Citado en 12 octubre del 2019] P. 8-29. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. [En Línea] GIT-G-01 guía para la calificación de la información. Bogotá D.C. 2015. [Consulta: 27 de abril del 2020]. P.7-22. Disponible en:

https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/3.3%20Procesos%20y%20Procedimientos/GIT-G-01_GUIA_PARA_LA_CALIFICACI%C3%93N_DE_LA_INFORMACI%C3%93N_AGN.pdf

COLOMBIA. COMANDO GENERAL DE LAS FUERZAS MILITARES - COMANDO CONJUNTO CIBERNÉTICO. [En línea] Defensa de la Infraestructura Crítica Cibernética [Citado en 12 abril de 2020] Disponible en https://www.ccoc.mil.co/

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. Bogotá D.C. (enero 5 de 2009) Diario Oficial. [En Línea] [Consultado: 12 de marzo de 2020] P. 1-4. Disponible en. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. boletín trimestral de las TIC, cifra tercer trimestre del 2019. [Sitio Web] Bogotá D.C. Colombia enero 2020. [Consulta 12 octubre de 2020] P.9-50 Disponible en: https://colombiatic.mintic.gov.co/679/w3-article-125648.html

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES [En Línea] Elaboración de la política general de seguridad y privacidad de la información. Guía No 1. (11 de mayo del 2016) V 001. [Citado el 12 de marzo de 2020] P. 24-25. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

COMANDO CONJUNTO CIBERNÉTICO (Colombia) Centro de operaciones de seguridad - Comando de operaciones cibernéticas conjuntas. SOC-CCOC. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: https://www.ccoc.mil.co/

Csirt gob cl, (Chile) Equipo de Respuesta ante Emergencias Informáticas. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://www.csirt.gob.cl/matriz-clasificacion-incidentes/

CSIRT. (Argentina). Centro Nacional de Respuesta a Incidentes de Seguridad Informática. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en Internet: https://www.ba-csirt.gob.ar/

CSIRT. (Chile). El Equipo de Respuesta ante Incidentes de Seguridad Informática. [Sitio Web] [Consulta: 12 de abril 2020] Disponible en Internet: https://www.csirt.gob.cl/

CYBERSHIELD. (Colombia). Asegurando el mundo un Byte a la vez. [Sitio Web] [Consulta: 12 abril 2020] Disponible en: https://www.cybershield-us.com/

DEPARTAMENTO NACIONAL DE PLANEACIÓN, Documento CONPES 3854, departamento nacional de planeación, [En Línea] política nacional de seguridad digital Colombia: 2016. [Consulta: 12 de octubre de 2019] P. 91. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

DIGIWARE. Equipo de respuesta a incidentes de seguridad informática de DigiSOC. [Sitio Web] Colombia. [Consulta: 12 abril de 2020] Disponible en: http://www.digiware.net

ECUCER. (Ecuador). Centro de Respuesta a Incidentes Informáticos. [Sitio Web] [Consulta: 12 abril 2020] Disponible en: https://www.ecucert.gob.ec/

EINAR LANFRANCO Lic y PÉREZ ESTÉVEZ Ernesto ¿De qué se trata?, modelos posibles, servicios y herramientas. [En línea] Colombia: [Consulta: 12 de octubre de 2019] P. 18. Disponible en: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf
EMBAJADA DE ESTADOS UNIDOS EN COLOMBIA. Expertos de EE. UU. [Sitio Web] fortalecen capacidades de funcionarios en ciberseguridad y diseño de servicios digitales. 2019. [Consulta: 27 de abril de 2020] Disponible en: https://co.usembassy.gov/es/expertos-de-ee-uu-fortalecen-capacidades-de-funcionarios-en-ciberseguridad-y-diseno-de-servicios-digitales/
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ SA ESP – ETB. Equipo de Respuesta a Incidentes de Seguridad Informática. [Sitio Web] Csirt-Etb. [Consulta: 12 abril de 2020] Disponible en: https://etb.com/inicio.aspx
Esaú A. Top 10 Aplicaciones de Seguridad. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://openwebinars.net/blog/top-10-aplicaciones-de-seguridad/
ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO. [En Línea] manual de políticas de seguridad y privacidad de la información Bogotá, D.C. 2018 [Consulta: 12 de marzo de 2020]. P. 71-79. Disponible en: https://www.escuelaing.edu.co/escuela/importantDoc/Manual-politica-seguridad-dela-Informacion.pdf
ESTADOS UNIDOS. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. BANCO INTERAMERICANO DE DESARROLLO y COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Impacto de los incidentes de seguridad digital en Colombia 2017. [En línea] Colombia, 2017. [Consultado: 12 diciembre 2019] P. 48-130 Disponible en: https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf
ETEK INTERNATIONAL. (Colombia) Equipo de respuesta a incidentes de seguridad informática de ETEK International. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: www.etek.com.co
FIRST. Foro global de respuesta a incidentes y equipos de seguridad. [Sitio Web] Estados Unidos de América: [Consulta: 12 octubre de 2019] Disponible en: https://www.first.org/members/teams/
FIRST. Foro global de respuesta a incidentes y equipos de seguridad. [Sitio Web] Estados Unidos de América: [Consulta: 12 octubre de 2019] Disponible en: https://www.first.org/members/map#country%3ACO
FIRST. Foro global de respuesta a incidentes y equipos de seguridad. Primera Historia. [Sitio Web] Estados Unidos de América: [Consulta: 12 octubre de 2019] Disponible en: https://www.first.org/about/history
Fuente. Consejo Nacional de Ciberseguridad. [Ren Línea] Guía nacional de notificación y gestión de ciberincidentes.: España. [Citado el 12 de octubre de 2019] P. 29-55 Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

GALEANO Susana. El número de usuarios de Internet en el mundo crece un 7% y alcanza los 4.540 millones (2020) m4rketing Ecommerce. digital. [Sitio Web] enero de 2020: [Consulta: 12 abril 2020] Disponible en: https://marketing4ecommerce.net/usuarios-internet-mundo/

GOB.EC. Portal único de tramites ciudadanos. Asesoría para la formación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) [Sitio Web] Ecuador. [Consulta: 12 de abril de 2020] Disponible en: https://www.gob.ec/arcotel/tramites/asesoria-formacion-equipos-respuesta-incidentes-seguridad-informatica-csirt

GUZMAN FLOREZ, Camilo y ANGARITA PINZON, Cristian. protocolos para la mitigación de ciberataques en el hogar. [En Línea] Bogotá: 2017. [Citado el 12 de octubre de 2019] P79 Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15321/1/Cibersecurity%20Home.pdf.

HARÁN Juan Manuel. WeLive Security. Malware de los años 80: recordando al virus informático Brain y al gusano Morris. Noviembre 2018. [En Línea] [Consultado: 12 mayo 2020] Disponible en: https://www.welivesecurity.com/la-es/2018/11/05/malware-anos-80-recordando-virus-informatico-brain-gusano-morris/

HERNÁNDEZ José Carlos. Universidad de Granada. Estrategias nacionales de ciberseguridad en américa latina [En Línea] (España). ISSN: 2340-8421. 2018. [Consulta: 25 de abril de 2020] Disponible en: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina
https://netcloudengineering.com/servidor-cloud-vs-local-empresas/

ICONTEC. Norma técnica ntc-iso/iec colombiana 27001. Bogotá D:C I.C.S.: 35.040.00. [En Línea] 2013 [Citado en 12 de marzo del 2020]. Disponible en Internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

INCIBE INSTITUCIÓN NACIONAL DE CIBERSEGURIDAD (España) Copias de seguridad, [En Línea]. una guía de aproximación para el empresario. PTE_AproxEmpresario_011_ Copias Seguridad 2018. v1 [Citado en 12 marzo de 2020] P. 3-32 Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

INCIBE INSTITUTO NACIONAL DE CIBERSEGURIDAD (España) [Sitio Web]. [Consulta: 12 abril de 2020] Disponible en: https://www.incibe.es/

INCIBE INSTITUTO NACIONAL DE CIBERSEGURIDAD. (España) Analizadores de red en sistemas de control. 10 de febrero de 2017 [Sitio Web]. [Consulta: 12 abril 2020] Disponible en: https://www.incibe-cert.es/blog/analizadores-red-sistemas-control

INFORMATICA MODERNA. Router Poe. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: http://www.informaticamoderna.com/Router.htm

INFOTECS. IPS: Sistema de Prevención de Intrusos. Actualización: 13 de marzo de 2019. [En Línea] Blog. [Consulta: 12 marzo 2020] Disponible en: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html
INTERNET SECURITY AUDITORS. Informática Forense y Peritajes. [Sitio Web]. 2020. Bogotá D.C. [Consulta: 12 abril de 2020] Disponible en: https://www.isecauditors.com/informatica-forense-peritajes
ISOTOOLS. ISO 27001 Cómo se debe realizar la clasificación de la información. (14 septiembre, 2017) [Sitio Web] Blog especializado en Sistemas de Gestión de Seguridad de la Información. [Consulta: 27 de abril de 2020] Disponible en: https://www.pmg-ssi.com/2017/09/iso-27001-clasificacion-de-la-informacion-2/
ITSSOC-CSIRT servicios de seguridad de ti Sas Soc Csirt, Equipo de Servicios de seguridad de TI SAS ITSSOC-CSIRT. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: https://www.itsecurityservices.com.co/
IZQUIERDO Robin. Pandorafms. Historia de los virus informáticos: Creeper y Reaper. Monitoring Blog. [Sitio Web] Colombia. octubre 10, del 2018 [Consulta: 12 octubre de 2019] Disponible en: https://pandorafms.com/blog/es/reeper-y-reaper/
LACORT Javier. WannaCry, el ransomware del ataque a Telefónica. España. 2017. [Citado en 12 mayo de 2020] Disponible en: https://hipertextual.com/2017/05/wannacry-ransomware-ataque-telefonica
LUISA Cruz Lobato. URVIO - Revista Latinoamericana de Estudios de Seguridad N.° 20, junio de 2017, pp. 16-30. La política brasileña de ciberseguridad como estrategia de liderazgo regional. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://revistas.flacsoandes.edu.ec/urvio/article/view/2576/2104
MALWAREBYTES. Hacker. Todo sobre el hackeo [En Línea]. Santa Clara, California Estados Unidos. [Consulta: 12 marzo 2020] Disponible en https://es.malwarebytes.com/hacker/
MODELO DE COORDINACIÓN y Atención de Emergencias en el ámbito de la Sociedad de la Información. [Anónimo] [En Línea] [Consultado: 12 de abril de 2020] P. 83-117 Disponible en: http://catai.net/blog/wp-content/uploads/2009/01/premioacademiacanariaseguridad.pdf
MUÑOZ Mirna, RIVAS Lizbeth. Revista ibérica de sistemas y tecnologías de información. DOI: 10.17013/risti. e 3.1-15. [En línea] [Consulta: 12 abril de 2020] P. 10-15 Disponible en: http://www.scielo.mec.pt/pdf/rist/nspe3/nspe3a02.pdf
MURQUINCHO PUMA Diego Eduardo, Propuesta para la creación de un comité de respuestas ante incidentes de seguridad informática (CSIRT), en el ámbito de la educación superior. Caso de estudio Universidad Nacional de Loja Ecuador. 10 diciembre 2018 [En línea] Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables [Consulta: 12 febrero de 2019] P. 4-25. Disponible en: https://www.studocu.com/ec/document/universidad-nacional-de-loja/seguridad-de-la-informacion/resumenes/articulo-revision-sistematica-csirt/4027803/view
NET CLOUD ENGINEERING. Servidor Cloud vs servidor local para empresas. [Sitio Web] [Consulta: 12 septiembre de 2020] Disponible en: https://openwebinars.net/blog/top-10-aplicaciones-de-seguridad/
NIC.br. (Brasil). Centro de Información y Coordinación [Sitio web] Brasil [Consulta: 12 de octubre de 2019] Disponible en: https://www.nic.br/

OEA. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (Estados Unidos) Buenas prácticas para establecer un Csirt Nacional. [En línea] abril de 2016. [Consulta: 23 abril 2020] P. 15-55 Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
OLIMPIA. (Colombia). Plataformas para la transformación digital. [Sitio Web] [Consulta: 12 abril 2020] Disponible en: https://www.olimpiait.com/
ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Reporte seguridad 2020 riesgos avances y el camino a seguir en América latina y el Caribe. Reporte ciberseguridad 2020. [En Línea] [Consulta: 10 abril de 2020] P.81-204 Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y BANCO INTERAMERICANO DE DESARROLLO. (Estados Unidos). Ciberseguridad, ¿estamos preparados en América latina y el caribe? [En línea] Informe ciberseguridad 2016. [Citado el 1 de 2octubre de 2019] P. 11-193. Disponible en: https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf
ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN. ISO / IEC 27000: 2018. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario. Ginebra, Suiza. Edición 5. [Sitio Web] febrero 2018 [Consulta: 12 de marzo 2020]. P. 27. Disponible en: https://www.iso.org/standard/73906.html
ORGANIZACIÓN MUNDIAL DE LA SALUD (Ginebra). [En Línea] Política de divulgación de información 2017. [Consulta: 12 de octubre de 2019] P. 4-12. Disponible en: http://www9.who.int/suggestions/InfoDisclosurePolicy_es.pdf
PECERT. (Perú) Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional. [Sitio Web] [Consulta: 12 de abril de 2020] Disponible en Internet: https://www.pecert.gob.pe/
PÉREZ AGUILERA Carlos J. política de retención de datos. [En Línea] Ofiteco Uninc. (08 de mayo del 2018) [Consulta: 12 de octubre de 2019] P. 4-7. 8. Disponible en: https://uning.es/wp-content/uploads/2018/06/Politica-de-retencion-de-datos.pdf
POLICÍA NACIONAL - FISCALÍA GENERAL DE LA NACIÓN, Sistema Nacional de Denuncia Virtual ... ¡ADenunciar. [En línea], Colombia: [Citado el 12 de octubre de 2019] Disponible en: https://adenunciar.policia.gov.co/adenunciar/Login.aspx?ReturnUrl=/adenunciar/%20
POLICÍA NACIONAL DE COLOMBIA. cc-csirt. [Sitio Web] servicios-proactivos. [Consulta: 12 abril de 2020] Disponible en: https://cc-csirt.policia.gov.co/servicios/servicios-proactivos
POLICÍA NACIONAL DE COLOMBIA. Centro Cibernético Policial. Informe Amenazas del Cibercrimen. [En Línea] En Colombia 2016 – 2017. [Citado en 12

abril de 2020] Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.
POLICÍA NACIONAL DE COLOMBIA. Csirt Ponal Equipo de Respuesta de Seguridad Informática Incidentes de la Policía Nacional de Colombia. [Sitio Web] Centro cibernético policial. [Consulta: 12 abril de 2020] Disponible en: https://cc-csirt.policia.gov.co/
POLÍTICA COMUNICADA. 'BA-Csirt' el primer centro de ciberseguridad en América Latina. [En línea] [Consulta: 12 octubre 2019] Disponible en: https://politicacomunicada.com/ba-csirt-el-primer-centro-de-ciberseguridad-en-america-latina/
PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto Número 1081. [En Línea] (mayo 26 de 2015) Bogotá. D.C. [Consulta: 12 de octubre de 2019] Disponible en: http://es.presidencia.gov.co/normativa/normativa/Decreto-1081-2015.pdf
PRIETO h y A Wilson. Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, Gestión y Respuesta a Incidentes de Ciberseguridad, [En línea] Colombia 2017, [Citado en 12 octubre de 2019]. P.24-32 Disponible en: https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf
RASSELI JUNIOR Luiz Alberto. Casos y Voces – Red clara. Conozca CSIRT.REUNA, el centro de respuesta ante incidentes de seguridad exclusivo para instituciones de I+E. [Sitio Web] (enero 2020). [Consulta: 12 abril de 2020] Disponible en: https://www.redclara.net/index.php/es/noticiasyeventos/casos-y-voces/2018-nace-csirt-reuna-el-centro-de-respuesta-ante-incidentes-de-seguridad-exclusivo-para-instituciones-de-i-e
SABBAGH Ana Paulina. Secretaría de Transparencia. Presidencia de la Republica de Colombia. [En Línea] transparencia y acceso a la información. Bogotá D.C. [Consulta: 02 de mayo de 2020] P. 12-20. Disponible en: https://secretariageneral.gov.co/sites/default/files/jornada_transparencia_-_ley_de_acceso_a_la_informacion_publica.pdf
SEGURIDAD INFORMÁTICA [Anónimo]. Capítulo 1, [En línea] seguridad informática conceptos básicos. [Consulta: 12 abril de 2020]. P. 3-4.19 Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf
SHIELDNOW. Equipo de respuesta a incidentes de seguridad. Colombia. [Sitio Web] [Consulta: 12 abril de 2020] Disponible en: https://shieldnow.co/
SUPER INTENDENCIA DE SOCIEDADES. (Colombia) Guía Para la Gestión de Incidentes. [En línea] 2017 Colombia: [Consulta: 12-octubre-2019] P.11-18 Disponible en: https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Infraestructura%20Tecnologica/Documentos/GINT-G-006%20Gu%EDa%20Gestion%20de%20Incidentes.pdf
UNIVERSIDAD DE JAÉN. Biblioteca. Alfingrado.03.1 bucear en internet. El 26 de abril del 2019. [en línea]. P. 3 [Citado en 12 abril de 2020] Disponible en:

https://www.slideshare.net/bibliotecauniversidadjaen/alfingrado031-bucear-en-internet-142308459
UNIVERSIDAD EAFIT. política de tratamiento de protección de datos personales de los titulares. [En Línea] [Consulta: 12 de octubre de 2019] p. 4-7. 14. Disponible en: http://www.eafit.edu.co/institucional/reglamentos/tratamiento-proteccion-datos-personales/Documents/Politica-Universidad-EAFIT-de-tratamiento-de-protecci%C3%B3n-de-datos-personales.pdf
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD (Colombia) Gerencia de Proyectos Informáticos – 204030, definición del problema [En Línea] [Consulta: 12 febrero 2020] P. 1 Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/5586/DefProblema.pdf?sequence=1
URIBE RAYAS Edgar Felipe. Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática. Centro de Investigación de Matemáticas A:C: Obtener grado en Maestro en Ingeniería de Software. México. (CSIRT) [Consulta: 12 abril 2020]. P. 21-211 Disponible en: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/437/1/ZACTE42.pdf
VALLEJOS Oscar. Introducción a Internet. Facultad de Ingeniería. [En línea] [Consulta: 12 abril 2020]. P. 2-23 Disponible en: http://ing.unne.edu.ar/pub/internet.pdf
Yi Min Shum. Situación digital, Internet y redes sociales Colombia 2020. [En Línea] [Citado en 12 septiembre de 2020] Disponible en: https://yiminshum.com/social-media-colombia-2020/
YÚBAL Fm. Xataka. La historia de Creeper, el primer virus informático jamás programado. Historia Tecnológica. [Sitio Web] 06 de mayo del 2018. México: [Consulta: 12 octubre 2019] Disponible en: https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primer-virus-informatico-jamas-programado

Fecha de Realización:	11 de marzo del 2021
Programa:	Especializacion en seguridad informática
Línea de Investigación	Infraestructura tecnológica y seguridad en redes
Título:	Estudio Documental, Para La Creación Del Centro De Respuesta A Incidentes Csirt Para Caso De Estudio “Escenario Administrativo” Cibersecurity De Colombia Ltda
Autor(es):	Libardo Barbosa Vargas
Palabras Claves:	Csirt, Seguridad, Ciberataque, Modelo, Vulnerabilidad
Descripción:	El presente proyecto, está basado en la creación de un escenario documental y administrativo, para la implementación de un CSIRT, para la empresa CIBERSECURITY DE COLOMBIA LTDA, la cual prestara sus servicios de atención a incidentes de ciberseguridad, a los clientes internos y externos, dentro del proyecto, se encontrara una oferta comercial de los servicios que este ofertara, se establecieron unos alcances y limitaciones, para determinar desde donde arranca y hasta donde nos permite ir en su implementación, se aplicaran diferentes políticas las cuales ayudaran a que el CSIRT, pueda cumplir con sus propósitos y procesos, se elaboró la respectiva Misión y Visión, en las cuales se da una orientación a los propósitos del mismo, se establecieron 4 objetivos específicos los cuales se describieran desde el capítulo 6 en adelante. Dentro de los diferentes marcos se da a conocer la problemática, una parte de historia de los CSIRT, así como los antecedentes, tanto de los incidentes de seguridad como de los CSIRT ya establecidos, se habla un poco sobre los socios estratégicos y aliados que se deben tener, nacionales como internacionales, se habla sobre la normatividad nacional con referencia a los delitos informáticos, se verificaron los diferentes modelos que se conocen de los CSIRT ya implementados a nivel nacional e internacional, se realiza una pequeña descripción en la relación que se realiza de cada uno de los principales CSIRT de los países vecinos en Latinoamérica, se realiza un proceso de la atención a incidentes de seguridad y su tratamiento, se establecen los perfiles y el modelo que tendrá el CSIRT para su funcionamiento.

Fuentes bibliográficas destacadas:

CENTRO CRIPTOLÓGICO NACIONAL. (España). Gua de creación de un cert / csirt. In Editor y Centro Criptológico Nacional. guía de seguridad [En línea] (ccn-stic-810) septiembre 2011, [Citado nl 12 diciembre de 2019] P. 13-60 Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-

Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf
OEA. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (Estados Unidos) Buenas prácticas para establecer un Csirt Nacional. [En línea] abril de 2016. [Citado en 23 abril de 2020] P. 8-55 Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. (Grecia). Enisa. cómo crear un CSIRT paso a paso [En línea] Producto WP2006/5.1(CERT-D1/D2) [Citado en 12 abril del 2020]. P. 8-90 Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport
URIBE RAYAS Edgar Felipe. Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática. Centro de Investigación de Matemáticas A:C:[En Linea] México. (CSIRT) [Citado en 12 abril del 2020]. P. 17-211 Disponible en: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/437/1/ZACTE42.pdf

Contenido del documento:

Introducción
Definición Del Problema
Planteamiento Del Problema
Formulación Del Problema
Alcance Y Limitaciones
Justificación
Objetivos
Objetivo General
Objetivos Específicos
Marco De Referencia
Marco Teórico
Estándares De Seguridad Informatica
Marco Conceptual
Antecedentes
Marco Legal
Marco Contextual
Diseño Metodológico
Estudio Metodológico
Enfoque Metodológico
Población Y Muestra
Faces De Trabajo
Estructura Organizacional Del Csirt
Desarrollo Del Plan Comercial.
Plan Estratégico
Necesidades
Políticas Del Csirt
Estudiar Y Aplicar El Intercambio De Modelos

	Modelos En Los Países Vecinos. Atencion Y Seguimiento A Incidentes De Seguridad Detección De Incidentes De Seguridad Reporte De Incidentes Evaluación. Gestión De Incidentes Definición De Perfiles Y Organigrama Del Csirt Misión Y Visión Del Csirt Definición De Roles Y Perfiles Organigrama De La Cibersecurity De Colombia Ltda Conclusiones Recomendaciones Bibliografía
Marco Metodológico:	Diseño Metodológico Estudio Metodológico Enfoque Metodológico Población Y Muestra Fuentes De Información.
Conceptos adquiridos:	Conocimientos sobre los diferentes servicios que puede ofertar un CSIRT, las funciones de los CSRT, posicionamiento de Colombia en temas relacionados en seguridad informática en comparación con otros países en el mundo y Latinoamérica, posicionamiento en ciberseguridad de Colombia según FIRST, El ciclo de vida de un incidente de seguridad.
Conclusiones:	El objetivo uno, que está representado en el capítulo 6, del presente proyecto, representa un enfoque importante al documento, puesto que permite identificar, partes esenciales como el plan comercial, el cual es de suma importancia, pues todo equipo de respuesta a incidentes de seguridad Informatica, debe elaborar su plan de servicios, permitiendo que se dé forma a su plan estratégico, puesto que este le permitirá ser reconocido no solo nivel nacional si no internacional, siendo que mediante sus estrategias de mercado y servicio, podrá conocer varios equipos que le podan servir de instrumento en su proyección. Dentro de este mismo capito se evidencian aspectos de suma importancia como las necesidades que debe satisfacer el CSIRT, así como las políticas y procesos que se deben implementar al interior de equipo, posto que esto les garantizara que se cumplan con los objetivos propuestos y trazados por la empresa.