DISEÑO ADMINISTRATIVO DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

JORGE LUIS FLÓREZ BENAVIDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2021

DISEÑO ADMINISTRATIVO DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

JORGE LUIS FLÓREZ BENAVIDES

Proyecto aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre Asesor
EDUARD MANTILLA TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTIAGO DE CALI
2021

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este trabajo de grado a mí señor padre, quien ha acompañado todo mi proceso educativo, apoyándome en los buenos y malos momentos, siempre enseñándome por medio del ejemplo, la ética necesaria para ser un excelente profesional.

AGRADECIMIENTOS

Agradezco a mi querida madre que en paz descase, quien brindó gran parte de su vida para protegerme y enseñarme los valores necesarios para ser una persona de bien y formarme como profesional. Gracias por ser una excelente madre, esposa, hermana y amiga.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

GLOSARIO

BITCOIN: Es un protocolo utilizado como criptomoneda para realizar actividades financieras virtuales.

BOOTNETS: Es un conjunto de redes o robots informáticos que se ejecutan automáticamente, con el propósito de controlar los equipos de una red y aprovechar sus características para realizar actividades sin autorización.

CIBERDELINCUENTES: Personas que ejecutan actividades ilícitas y delictivas en redes de datos y sistemas de información.

CIBERSEGURIDAD: Conjunto de estrategias y técnicas para asegurar las redes, equipos de cómputo, servidores y dispositivos móviles ante ataques cibernéticos.

CLOUD COMPUTING: La computación en la nube abarca un conjunto de tecnologías que permiten ofrecer servicios informáticos a través de la red de internet.

EXPLOIT: Es un fragmento de código o software que contiene comandos que permiten identificar y aprovechar vulnerabilidades en los sistemas de información.

HACKER: Persona con conocimientos en seguridad informática, dedicada a vulnerar la seguridad y acceder a los sistemas de información con o sin autorización.

IOT: El internet de las cosas se refiere a la conexión de objetos cotidianos a la red de internet, objetos como electrodomésticos, edificios, automóviles, entre otros.

MALWARE: Es un programa o software malicioso, que ejecuta acciones perjudiciales y no autorizadas en un sistema de información.

PHISHING: Conjunto de técnicas que buscan engañar a las víctimas suplantando a una persona u organización, por medio de herramientas informáticas, para obtener datos o información personal.

RANSOMWARE: Es un tipo de malware que secuestra la información de un sistema informático, con el propósito de solicitar sumas de dinero a cambio de liberar la información.

RIESGO INFORMÁTICO: Es la posibilidad de que ocurra un evento que limita y genera un impacto negativo en el cumplimiento de un objetivo o realización de una actividad.

SAAS: El Software como Servicio es un modelo de negocio que permite ofrecer de forma remota las funcionalidades de un determinado software, por medio de un equipo cliente conectado a internet.

SPAM: Son un tipo de mensajes publicitarios no deseados, enviados masivamente a grandes cantidades de usuarios, que pueden generar riesgos de seguridad en los equipos receptores.

SPYWARE: Es un tipo de malware que espía sin consentimiento un computador y recopila su información, para luego enviarla a la persona u organización responsable del spyware.

TOKEN: Es un dispositivo utilizado para brindar seguridad en los procedimientos de autenticación y acceso a los sistemas informáticos.

VULNERABILIDADES INFORMATICAS: Son las debilidades de los sistemas de información, que ponen en riesgo su seguridad y son explotadas por los atacantes.

RESUMEN

Según informes de las multinacionales CISCO[1] y FORTINET[2], en Colombia existen importantes brechas de ciberseguridad, que afectan principalmente al sector empresarial y gubernamental, adicionalmente afirman que los índices de ataques informáticos en el país son alarmantes, generando potenciales problemas para la seguridad de las empresas. Una de las causas de los elevados índices de ciberataques, es el constante desarrollo de herramientas y técnicas cada vez más sofisticadas para vulnerar las redes y los sistemas, por lo tanto, las empresas requieren de una constante actualización, especialización e implementación de nuevas estrategias para asegurar sus activos de información.

Este proyecto aplicado se desarrolla sobre el escenario hipotético, de una empresa que presta servicios de seguridad de la Información llamada "Cibersecurity de Colombia LTDA", que tiene como objetivo consolidarse como un Centro de Respuesta CSIRT, para fortalecer la respuesta a incidentes y la gestión de vulnerabilidades según los servicios contratados por sus clientes.

El objetivo del proyecto es el diseño de la documentación administrativa de un Equipo de Respuesta a Incidentes Cibernéticos (CSIRT) para la empresa Cibersecurity de Colombia LTDA, su desarrollo se fundamenta en una metodología de investigación documental descriptiva, que comprende la selección, análisis e interpretación de documentos y material de consulta, referente a los procesos administrativos y funcionamiento de diferentes equipos de respuesta CSIRT.

Como resultado se busca la documentación administrativa que permita el funcionamiento de un CSIRT, incluyendo el ámbito de actuación del equipo de respuestas, la taxonomía de ataques, el catálogo de servicios, los requisitos y perfiles del equipo de trabajo, las políticas y procedimientos operacionales y la estructura orgánica sugerida.

[1] Vega Barbosa, C. Las pymes como blanco para los ciberdelincuentes. [En línea]. 2018. [Consultado el 5 de Octubre de 2019]. Disponible en: https://www.elespectador.com/tecnologia/las-pymes-como-blanco-para-los-ciberdelincuentes-articulo-828209

[2] Revista Dinero. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [En línea]. 2019. [Consultado el 5 de Octubre de 2019]. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

PALABRAS CLAVE: AMENAZAS, CIBERDEFENSA, CIBERDELINCUENTES, CIBERSEGURIDAD, CSIRT, SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA, RIESGO INFORMÁTICO, VULNERABILIDADES.

ABSTRACT

According reports from the multinationals CISCO and FORTINET, exist in Colombia important cybersecurity gaps, which mainly affect the business and government sectors, additionally affirm alarming rates of informatic attacks in the country, generating potential security problems for companies. One cause for high rates of cyber-attacks is the constant development of increasingly sophisticated tools and techniques to violate networks and information systems, therefore, companies require constant updating, specialization and implementation of new strategies to secure your information assets.

This applied project is developed on the hypothetical scenario of an Information security services company called "Cibersecurity de Colombia LTDA", whose purpose is to consolidate itself as a Cyber Incident Response Center, to strengthen the incidents response and the vulnerabilities management, according services contracted by its clients.

The objective of this applied project is the design of the administrative documentation of a Computer Security Incident Response Team (CSIRT), for the company Cibersecurity de Colombia LTDA. the development is based on a descriptive documentary research methodology, which includes the selection, analysis and interpretation of documents and consultation material, referring to the administrative processes and operation of different CSIRT.

As a result, the administrative documentation that allows the operation of a CSIRT is sought, including the scope of action of the response center, the taxonomy of attacks, the catalog of services, the requirements and profiles of the work team, the operational policies and procedures and the suggested organizational structure.

KEYWORDS: COMPUTER RISK, COMPUTER SECURITY, CYBER DEFENSE, CYBER CRIMINALS, CYBER SECURITY, CSIRT, INFORMATION SECURITY, THREATS, VULNERABILITIES.

INTRODUCCIÓN

El constante crecimiento y globalización de las Tics, ha provocado que la seguridad de la información tome mayor importancia, en la actualidad, cada vez más empresas dependen en menor o mayor medida de arquitecturas tecnológicas y sistemas informáticos. Ese crecimiento en la demanda de los sistemas de información ha generado un mayor campo de acción para los riesgos y amenazas informáticas de las organizaciones, donde los ciber ataques y delitos informáticos están creciendo con mayor frecuencia, por lo tanto, se hace necesaria la implementación de métodos y estrategias, para reducir y controlar dichos riesgos y amenazas, con el propósito de no afectar la continuidad de los negocios. Una de esas estrategias comprende la implementación de Equipos de Respuesta ante Incidentes Cibernéticos (CSIRT).

En el presente proyecto se realiza una revisión documental fundamentada en diferentes referencias bibliográficas, concernientes a los Equipos de Respuesta ante Incidentes Cibernéticos (CSIRT), que permite dar a conocer los aspectos más relevantes de los CSIRT, saber cómo funcionan y cuáles son sus requerimientos, características, servicios, tecnologías, amenazas, riesgos y sus modelos de operación, así como conocer su estado actual, su administración y el marco regulatorio en Colombia. Adicionalmente se desarrolla la documentación desde el enfoque Administrativo, para poner en marcha un CSIRT en la empresa de seguridad informática Ciber security de Colombia LTDA.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Uno de los primeros incidentes que afectó la seguridad de las TICS ocurrió en 1988, a causa del gusano informático llamado “Morris” desarrollado por Robert Tappan Morris, el cual afectó el 10% de los equipos y sistemas conectados a Arpanet, red que en su momento dio origen a la internet. El gusano informático aprovechaba las vulnerabilidades del sistema operativo Unix, para reproducirse hasta el punto de bloquear los ordenadores, causando pérdidas de más de 15 millones de dólares a nivel global. Ese incidente de ciberseguridad generó la necesidad de coordinar el trabajo de los profesionales en seguridad informática, apoyándose en estructuras organizativas que permitieran identificar, gestionar y controlar de forma rápida y eficiente, incidentes similares al ocurrido con el gusano Morris.[3]

A causa de ese incidente de seguridad la Agencia de Proyectos de Investigación Avanzados de Defensa (DAPRA), enfocó el problema de un modo más estructurado y propició la creación del primer equipo de respuestas para emergencias informáticas (CERT), ubicado en la universidad de Carnegie Mellon, Pensilvania. Bajo esas siglas empezaron a conformarse más grupos en diferentes universidades estadounidenses, con el objetivo de gestionar la seguridad de las redes informáticas, brindando servicios de respuestas rápidas ante ciberataques y publicando las amenazas y vulnerabilidades detectadas, permitiendo ofrecer información de apoyo para mejorar la seguridad entre los diferentes equipos CERT. Para complementar el concepto de CERT, se empezó a hablar de los equipos de respuesta CSIRT, los cuales ofrecen valor agregado a los servicios de prevención y gestión de incidentes de seguridad. A principios de los años 90, el concepto de CERT se trasladó a Europa y con el apoyo la Asociación Transeuropea de Investigación y Educación de Redes (TERENA), se empezaron a conformar los primeros equipos de respuesta en el continente europeo.[4]

Para el caso de américa Latina, la República de Argentina fue pionera en la operación de los CSIRT, estableciendo la Oficina Nacional de Tecnologías de

[3] CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. 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

[4] CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. 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

Información (ONTI), a través de la cual en el año 2005 creó el Equipo de Respuesta ante Emergencias Informáticas (ArCERT), que basó sus primeros esfuerzos en la inclusión digital, acceso y sensibilización sobre temas de ciberseguridad. Referente a Colombia con el fin de proteger sus infraestructuras críticas, el gobierno adoptó una política integral de ciberseguridad y ciberdefensa que responde a los incidentes relacionados con la seguridad digital, donde los aspectos técnicos están a cargo de tres instituciones principales:[5]

- Centro Cibernético Policial (CCP), encargado de asegurar la integridad de las redes de las fuerzas policiales y de la sociedad civil, utilizando toda su capacidad de investigación y control ciudadano.

- Comando Conjunto Cibernético (CCOC), encargado de mitigar los ataques cibernéticos y salvaguardar los bienes militares del país.

- ColCERT, encargado de la coordinación y supervisión a nivel nacional de todo lo relacionado con la ciberseguridad y ciberdefensa.

Adicional a las iniciativas del gobierno Colombiano para fortalecer la ciberseguridad, el sector privado también ha realizado grandes aportes al panorama de la seguridad, gracias a la creación de equipos de respuesta CSIRT que ofrecen sus servicios al sector empresarial y la ciudadanía en general. Diferentes empresas han optado por tercerizar los servicios de ciberseguridad en lugar de invertir recursos para crear sus propios equipos de respuestas a incidentes informáticos, lo que ha generado un fuerte mercado para los CSIRT comerciales. Algunos CSIRT que prestan servicios comerciales en Colombia son los siguientes:

- BS-CSIRT: Es un centro de operaciones con sede en Colombia que brinda servicios de ciberseguridad para el sector comercial.

- CSIRT-CCIT: Este equipo de respuesta pertenece a la Cámara Colombiana de Informática y Telecomunicaciones, que presta servicios a empresas privadas del sector de las telecomunicaciones.

- DigiCSIRT: Equipo de respuesta que brinda servicios a los clientes de la empresa DigiSoc SAS para todos los sectores económicos.

- ETEK-CSIRT: Equipo de respuesta para los miembros de la firma ETEK y clientes privados que requieran servicios de ciberseguridad.

[5] OEA. Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. [En línea]. 2013. [Consultado el 16 de Diciembre de 2020]. Disponible en: http://technoint.weebly.com/uploads/2/1/2/9/21297584/tendencias_del_cibercrimen_hecho_por_la_oea.pdf

- ITSSOC-CSIRT: Esquipo de respuesta que brinda servicios para el sector privado y gubernamental, especializado en el sector financiero y de seguros.

Este proyecto aplicado toma como referencia la empresa Cibersecurity de Colombia LTDA, que presta servicios de seguridad informática para diferentes clientes en todo el territorio colombiano. Uno de los objetivos de la empresa es consolidarse como un centro de respuestas CSIRT, que permita ofrecer servicios para Pymes y para el sector gubernamental, teniendo en cuenta diferentes niveles de servicio para brindar respuestas ágiles a incidentes y ejecutar una eficiente gestión de vulnerabilidades.

1.2 FORMULACIÓN DEL PROBLEMA

La multinacional CISCO Systems estima que más de la mitad de las PYMES de Latinoamérica tienen importantes brechas de seguridad, en razón de que los ciberataques no solo están dirigidos a las grandes empresas y al sector gobierno, las organizaciones de menor escala también son el objetivo de este tipo de delincuentes. Según estudios de CISCO, el 53% de las pymes latinoamericanas reportaron brechas de seguridad aludiendo que es un problema muy costoso, pues en el 40% de los casos de ataques cibernéticos, se generaron tiempos de inactividad empresarial de alrededor de ocho horas, lo cual generó impactos negativos en la productividad y prestación de los servicios. Adicionalmente en el 39% de los ataques se generaron daños en más del 50% de los sistemas de información y equipos, provocando pérdidas que oscilan entre los 320 millones y 8.000 millones de pesos por empresa damnificada.[6]

Actualmente Colombia es uno de los países de Latino América que más recibe intentos de ataques informáticos, donde las instituciones del gobierno y el sector empresarial son los principales objetivos. La compañía de ciberseguridad FORTINET realizó un estudio donde se reveló que, en el segundo trimestre del 2019 el país recibió más de 40 billones de intentos de ciberataques, situando a Colombia como uno de los países con más intentos de intrusiones informáticas de la región.[7]

[6] Vega Barbosa, C. Las pymes como blanco para los ciberdelincuentes. [En línea]. 2018. [Consultado el 5 de Octubre de 2019]. Disponible en: https://www.elespectador.com/tecnologia/las-pymes-como-blanco-para-los-ciberdelincuentes-articulo-828209

[7] Revista Dinero. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [En línea]. 2019. [Consultado el 5 de Octubre de 2019]. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

Las estadísticas demuestran que los ciberataques están en constante crecimiento y evolución, diariamente los delincuentes informáticos trabajan para aprovechar las vulnerabilidades de las redes y aplicaciones, desarrollando nuevas versiones de ataques y técnicas más sofisticadas para lograr sus objetivos. En Colombia diferentes empresas han reportado brechas de seguridad, confirmando que los índices de ciberataques son alarmantes, según lo anterior, se plantea la siguiente pregunta:

¿Cómo ayuda el diseño administrativo de un CSIRT en la gestión de incidentes informáticos para la empresa Cibersecurity de Colombia?

2 JUSTIFICACIÓN

La dificultad de mantener elevados niveles de seguridad para los sistemas de información, es una fuerte razón para implementar un equipo de respuesta a incidentes cibernéticos, su importancia se incrementa a causa de que los ataques informáticos son cada día más sofisticados y complicados de detectar, por lo tanto, se requiere de una constante actualización, especialización e implementación de nuevas estrategias y herramientas para asegurar los activos de información.[8]

Un equipo de respuesta a incidentes informáticos CSIRT está conformado por expertos de diferentes áreas relacionadas con la ciberseguridad, encargados de la prevención, identificación y respuesta ante incidentes informáticos. El CSIRT ofrece los servicios necesarios para mitigar y eliminar las vulnerabilidades, amenazas y los riegos informáticos de una organización, adicionalmente brindan respuestas rápidas y oportunas ante cualquier tipo de incidente o solicitud de seguridad. Estos equipos de respuesta no solo se encargan de la gestión de incidentes, también diseñan planes y estrategias para la recuperación ante desastres. Los principales objetivos de los equipos de respuesta son:[9]

- Definir las políticas, procedimientos y servicios de respuesta a incidentes informáticos.
- Informar sobre los incidentes detectados.
- Gestionar los incidentes.
- Identificar causas y responsables de los incidentes.
- Recuperar la organización ante los incidentes.
- Evitar la repetición de incidentes.

Disponer de un equipo de respuesta a incidentes informáticos ayuda a las organizaciones a prevenir y mitigar los incidentes que pueden afectar

[8] CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. 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

[9] De la Torre Moscoso, H. M., & Parra Rosero, M. A. Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. [En línea]. 2018. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://repositorio.espe.edu.ec/jspui/handle/21000/15071

negativamente sus objetivos y su patrimonio, las principales ventajas de estos equipos de respuesta son:[10]

- Centralización de las solicitudes relacionadas con la seguridad informática dentro de la Organización (punto de contacto).

- Reacción temprana ante los incidentes de seguridad.

- Posibilidad de contar con las herramientas y personal capacitado para apoyar a los usuarios que requieren solucionar incidentes de seguridad.

- Permite realizar seguimiento y trazabilidad de los avances en la gestión de incidentes de seguridad.

- Fomenta la sensibilización y participación de los usuarios.

El presente proyecto aplicado busca contribuir al desarrollo social, académico y tecnológico de la región, en el ámbito social se contribuye al fortalecimiento de la inclusión digital de las personas, permitiendo su sensibilización en temas relacionados con la ciberseguridad. En el entorno académico, el diseño administrativo de un CSIRT permite generar la documentación necesaria, para construir una base de conocimiento que facilite la investigación y trabajos futuros. En el contexto tecnológico, por medio de un CESIRT se fortalece la seguridad de la infraestructura Tic de las organizaciones, gracias a una mejor gestión de los riesgos y amenazas que afectan la seguridad de los activos de información.

La motivación personal para desarrollar el proyecto aplicado inicia en el ámbito laboral, ya que muchas empresas han afrontado problemas de ciberseguridad durante sus jornadas laborales, afectando los procesos y la productividad del recurso humano. Con la capacitación constante y el desarrollo del presente proyecto, se busca adquirir conocimientos para proponer estrategias que mitiguen futuros ataques y amenazas informáticas en las empresas.

[10] Palacios Santamaría, P. A., & Andrés, P. Equipo de respuesta ante incidentes informáticos para La Universidad Regional Autónoma de Los Andes. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: http://dspace.uniandes.edu.ec/handle/123456789/8158

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar la documentación desde el enfoque directivo administrativo, que permita dar desarrollo a las actividades propias de un CSIRT para la empresa Cibersecurity de Colombia Ltda.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer la taxonomía de ataques y el ámbito de actuación del CSIRT.
- Elaborar el catálogo de servicios proactivos, reactivos y complementarios del CSIRT.
- Proponer la estructura orgánica y los perfiles del equipo de trabajo para la conformación del CSIRT.
- Formular las políticas y procedimientos operacionales del CSIRT.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Existen diferentes investigaciones recientes referentes al tema principal este proyecto aplicado, el propósito del marco teórico es disponer de una base de conocimientos que sirva como referencia para desarrollar los objetivos del proyecto, para tal fin, se resumen algunas investigaciones referentes al diseño de equipos de respuesta ante incidentes informáticos CSIRT, de diferentes sectores como el educativo, empresarial y gubernamental.

4.1.1 Implementación de un equipo de respuesta a incidentes de seguridad informática CSIRT en la Fiscalía General del Estado

Esta investigación tiene como objetivo la implementación de un CSIRT para la Fiscalía General del Estado - Ecuador (FGE), inicialmente los autores describen el estado del arte, por medio de una revisión bibliográfica y la recolección documental de casos de éxito en la implementación de equipos de respuesta CSIRT en Latinoamérica. Seguidamente muestran un estudio de la situación actual y contexto de la FGE enfocado hacia la seguridad informática, obteniendo como resultado un análisis detallado de las amenazas cibernéticas más concurrentes en la organización. Con las anteriores actividades los autores obtienen una línea base para realizar el diseño del CSIRT de la FGE y toman como referencia las mejores prácticas definidas por el estándar RFC 2350 y el Foro Mundial FIRST.[11]

El diseño desarrollado define la comunidad objetivo del CSIRT, las políticas, procedimientos, servicios y el equipo necesario para iniciar operaciones, adicionalmente define la estructura orgánica y funcional, la infraestructura tecnológica necesaria, el presupuesto y las normativas para iniciar la prestación de servicios de ciberseguridad. Finalmente, Los autores concluyen que se logró satisfactoriamente la implementación del CSIRT en la Fiscalía General del Estado, basándose en las mejores prácticas y estándares internacionales, logrando un incremento en el nivel de ciberseguridad en la institución.

[11] Hurtado Vargas, L. F. & Chuquiguanca Vicente, L. R. Implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) en la Fiscalía General del Estado. [En línea]. 2020. [Consultado el 16 de Diciembre de 2020]. Disponible en: https://repositorio.uisek.edu.ec/handle/123456789/3959

4.1.2 Equipo de respuestas ante incidentes de seguridad informáticos para la Universidad Regional Autónoma de los Andes

El objetivo de esta investigación es la implementación de un CSIRT, para la Universidad Regional Autónoma de los Andes - Ecuador. Inicialmente el autor realiza una recopilación de información por medio de entrevistas, encuestas y revisión documental, partiendo del contexto de la universidad la cual dispone de un número significativo de sistemas de información, importantes para la gestión y funcionamiento del campus universitario. La investigación se desarrolló en base a una metodología cualitativa y cuantitativa, permitiendo la recolección de información importante para conocer la problemática de estudio y las alternativas de solución. La propuesta de solución al problema plantea el diseño de un área especializada que integra conceptos, metodologías y procedimientos para la gestión de evidencias e incidentes informáticos, permitiendo a los investigadores el análisis de los incidentes cibernéticos recopilados.

El autor concluye que la implementación del CSIRT aportó mejoras en la seguridad de la información de la Universidad Regional Autónoma de los Andes, ya que el prototipo implementado permite una doble capa de seguridad en los sistemas de información del campus universitario, y gracias a las pruebas realizadas, se logró comprobar que el sistema de registro de incidencias soluciona la problemática de estudio y cumple con el objetivo planteado.[12]

4.1.3 Gestión de incidentes de seguridad de la información para la Superintendencia Financiera de Colombia

El objetivo de la investigación es Implementar un sistema de gestión de incidentes de seguridad de la información para la Superintendencia Financiera de Colombia, la cual cuenta con políticas de seguridad de la información ya definidas y para complementarlas se diseñó un modelo para la gestión de incidentes cibernéticos, aprobado por el área de seguridad de la dirección de tecnología de la institución. La metodología aplicada busca la optimización de los procesos de tecnología para mejorar la operación del negocio, aprovechando las herramientas disponibles por la superintendencia y tomando como referencia un modelo internacional para estructurar los procesos, definir las actividades, las categorías y los responsables del sistema de gestión de incidentes. Adicionalmente se definen los subprocesos de registro, categorización, clasificación de incidentes, validación, investigación y diagnóstico.[13]

[12] Palacios Santamaría, P. A., & Andrés, P. Equipo de respuesta ante incidentes informáticos para La Universidad Regional Autónoma de Los Andes. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: http://dspace.uniandes.edu.ec/handle/123456789/8158

[13] Pachón Ramírez, J. A. Gestión de incidentes de seguridad de la información para la superintendencia financiera de Colombia. [En línea]. 2016. [Consultado el 16 de Diciembre de 2020]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2773

El autor concluye que, con la implementación del proceso de gestión de incidentes para la Superintendencia Financiera de Colombia, se asegura la continuidad del negocio, manteniendo unos niveles satisfactorios de calidad y disponibilidad del servicio, permitiendo gestionar todos los incidentes informáticos por parte de la dirección de tecnología de la información de la institución.

4.1.4 Modelo de gestión de incidentes de seguridad de la información para PYMES

Esta investigación tiene como objetivo diseñar un modelo de gestión de incidentes de seguridad de la información para pequeñas y medianas empresas PYMES, con lo cual se mejora la gestión de incidentes que afectan la integridad, confidencialidad y disponibilidad de la información. La metodología utilizada para el desarrollo del proyecto fue la monografía de compilación y análisis de experiencias. Inicialmente el autor realizó una consulta y recopilación documental referente al tema de investigación, entre el material recolectado se obtuvieron páginas en internet, libros de seguridad de la información, normas internacionales, e indagaciones realizadas a expertos en seguridad informática, seguidamente el autor realizó un análisis de la información recolectada, que entregó como resultado las ventajas, desventajas y beneficios que ofrece el diseño de un modelo de gestión de incidentes de seguridad de la información. Finalmente, el autor elabora un documento compilatorio donde describe las características y las etapas que se deben ejecutar en la definición del modelo de gestión de incidentes.[14]

El autor concluye que un sistema de gestión de seguridad de la información no define un modelo de gestión de incidentes, provocando vacíos que generan vulnerabilidades en las empresas, pero que pueden ser corregidos gracias a los modelos de gestión de incidentes, los cuales preparan a las empresas para detectar y corregir las vulnerabilidades que puedan generar impactos negativos en las empresas.

[14] Delvasto Ramírez, R. A. Modelo de Gestión de incidentes de seguridad de la información para PYMES. [En línea]. 2016. [Consultado el 16 de Diciembre de 2020]. Disponible en: https://repository.unad.edu.co/handle/10596/6170

4.2 MARCO CONCEPTUAL

La ciberseguridad se puede definir como la capacidad que tienen las organizaciones de minimizar los niveles de riesgos cibernéticos a los que están expuestas, específicamente en sus activos de información, transacciones financieras y propiedad intelectual.[15]Una estrategia efectiva para fortalecer la ciberseguridad de las organizaciones es la gestión de los incidentes informáticos y la centralización de los recursos y capacidades de seguridad, por medio de equipos de respuestas a incidentes cibernéticos, los cuales brindan respuestas rápidas y efectivas ante posibles ataques y amenazas que afecten los activos de información. A continuación, se describen los principales conceptos y características referentes a los equipos de respuesta CSIRT.

4.2.1 Equipo de Respuesta a Incidentes Cibernéticos

Un equipo de respuesta a incidentes cibernéticos CSIRT es un equipo de especialistas en temas de ciberseguridad, dedicados a prevenir y responder oportunamente ante incidentes que afecten la seguridad de los activos de información en una organización. Existen diferentes nombres y abreviaturas para identificar este tipo de centros, los cuales tienen objetivos similares, algunas de estas abreviaturas son CSIRT, CERT, CIRT, IRT, SERT [16]

4.2.2 Taxonomía de ataques de un CSIRT

Una taxonomía es una clasificación que permite un mejor entendimiento sobre un tema o campo de estudio, para el caso de la seguridad informática existen clasificaciones taxonómicas que permiten conservar, organizar y representar de forma eficiente la información sobre incidentes de ciberseguridad. Las taxonomías no son únicas, por lo tanto, no se cuenta con un sistema universal, encontrando clasificaciones simples y otras más completas.[17]

Las clasificaciones taxonómicas deben cumplir ciertas características que permiten un adecuado entendimiento del tema o campo de estudio, en términos

[15] CORTÉS BORRERO, R. ESTADO ACTUAL DE LA POLÍTICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA. [En línea]. 2015. [Consultado el 5 de Noviembre de 2019]. Disponible en: https://doi.org/10.15425/redecom.14.2015.06

[16] Miranda, J. M., & Ramirez, H. Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (17), 1–15. 2016. https://doi.org/10.17013/risti.17.1-15

[17] Bayona, Z. O. Hacia una Taxonomía de Incidentes de Seguridad en Internet. [En Línea]. 2006. [Consultado el 14 de marzo de 2021]. Disponible en: https://revistas.udistrital.edu.co/index.php/reving/article/view/2308/3126

generales, una taxonomía debe ser excluyente, exhaustiva, no ambigua, precisa, repetible, aceptada y útil. Para obtener una clasificación de incidentes de seguridad cumpliendo las características anteriormente citadas, se puede hacer uso de los siguientes métodos basados en listas:

- **Términos:** Es una lista que contiene definiciones de términos de ciberseguridad como bombas lógicas, troyanos, virus, gusanos, denegación de servicio, degradación de servicio, copia no autorizada, entre otros.

- **Categorías:** Esta aproximación a la taxonomía de ataques incluye una estructura más elaborada, Cheswick y Bellovin[18] incluyen 7 categorías para clasificar los ciberataques (ingeniería social, errores de SW, robo de contraseñas, autenticación fallida, problemas de protocolos, pérdida de información y denegación de servicio).

- **Resultados.** Esta es una variación del método de la lista de categorías que agrupa los ataques según los resultados obtenidos. Como ejemplos se pueden mencionar la fuga de información, denegación de servicios, confidencialidad, exactitud, integridad, autenticidad y disponibilidad.

- **Empíricas.** Esta es una variación de método de resultados que utiliza una lista más completa basada en información de clasificación empírica, en este método se puede citar el robo de información, abuso de recursos, errores de autenticación, enmascaramiento, abuso de sistema informático, entre otros.

- **Taxonomías basadas en procesos.** Este método simplificado clasifica las amenazas de seguridad en cuatro categorías relacionadas con la interrupción, intercepción, modificación y fabricación.

4.2.3 Servicios de un CSIRT

Los servicios de un Equipo de Respuestas a Incidentes Informáticos dependen de las necesidades del entorno sobre el cual actúa, por lo general los servicios están alineados con las necesidades y objetivos estratégicos de las organizaciones. A continuación, se presenta una tabla con los principales servicios de un CSIRT:[19]

[18] William R. Cheswick y Steven M. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Publishing Company, Estados Unidos, 1994.

[19] Luna, R. Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). [En línea]. 2015. [Consultado el 17 de Octubre de 2019]. Disponible en: http://www.revistascientificas.udg.mx/index.php/REC/article/view/5209/4865

Cuadro 1. Servicios de un CSIRT

Servicios reactivos	Servicios proactivos	Manejo de instancias
Alerta y advertencias	Comunicados	Análisis de instancias
Tratamiento de incidentes	Observatorio de tecnología	Respuesta a las instancias
Análisis de incidentes	Evaluaciones o auditoría de la seguridad	Coordinación de la respuesta a las instancias
Apoyo a la respuesta e incidentes	Configuración y mantenimiento de la seguridad	Gestión de la calidad de la seguridad
Coordinación de la respuesta a incidentes	Desarrollo de herramientas de seguridad	Análisis de riesgos
Respuesta a incidentes	Servicios de detección de intrusos	Continuidad negocio y recuperación tras un desastre
Respuesta a incidentes en el sitio	Difusión de información relacionada con la seguridad	Consultoría de seguridad
Tratamiento de la vulnerabilidad		Sensibilización
Análisis de la vulnerabilidad		Educación / Formación
Respuesta a la vulnerabilidad		Evaluación o certificación de productos

Fuente.
http://www.revistascientificas.udg.mx/index.php/REC/article/view/5209/4865

4.2.4 Tipos de CSIRT

Los CSIRT se estructuran dependiendo el sector y tipo de organización al que van a atender, diferenciándose por la misión y objetivos de la organización, la comunidad a la que dirigen sus servicios y los servicios que ofrecen a la organización. Dependiendo del sector se pueden encontrar CSIRT para diferentes ámbitos como el académico, comercial, público, interno, militar, Nacional, Pyme, entre otros. [20]

4.2.5 Beneficios de un CSIRT

Disponer de un equipo responsable de la ciberseguridad, estructurado en un modelo de coordinación centralizada y especializado en atender solitudes e incidentes informáticos, ayuda a las organizaciones a prevenir, mitigar y eliminar

[20] Armas, H. andrés. GESTIÓN DE SEGURIDAD EN LA RED DE DATOS DE LA CORTE CONSTITUCIONAL MEDIANTE EL DISEÑO DE UN CSIRT (EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD). [En línea]. 2012. [Consultado el 17 de Octubre de 2019]. Disponible en: https://dspace.ups.edu.ec/handle/123456789/3776

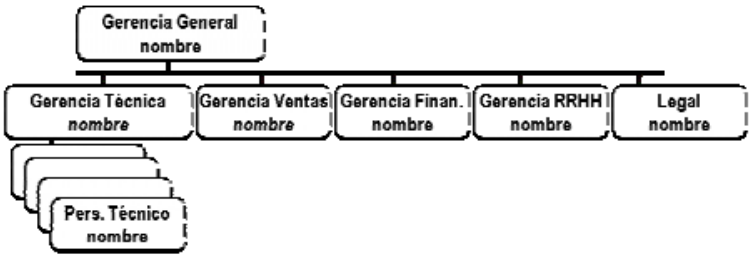
los riesgos que pueden afectar negativamente sus patrimonios, fomentando la cooperación entre los miembros de la organización y sus interesados. La centralización de actividades de seguridad es una tendencia recomendada por estándares internacionales, lo cual ayuda a cumplir las normatividades y buenas prácticas del sector. Otro beneficio de los equipos de respuesta es la rápida y oportuna respuesta ante la operación y mantenimiento de la infraestructura tecnológica, que difícilmente es asumible con personal y equipos dispersos y descoordinados.[21]

4.2.6 Modelos de CSIRT

4.2.6.1 Modelo de CSIRT independiente

Este modelo contempla un CSIRT que funciona como una organización independiente, con una estructura propia donde hay niveles jerárquicos como directivos, jefes de área, líderes, y operativos.

Figura 1. Modelo de CSIRT Independiente



Fuente: http://catai.net/blog/wp-content/uploads/2009/01/premioacademiacanariaseguridad.pdf

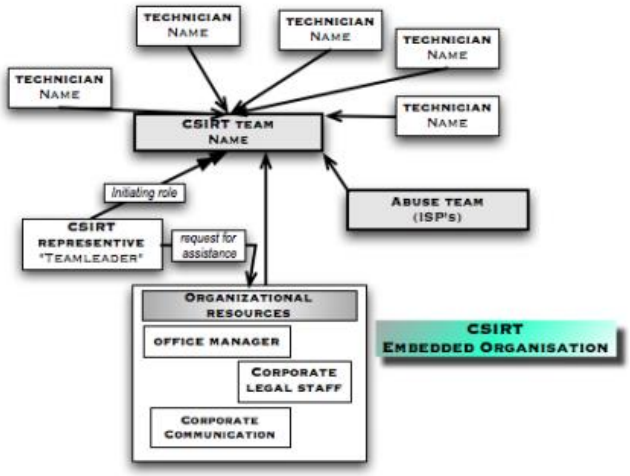
4.2.6.2 Modelo de CSIRT incrustado

Este modelo se implementa dentro de la estructura de una organización existente utilizando los recursos y capacidades del área del departamento de sistemas existente. El CSIRT incrustado está dirigido por un jefe encargado de gestionar todas las actividades de nivel directivo administrativo del equipo de trabajo, adicionalmente supervisa el personal necesario para resolver las solicitudes e

[21] Uyana García, M. A. Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. [En línea]. 2014. [Consultado el 17 de Octubre de 2019]. Disponible en: http://repositorio.espe.edu.ec/jspui/handle/21000/8063

incidencias que ocurren en la organización. Este tipo de CSIRT se adapta a las necesidades de la organización a medida que surgen situaciones específicas.[22]

Figura 2. Modelo de CSIRT Incrustado



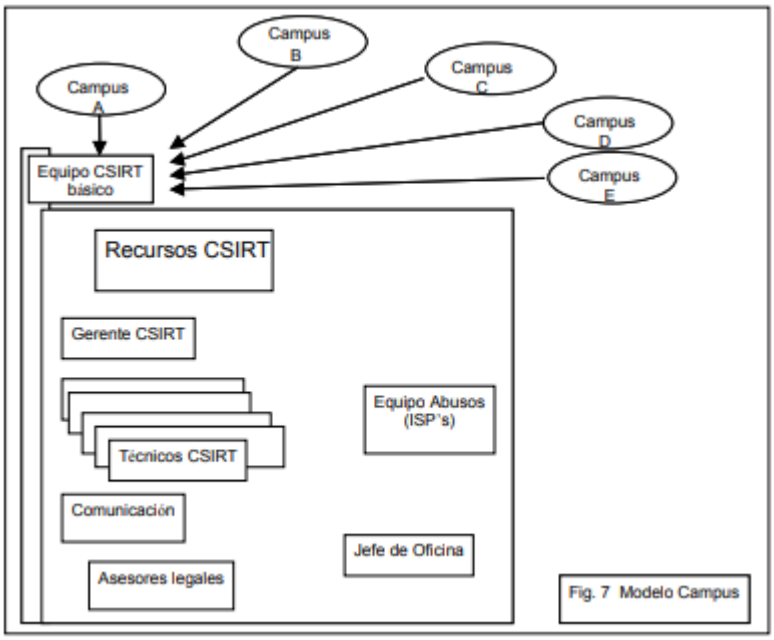
Fuente: http://catai.net/blog/wp-content/uploads/2009/01/premioacademiacanariaseguridad.pdf

4.2.6.3 Modelo de CSIRT campus

Este modelo es muy utilizado en los ambientes académicos por lo general universitarios, inclusive puede abarcar una o varias instituciones de educación y dependencias situadas en diferentes ubicaciones geográficas o todo un país. Por lo general, este tipo de CSIRT tiene otros equipos de respuestas locales que están bajo el control de una sede principal o central, la cual actúa como coordinador de las solicitudes e incidentes a nivel regional o nacional, proporcionando servicios, información y procedimientos a los demás equipos, logrando una mejor estandarización e integración de los servicios del CSIRT, permitiendo una mayor optimización de los recursos y procesos.

[22] Asociación CATAI. Modelo de Coordinación y Atención de Emergencias en el ámbito de la Sociedad de la Información. [En línea]. 2007. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://catai.net/blog/wp-content/uploads/2009/01/premioacademiacanariaseguridad.pdf

Figura 3. Modelo de CSIRT Campus



Fuente: http://catai.net/blog/wp-content/uploads/2009/01/premioacademiacanariaseguridad.pdf

4.2.6.4 Modelo de CSIRT voluntariado

Este modelo es utilizado por equipos de respuesta compuestos por grupos de especialistas, que se organizan para apoyarse entre sí y brindar asesorías a otros grupos u organizaciones. Por lo general, son colectivos sin ánimo de lucro que actúan de forma voluntaria motivados por fines de investigación y desarrollo tecnológico.[23]

4.3 MARCO HISTÓRICO

En el año 1988 ocurrió uno de los primeros incidentes cibernéticos que afectó la infraestructura y servicios TIC a nivel mundial, el gusano informático llamado “Morris” se propagó rápidamente infectando diferentes equipos y sistemas de información, provocando caos y millonarias pérdidas. La respuesta y gestión de ese incidente de seguridad fue poco eficiente y descoordinada, obligando a los expertos a redoblar sus esfuerzos en soluciones complicadas y poco eficaces. Ese

[23] ENSIA. CSIRT Setting up Guide in Spanish — ENISA. [En línea]. 2006. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish

incidente fue una de las razones para que la Universidad Carnegie Mellon, creara el primer equipo de respuestas ante emergencias informáticas CERT, el cual actuaba como un centro de seguridad mediante la detección, difusión y comunicación de este tipo de emergencias. Posteriormente se fundaron más equipos de respuesta CERT en diferentes países, y se introduce el concepto de CSIRT, “equipos de respuesta ante incidentes cibernéticos” los cuales mejoraban los servicios de los primeros CERT, pero tenían dificultades de coordinación y comunicación a causa de los idiomas y las zonas horarias. En el año 1989 se generó un nuevo incidente de seguridad informática, provocado por el gusano llamado “walk”, el cual generó la necesidad de mejorar la comunicación y coordinación de los equipos de respuesta del momento.[24]

En diferentes países los equipos de respuesta CSIRT surgieron como estrategia de instituciones académicas y redes de investigación, con el tiempo se fueron implementado en otros sectores como el gubernamental, empresarial y financiero. En sus inicios estos equipos de respuestas solo se dedicaban a emitir alertas y recomendaciones básicas de seguridad a las organizaciones, sin embargo, se crearon nuevos CSIRT más especializados con facultades para tomar decisiones y con más autonomía. El constante crecimiento de ataques informáticos incrementó el interés de los gobiernos y el sector privado por financiar las iniciativas de los CSIRT, en razón de que organismos internacionales recomendaron el establecimiento de equipos de respuesta CSIRT nacionales, adicionalmente se implementaron normativas y convenios de cooperación en materia de ciberseguridad y ciberdefensa.

En el año 1990 se crea el foro global de respuesta a incidentes y equipos de seguridad (FIRST), este comprende una comunidad de equipos de respuesta con más de 500 miembros, convirtiéndose en la organización de CSIRT más importante del mundo. Los equipos que pertenecen a FIRST están en la capacidad de atender incidentes cibernéticos de forma rápida y eficaz, ya que se trabaja articuladamente con otros CSIRT de diferentes sectores como el gubernamental, comercial, educativo, financiero, entre otros. El propósito de FIRST es fomentar la cooperación y coordinación para permitir reacciones rápidas ante incidentes y colaborar con la divulgación de información entre sus miembros. Actualmente FIRST continúa siendo referente a nivel mundial en la coordinación e implementación de buenas prácticas en los CSIRT, para ser miembro de esta organización es necesario que los grupos de respuesta interesados realicen un procedimiento de validación y certificación acorde al estándar RFC 2350.

[24] Hurtado Vargas, L. F. & Chuquiguanca Vicente, L. R. Implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) en la Fiscalía General del Estado. [En línea]. 2020. [Consultado el 16 de Diciembre de 2020]. Disponible en: https://repositorio.uisek.edu.ec/handle/123456789/3959

4.4 ANTECEDENTES O ESTADO ACTUAL

4.4.1 Panorama actual de la ciberseguridad

Según Luisa Esguerra, Country Manager de la multinacional Symantec, La ciberseguridad en Colombia ha evolucionado positivamente en los últimos años, gracias a las mejoras en las regulaciones locales y a las inversiones en ciberseguridad y ciberdefensa que rondan los 20 mil millones de pesos, realizadas por empresas de sectores económicos como el financiero, telecomunicaciones y gobierno, enfocándose principalmente en la protección de la computación en la nube, el correo electrónico, la infraestructura, la fuga de información y el monitoreo avanzado.[25] Pero según la firma de reclutamiento avanzado "Michael Page" menciona que por causa de la gran demanda en el sector de la ciberseguridad, no hay suficiente personal calificado para desempeñarse en la industria, por tal razón, es necesario que más personas se formen y capaciten en tecnologías de la información y ciencias de la computación.[26]

Actualmente el país se encuentra en un rango medio de ciberseguridad según índices de referencia mundial, donde Japón cuenta con los mejores indicadores y Argelia con los peores. Diferentes análisis han demostrado que en Colombia mas del 12% de los equipos móviles están infectados con algún tipo de malware, en cuanto a computadores, las infecciones son mayores, llegando a un 16%. Sobre la preparación para soportar un ciberataque el país tiene un puntaje de 0,56 cuando 1 es el tope, en cuanto a la generación de ataques informáticos desde el interior del país, Colombia sale mejor librado, produciendo solo el 0,5% de los ataques al sistema financiero, donde en otros países ronda por el 2%.[27]

4.4.2 Tendencias y retos en materia de ciberseguridad

En el año 2018 se presentó una acelerada actividad de amenazas informáticas en diferentes ámbitos como el empresarial y hogar, los ataques informáticos a los principales sistemas corporativos aumentaron y continuaron creciendo a un ritmo

[25] Gerente.com. Ciberseguridad en Colombia tiene pocos expertos. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: http://gerente.com/co/ciberseguridad-expertos-colombia/

[26] ACIS. Hay escases de personal calificado en la industria de ciberseguridad en Colombia. [En línea]. 2017. [Consultado el 17 de Octubre de 2019]. Disponible en: https://acis.org.co/portal/content/hay-escases-de-personal-calificado-en-la-industria-de-ciberseguridad-en-colombia

[27] Revista Semana. Así está Colombia en el ranking de ciberseguridad mundial. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

acelerado. Expertos en temas de ciberseguridad de todo el mundo compartieron las amenazas que se prevén para los próximos años, las cuales se presentan a continuación:[28]

- El spam se especializa y se personaliza, permitiendo a los atacantes segmentar grupos de personas y organizaciones en determinadas áreas geográficas, para enviar ofertas fraudulentas diseñadas para llamar la atención y engañar a los usuarios.

- La confianza digital continúa siendo tema de preocupación para entidades financieras, alrededor de dos tercios de los usuarios del sector, están preocupados por los posibles problemas y delitos informáticos con sus tarjetas y cuentas.

- Los sistemas de autenticación sin contraseña prometen mayor seguridad, ya que actualmente existen muchos riesgos y vulnerabilidades en las combinaciones de usuarios y contraseñas, por lo tanto, en los próximos años se prevé un aumento en los sistemas de autenticación sin contraseñas.

- Las tiendas de descarga de aplicaciones son un gran mercado para los ciberdelincuentes, ya que este tipo de plataformas brindan el entorno perfecto para los malware, generando en los usuarios falsas expectativas de confianza, hasta el punto de que los usuarios descargan apps sin conocer su legitimidad.

- Gestión de credenciales: Los ciberdelincuentes saben que muchas personas utilizan las mismas combinaciones de usuario y contraseña en diferentes portales web y sistemas de información, por lo tanto, los ataques de relleno de credenciales o “credential stuffing” aumentarán, ya que brindan una manera rápida y simple de validar usuarios y contraseñas.

- Las organizaciones están basando sus estrategias de seguridad en los sistemas de seguridad del sector bancario, técnicas de autenticación como la biometría, push, token en el móvil, son muy efectivas y mantienen felices a los bancos.

[28] Revista Dinero. Ciberseguridad en el 2019 en Colombia. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

4.4.3 Casos de ciberataques en Colombia

En mayo del año 2017 el ministerio de las TIC alerto sobre un ataque cibernético de escala mundial que afecto diferentes empresas en Colombia, el ataque se denominó “Wanna Cry” el cual es un malware del tipo Ransomware que secuestra la información de los equipos victimas a cambio de un pago en bitcoins para su liberación. El director del centro cibernético policial confirmo que al menos 11 importantes empresas del sector privado reportaron fallas ocasionadas por dicho malware, el director reiteró que las empresas y personas afectadas por este ataque no tuvieron las precauciones suficientes ya que no contaban con los sistemas operativos actualizados en sus últimas versiones.[29]

Los ataques DDos a portales web, el ransomware y los ataques contra el sistema financiero, son las amenazas más concurrentes en Colombia, por otra parte, en el primer trimestre de 2019 se detectaron cerca de 30.000 archivos de malware para el sector financiero.[30]La lucha contra la ciberdelincuencia es uno de los principales retos del país, esta actividad se actualiza y se transforma constantemente con el propósito de aprovechar las vulnerabilidades de los sistemas y acceder a los millones de datos e información sensible de empresas y personas. Según balances de la policía Nacional, en el 2017 los delitos informáticos afectaron más de 400 empresas de todo el territorio colombiano, donde el secuestro de información fue el delito que causó más perdidas, otro delito que afecta las empresas del país es la suplantación de correo corporativo, que puede provocar pérdidas de casi 400 millones de pesos por cada ataque, según el centro cibernético policial.[31]

La Unidad Nacional de Protección por medio de su director, denuncio que diariamente reciben cientos de ataques cibernéticos, por tal razón, el gobierno nacional inicio un proceso de reingeniería y modernización del componente tecnológico de la unidad, lo anterior, con el propósito de prevenir hackeos o robos de información sensible de quienes gozan de esquemas de seguridad en el país. El director confirmó que diariamente reciben 500 intentos de hackeos, en razón de que la unidad cuenta con equipos tecnológicos obsoletos.[32]

---

[29] El Heraldo. Ciberataque golpeó a 11 empresas y una entidad pública en Colombia. [En línea]. 2017. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elheraldo.co/ciencia-y-tecnologia/ciberataque-golpeo-11-empresas-y-una-entidad-publica-en-colombia-361747

[30] Velasquez, A. M. Principales ataques de cibercriminales en Colombia. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-ataques-de-cibercriminales-en-colombia-371096

[31] Portafolio. El secuestro de información desangra a las empresas del país. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

[32] Jerez, D. UNP advierte que recibe 500 ataques cibernéticos al día. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.lafm.com.co/colombia/unp-advierte-que-recibe-500-ataques-ciberneticos-al-dia

En marzo del 2018 la Registraduría General de la Nación fue víctima de 4 ataques cibernéticos encaminados a afectar la disponibilidad del sitio web de la entidad, tres de dichos ataques se originaron en Colombia y uno de ellos en Venezuela. En una sola semana se registraron 28.000 ataques a las páginas de la Registraduría y del Servicio Electoral. Estos ataques se generaron desde direcciones IP de mala reputación que buscan dañar la funcionalidad y operatividad de las páginas de las entidades. Estos datos los entrego el registrador faltando cuatro días para iniciar las jornadas electorales, con lo que se confirma que este tipo de ataques se incrementan en dichas épocas.[33] Es importante recordar que en vísperas de las elecciones del 2016 lograron hackear la página de la Registraduría con intenciones de sabotear los resultados del plebiscito.[34]

4.4.4 CSIRT en Colombia

En Colombia existen diferentes equipos de respuesta CSIRT que fortalecen la ciberseguridad y ciberdefensa del país, el principal es el grupo de respuesta a emergencias cibernéticas de Colombia (ColCERT), el cual tiene sus inicios en el año 2008 como parte de un ejercicio de ciberseguridad, patrocinado por el Comité Interamericano contra el Terrorismo (CICTE), sin embargo, 3 años más tarde y gracias al Consejo Nacional de Política Económica y Social (CONPES 3701 2011), fue creado formalmente el ColCERT como coordinador a nivel nacional en temas de seguridad digital. La principal función del ColCert es “proteger las infraestructuras críticas del estado Colombiano frente a emergencias de ciberseguridad y ciberdefensa, que atenten o comprometan la seguridad y defensa nacional”, adicionalmente presta servicios coordinados con el comando conjunto cibernético de Colombia y el centro cibernético policial.[35]

4.4.4.1 Comando conjunto cibernético de las fuerzas militares

Este comando se desempeña como unidad elite en temas de ciberseguridad y ciberdefensa, incluyendo la infraestructura cibernética nacional. Desarrolla operaciones militares en el ciberespacio con el objetivo de defender la soberanía,

[33] El Espectador. Registraduría ha recibido cuatro ataques informáticos a su página web. [En línea]. 2018 [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elespectador.com/economia/se-han-registrado-cuatro-intentos-para-tumbar-la-pagina-de-la-registraduria-mindefensa-articulo-743295

[34] El Heraldo. Hackean página de Registraduría a cuatro días del plebiscito. [En línea]. 2016. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elheraldo.co/politica/hackean-pagina-de-registraduria-cuatro-dias-del-plebiscito-288431

[35] Hurtado Vargas, L. F. & Chuquiguanca Vicente, L. R. Implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) en la Fiscalía General del Estado. [En línea]. 2020. [Consultado el 16 de Diciembre de 2020]. Disponible en: https://repositorio.uisek.edu.ec/handle/123456789/3959

la independencia e integridad territorial, contribuyendo a generar un ambiente de paz, defensa y seguridad Nacional.[36]

4.4.4.2 Centro cibernético policial

El centro cibernético policial ejecuta labores de ciber patrullaje, con el objetivo de identificar posibles vulnerabilidades y amenazas que pongan en peligro la disponibilidad, confidencialidad e integridad de la información que se transmite en la web. El centro ha identificado tempranamente actividades ilícitas definidas como Cass (crimen como servicio), este tipo de ciber ataques se han incrementado con el tiempo, debido a que los criminales están guiando sus ataques a la medida de las víctimas. Desde la unidad investigativa del centro cibernético policial se despliegan acciones conjuntas con los administradores de redes sociales y plataformas informáticas internacionales, para enfrentar prácticas conocidas como Bulo o Hoax.[37]

4.4.4.3 Grupo de respuesta a emergencias cibernéticas de Colombia

El grupo de respuesta a emergencias cibernéticas de Colombia – ColCERT, coordina la ciber seguridad y ciber defensa Nacional, la cual está contemplada dentro de los procesos misionales de la gestión de la seguridad del Ministerio de Defensa Nacional. Adicionalmente estructura y organiza las acciones y estrategias necesarias para proteger las infraestructuras críticas del país, frente a emergencias y ataques cibernéticos que pongan en riesgo la seguridad y defensa Nacional.[38]

4.4.4.4 Csirt Asobancaria

El equipo de respuestas de Asobancaria es el primer centro de ciberseguridad para el sector bancario del país, el cual identifica los riesgos e incidentes de ciberseguridad a nivel nacional e internacional, a partir de información clasificada que permite la implementación de medidas preventivas ante ciberataques. Para lograr este objetivo, cuenta con más de 15 fuentes de información local y globalizada y se conecta en simultáneo con otros CSIRT para generar alertas

[36] CCOCI. COMANDO CONJUNTO CIBERNÉTICO. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.ccoc.mil.co/quienes_somos/ccoc/que_hacemos

[37] El Espectador. Un oficial del Centro Cibernético Policial de Colombia explica estrategia para elecciones. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elespectador.com/noticias/judicial/un-oficial-del-centro-cibernetico-policial-de-colombia-explica-estrategia-para-elecciones-articulo-737056

[38] colCERT. Grupo de Respuesta a Emergencias Cibernéticas de Colombia. [En línea]. 2017. [Consultado el 17 de Octubre de 2019]. Disponible en: http://www.colcert.gov.co/?q=acerca-de

tempranas a posibles amenazas informáticas.[39] Este equipo de respuestas será centro de excelencia en materia de ciberseguridad del sector y su reto es evolucionar constantemente a la velocidad de los avances tecnológicos y las nuevas generaciones de ataques informáticos.[40]

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

Los diferentes servicios de un CSIRT permiten la rápida identificación y gestión de incidentes informáticos, que por lo general se fundamenta en estrategias y tecnologías de ciberseguridad que se describen a continuación:

4.5.1 Sistemas de detección de intrusos

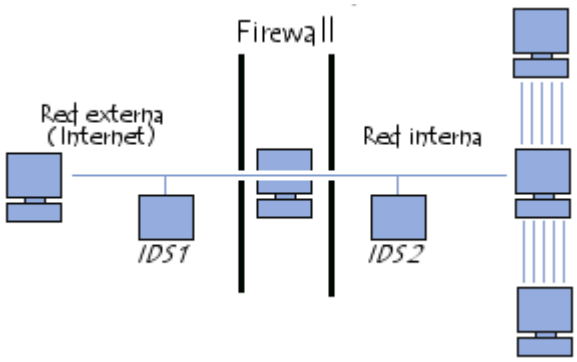
Los sistemas de detección de instrucciones son mecanismos que analizan el tráfico de una red de datos, con el propósito de detectar peticiones y actividades sospechosas, reduciendo el riesgo de ataques informáticos e intrusiones. Los IDS se pueden clasificar en IDS de red e IDS de host. El N-IDS es un sistema que verifica los paquetes de información que circulan por una red de datos, en busca de actividades maliciosas o anomalías ayudándose de los adaptadores de red, activando un modo de análisis invisible que no cuenta con direcciones IP ni protocolos asignados, siendo desapercibidos por los atacantes. Por lo general, los IDS se implementan en diferentes sectores de la red, es posible configurarlos fuera de la red para analizar los intentos de ataques, como también se pueden configurar dentro de la red para analizar los paquetes que hayan superado el firewall.[41]

[39] La República. Asobancaria presenta primer equipo de seguridad cibernética. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.larepublica.co/finanzas/asobancaria-presenta-primer-equipo-de-seguridad-cibernetica-2763005

[40] El Colombiano. La banca estrena bloque de reacción inmediata contra ciberataques. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elcolombiano.com/negocios/innovacion/seguridad-sistema-financiero-ciberataques-HX9213801

[41] Villagómez, C. Sistema de detección de intrusiones (IDS). [En línea]. 2017. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

Figura 4. Sistema de detección de intrusos



Fuente: https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

El H-IDS se ubica en un host cliente, permitiendo ser configurado en diferentes sistemas operativos como Windows, Linux, Solaris, Mac Os, entre otros. Este tipo de IDS actúa como un “Daemon” que se ejecuta en segundo plano transparente al usuario. Generalmente el H-IDS analiza la información que se almacena en los registros del sistema y los paquetes de información que ingresan y salen del host, en busca de acciones sospechosas como ataques de denegación de servicio, troyanos, accesos no autorizados, código malicioso, entre otros.

4.5.2 Sistemas de prevención de intrusos

Un sistema de prevención de intrusiones es un dispositivo o software de seguridad encargado de monitorear y analizar actividades en las capas de red y aplicación del modelo OSI, con el propósito de identificar actividades sospechosas y reaccionar en tiempo real en caso de la materialización de un ataque informático. Los IPS son una alternativa a los sistemas firewall e IDS, por lo que muchas de sus funcionalidades son heredadas de estas dos tecnologías, complementándolas con un comportamiento más proactivo ante los ataques y amenazas informáticas. La ventaja de los sistemas de prevención de intrusiones respecto de los firewalls, radica en que toman decisiones sobre el control de acceso, basados en los flujos de tráfico, en lugar de realizarlo por medio de puertos o direcciones IP. La diferencia entre un IDS y un IPS se determina según la manera de operar, siendo reactivos o proactivos, pues los IDS alertan ante la detección de una intrusión, por el contrario, los IPS pueden establecer reglas y políticas para proteger las redes ante posibles ataques.[42]

[42] Infotecs. IPS: Sistema de Prevención de Intrusos. [En línea]. 2019. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

4.5.3 APT´s Advanced Persistent Threat

Es un tipo de ataque informático que tiene el propósito de vulnerar los sistemas de información para apoderarse de sus datos y realizar actividades de espionaje. Una de sus características principales es que se ejecuta durante largos periodos de tiempo, ya que la preparación del ataque se realiza con antelación y planificadamente, teniendo en cuenta una investigación detallada de los sistemas y equipos objetivos. Los ataques ejecutados mediante APT integran malware totalmente personalizado según el objetivo elegido.[43]

Inicialmente los APTs se relacionaban con el espionaje político y de gobiernos, actualmente este tipo de ataques se enfocan hacia el hurto de información y datos sensibles que posteriormente son vendidos o canjeados de alguna forma. Llama la atención lo rápido que se sofistican este tipo de ataques, tal vez porque son muy lucrativos, por tal razón, muchos expertos se encargan de diseñar, implementar y ejecutar los APTs por grandes sumas de dinero. Algunas de las acciones que ejecutan este tipo de ataques son el acceso a información confidencial, implantación de Blackdoors y la inserción de código malicioso.

Este tipo de ataques se caracterizan por tener mucho éxito, ya que son ejecutados por ciberdelincuentes muy profesionales y con mucha experiencia, los cuales prefieren tomarse todo el tiempo necesario para no ser detectados y no dejar rastros de las técnicas utilizadas. Otra característica importante es que desde el momento en que el ataque APT logra vulnerar un ordenador, empieza a expandirse hacia otros en cuestión de pocas horas, ya que realizan lecturas de las bases de datos y roban las credenciales de los sistemas, para iniciar sesiones en todos los demás ordenadores que van localizando. Los APT identifican y aprenden de las cuentas de usuarios y servicios que permiten altos niveles de permisos y privilegios, por lo tanto, priorizan ese tipo de usuarios y así comprometen los activos de información más importantes de la organización. Según lo anterior, existen ciertos patrones para identificar APTs, los cuales se describen a continuación:

- Un injustificado aumento en el número de registros e inicios de sesión en horas no habituales, en este caso el equipo de seguridad debe conocer cuáles son los horarios que registran altos volúmenes de inicios de sesión en los sistemas, con el propósito de identificar patrones y comportamientos sospechosos.

- Presencia de Backdoors que por lo general son del tipo troyanos, por medio de las cuales se asegura el acceso permanente en los equipos afectados y

[43] Fernández, L. Qué son los Advanced Persistent Threats y cómo protegernos de los APT. [En línea]. 2020. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/advanced-persistent-threats-apt-protegernos/

por consiguiente permiten el acceso a la organización afectada siempre que se desee.

- Flujos de información y datos mayores que lo habitual, especialmente información que tiene origen dentro de la organización o en equipos externos desconocidos.

- Circulación de datos sospechosos, lo cual puede indicar que una red o sistema puede verse afectado por un APT, ya que se generan volúmenes de información en lugares donde no se deberían generar.

- Campañas específicas de Phishing (Spear Phishing), la cuales se dirigen específicamente hacia una víctima previamente seleccionada.

4.5.4 EDR Endpoint Detection And Response

Es una herramienta que integra el monitoreo y análisis continuo en cualquier sistema informático, equipo y red de datos. Su propósito es la identificación, detección, y prevención de amenazas avanzadas persistentes (APT). Anteriormente los EDR se implementaban en grandes empresas con centros de operaciones de seguridad (SOC) dedicados, actualmente este tipo de soluciones se implementan en todo tipo de empresas sin importar su tamaño.[44]

La evolución de las tecnologías de la información ha provocado que los fabricantes de soluciones de seguridad incluyan en sus EPP (End Point Protection Plataform) funcionalidades de EDR, buscando que las empresas estén protegidas ante cualquier incidente de seguridad, proporcionando herramientas adicionales para controlar amenazas informáticas desconocidas. Este tipo de herramientas permiten realizar análisis forenses y brindan respuestas efectivas ante cualquier ataque, inclusive detectan los ataques que los antivirus convencionales han pasado por alto. Adicionalmente monitorizan y analizan todas las actividades y tráfico de la red, en busca de amenazas informáticas en tiempo real permitiendo la toma de decisiones de inmediato. Los EDR son más efectivos que los antivirus, ya que detectan malware no convencional utilizando técnicas novedosas como:

- Analítica y Aprendizaje.

- Alertas generadas por sistemas externos.

- Sandboxing.

[44] Tecnozero.¿Qué es un EDR? ¿Por qué es diferente de un antivirus?. [En línea]. 2020. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/

- Investigación y análisis de incidentes rastreando historiales

- Herramientas para eliminar elementos infectados, ponerlos en cuarentena y volver el sistema a un estado anterior a la infección.

El EDR monitorea toda la actividad de los end points y realiza la clasificación de los archivos según sean seguros o peligrosos, si se detecta un archivo sospechoso o desconocido en uno de los end points, automáticamente lo envía a cuarentena. Entre las principales características de los EDR se encuentran:

- Detección: Utilizan inteligencia artificial para mejorar la precisión de identificación y clasificación de las amenazas, optimizando los recursos del sistema.

- Contención: Permiten el bloqueo avanzado, detectando rápidamente las nuevas amenazas y bloqueando ataques en directo.

- Investigación: Permite una respuesta rápida frente a incidentes.

- Eliminación: Realiza una reparación efectiva del end point, permitiendo la restauración anterior a una eventual infección.

- Permiten una mejor anticipación a los ciberataques dirigidos analizando los patrones de comportamiento de las amenazas.

- Permiten una menor exposición a incidentes de seguridad.

- Proporciona una visión completa de las amenazas de los end points.

4.5.5 Firewall de aplicación web

Un firewall de aplicación web (WAF), es un sistema que permite la protección de las aplicaciones WEB ante ataques informáticos. Su funcionamiento es similar al de un firewall convencional de red, la diferencia radica en que el WAF se centra más en el análisis del tráfico específico y funcionalidades de una aplicación web, y no de todo el tráfico de una red de datos. Para comprender mejor el funcionamiento de un WAF es conveniente tener claro que un firewall es un dispositivo o software que filtra el tráfico de entrada y de salida de una red de datos. Los firewalls trabajan en la capa de red del modelo OSI y permiten o limitan el tráfico según las reglas y permisos previamente configurados. Según lo anterior, un firewall de aplicaciones web se puede definir como un complemento o un conjunto de reglas que analizan y filtran el tráfico web entre un cliente y el

servidor. En otras palabras, el WAF es un intermediario que permite o limita el flujo de tráfico entre la aplicación web y el servidor, sin embargo, no protege contra ataques informáticos más especializados como la explotación de vulnerabilidades web. En las organizaciones los firewalls de aplicaciones web son muy utilizados para proteger los equipos contra ataques de malware o software malicioso, garantizando que la información viaje segura por toda la red de datos.[45]

Los WAF analizan el tráfico HTTP para identificar y bloquear peticiones Cross Site Scripting XSS, ataques de inyección SQL, local file inclusión LFI, entre otros ataques. Lo anterior se logra comprobando las firmas de ataques conocidos, aunque la fortaleza de los WAF se centra en ataques de manipulación de parámetros, cookies, Javascript, cabeceras HTTP. Este tipo de firewalls son tan robustos que pueden proteger cualquier tipo de aplicación web, sin importar donde se encuentre alojada, o su lenguaje de programación, adicionalmente reaccionan antes de que los ataques afecten las aplicaciones web. Las reglas que hacen parte de la configuración del WAF son patrones que permiten el filtrado de la información en una red de datos. Una vez activas las reglas, toda la información circulante entre el cliente y servidor es analizada con base a dichas reglas, si en algún momento se encuentra una anomalía en la información, inmediatamente es bloqueada y se activan las respectivas alertas de seguridad.

4.5.6 Firewall de bases de datos

El firewall de bases de datos es un software que permite filtrar las peticiones que llegan al sistema de gestión de bases de datos (SMBD), mediante un conjunto de reglas previamente establecidas y configuradas. Adicionalmente al utilizar mecanismos de filtrado de peticiones, no solo se bloquean las transacciones malintencionadas, sino que se pueden monitorear todas las actividades y respuestas del SMBD, generando archivos Logs que almacenan todo el historial de las actividades.[46]

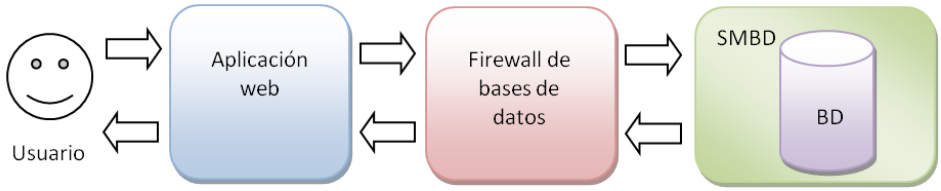
El registro e historial de las actividades es muy importante, ya que permite identificar desde donde se realizan los ataques recibidos por una base de datos, los horarios más incidentes y los tipos de ataques más concurrentes, permitiendo la generación de estadísticas por medio de las cuales se pueden identificar los comportamientos de los próximos ataques, y así tomar las medidas de seguridad necesarias. Los firewalls de bases de datos se implementan entre la aplicación

[45] UNAM. Firewall de Aplicación Web - Parte I. [En línea]. 2018. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://revista.seguridad.unam.mx/numero-16/firewall-de-aplicación-web-parte-i

[46] UNAM. Firewall de bases de datos. [En línea]. 2018. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

web y el sistema de gestión de bases de datos (SMBD), como se observa en la imagen 1.

Figura 5. Firewall para bases de datos



Fuente: https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

Cuando un atacante intenta vulnerar el sistema de gestión de bases de datos y obtener acceso a la información almacenada, el firewall de bases de datos proporciona una capa adicional de seguridad que impedirá la vulneración del sistema, permitiendo solo el paso a las peticiones de usuarios y consultas previamente autorizadas según las reglas de seguridad.

4.5.7 Gestión unificada de amenazas

la gestión unificada de amenazas UTM busca unificar las herramientas y estrategias de seguridad en una sola solución para las organizaciones, por lo general, un solo producto de seguridad informática que ofrece diferentes funcionalidades para proteger la red y sistemas de información. Una solución UTM incluye el firawall o cortafuegos, aplicaciones de antivirus, antimalware, antispam, detección y prevención de intrusiones, filtros de contenidos, entre otras. Algunas UTM también ofrecen servicios de traducción de direcciones de red, servicios de enrutamiento remoto y compatibilidad con VPN. Este tipo de soluciones se basan en la simplicidad, ya que las organizaciones pueden centralizar los productos y estrategias de seguridad en una sola solución, que se administra y monitorea desde un mismo sistema de información.[47]

4.5.8 Zona Desmilitarizada DMZ

Una zona desmilitarizada DMZ en términos de seguridad informática, se utiliza para ubicar servidores que van a ser accedidos desde afuera de las instalaciones de una organización, por lo general son servidores web, servidores de e-mail, servidores DNS, entre otros. Solo los servicios alojados en los servidores de la

[47] Cedeño Cruz, A. Y. Simulación de una gestión unificada de amenazas para administrar la red de datos de la Empresa FAINCA GROUP utilizando la tecnología OPEN SOURCE. [En línea]. 2018. [Consultado el 17 de Diciembre de 2020]. Disponible en: http://repositorio.ug.edu.ec/handle/redug/27039

DMZ podrán establecer conexiones entre la DMZ y la red local, por ejemplo, conexiones entre un servidor y una base de datos situada en la red local.[48]

Una zona desmilitarizada ubica los servidores de acceso público en segmentos independientes aislados de la red, con el propósito de impedir que los servidores estén en contacto con otros segmentos de la red. Una DMZ permite aislar los servidores que tienen acceso a la red de internet, por ejemplo, un servidor de correo, con lo cual el tráfico interno en la red no será visible por la DMZ, generando un mejor nivel de seguridad en los sistemas de una organización. Para la implementación de una DMZ es muy importante la utilización de uno o varios firewalls, que es donde se configuran las políticas de acceso y seguridad de la DMZ.[49]

[48] Batista Díaz, C. M. Lujo Aliaga, Z. Cedeño Galindo, L. V. Propuesta e implementación de la arquitectura de la red LAN en la empresa Acinox Las Tunas. [En línea]. 2018. [Consultado el 18 de Diciembre de 2020]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7107368

[49] Maridueña Carrión, N. E. LA IMPORTANCIA DE LOS IPS Y BYOD EN LAS ORGANIZACIONES: CASO DE ESTUDIOS CONFIDENCIAL S.A. [En línea]. 2017. [Consultado el 18 de Diciembre de 2020]. Disponible en: https://www.bibliotecasdelecuador.com/Record/oai:localhost:123456789-1436

4.6 MARCO LEGAL

4.6.1 Regulación de los CSIRT

Los siguientes son algunos de los lineamientos y marcos legales que regulan la conformación y funcionamiento de los CSIRT en Argentina, Uruguay y Colombia.

Los CSIRT en Argentina se rigen bajo la "Resolución de jefatura de gabinete de ministros 580/2011, la cual se refiere a la creación del programa nacional de infraestructuras críticas de información y ciberseguridad, que tiene como objetivo la elaboración de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas de las entidades, los organismos interjurisdiccionales, el sector privado y las organizaciones civiles."

En Uruguay los CSIRT se rigen bajo la "Ley 18.362 año 2008, decreto poder ejecutivo 451 año 2009, por medio del cual se crea el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), el cual faculta a regular la protección de los activos críticos de información del Estado y le encarga difundir las mejores prácticas en el tema, centralizar, coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan."

En Colombia los CSIRT se rigen bajo las normativas que regulan las tecnologías de la información y las políticas de ciberseguridad y ciberdefensa como la ley 1273 de 2009, el Conpes 3701 de 2011, el Conpes 3854 de 2016, la Ley 1928 de 2018 y la ley 1978 de 2019, normativas expedidas por gobierno nacional que se describen a continuación.

4.6.2 Ley 1273 de 2009

La ley 1273 de 2009 se refiere al marco regulatorio para la protección de la información y de los datos de los sistemas que utilizan las TICs en Colombia. Esta ley se conforma por artículos que describen delitos y prácticas indebidas para la seguridad de la información y sus respectivas sanciones, multas y condenas, las cuales se refieren a delitos relacionados con el acceso no autorizado a sistemas informáticos, interceptación de comunicaciones, uso de software malicioso, suplantación, estafa por medios digitales, entre otros.[50]

[50] Colombia, C. de la R. de. Ley 1273 de 05 Enero de 2009. [En línea]. 2009. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

4.6.3 CONPES 3701 de 2011

Este documento se refiere a los lineamientos para la ciberseguridad y ciberdefensa de Colombia, adicionalmente le asigna presupuesto al ministerio de defensa nacional para crear una estrategia orientada a mitigar las amenazas cibernéticas que afectan al país. Este documento CONPES surge de los problemas que afrontaba el estado durante el año 2010, donde la capacidad para contrarrestar las amenazas informáticas era muy limitada y evidenciaba muchas debilidades al no tener una estrategia definida al respecto. La aplicación de este lineamiento incluye recomendaciones y buenas prácticas que se deben aplicar en las organizaciones involucradas.[51]

4.6.4 CONPES 3854 de 2016

El rápido crecimiento del entorno digital genera incertidumbre y riesgos de ciberseguridad nacional que deben ser tratados. Estos riesgos podrían generar amenazas cibernéticas para los diferentes sectores económicos del país. La política de ciberseguridad y ciberdefensa Nacional se ha dedicado a contrarrestar las amenazas informáticas, pero se ha dejado por fuera la gestión del riesgo en el ecosistema digital, hecho que requiere una mayor atención, prevención y gestión por parte de los países de la región. Es por esta razón que la política nacional de seguridad digital cambia su enfoque tradicional, incluyendo la gestión del riesgo cibernético como uno de sus principios fundamentales.[52]

4.6.5 Ley 1928 del 24 de julio de 2018

Por medio de esta ley se aprueba el “convenio sobre la ciberdelincuencia” adoptado en Budapest el 23 de noviembre de 2001, firmado por los estados miembros del concejo europeo, el cual fija una política penal que busca proteger a la sociedad ante la ciberdelincuencia, a través de la definición e implementación de legislaciones adecuadas, que facultan de suficientes poderes legales a los estados para luchar contra los delitos informáticos, promoviendo la cooperación y participación de los gobiernos y el sector privado.[53]

---

[51] CONPES. CONPES 3701 de 2011. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[52] CONPES. CONPES 3854 de 2016. [En línea]. 2016. [Consultado el 17 de Octubre de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[53] Colombia, C. de la R. de. LEY 1928 DE 24 Julio 2018. [En línea]. 2018. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501

4.6.6 Ley 1978 DE 2019

La ley de modernización del sector TIC contiene 51 artículos que ofrecen la herramientas y estrategias para incentivar la inversión privada en el sector de las TICs, tiene por objeto “alinear los incentivos de los agentes y autoridades del sector de Tecnologías de la Información y las Comunicaciones (TIC), aumentar su certidumbre jurídica simplificar y modernizar el marco institucional del sector, focalizar las inversiones para el cierre efectivo de la brecha digital y potenciar la vinculación del sector privado en el desarrollo de los proyectos asociados, así como aumentar la eficiencia en el pago de las contraprestaciones y cargas económicas de los agentes del sector.”[54]

[54] Secretaría del senado. Ley 1978 de 2019. [En línea]. 2019. [Consultado el 25 de Noviembre de 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1978_2019.html

5 DISEÑO METODOLÓGICO

Para el desarrollo del proyecto aplicado se utiliza una metodología de revisión documental descriptiva, que comprende la selección, análisis e interpretación de documentos y material de consulta referente a los procesos administrativos y funcionamiento de diferentes equipos de respuesta CSIRT. La metodología tiene un componente cuantitativo, ya que uno de los objetivos específicos es la cuantificación y medición del impacto de los ataques y amenazas informáticas en Colombia, permitiendo definir la taxonomía de ataques y ámbito de actuación del CSIRT. Adicionalmente la metodología cuenta con un componente cualitativo, en el cual se realiza la indagación y análisis de las características y funcionalidades de los equipos de respuesta CSIRT, con el propósito de definir los servicios y establecer los procedimientos necesarios para la operación de un equipo de respuestas a incidentes cibernéticos.

Como técnica de recolección de información se utiliza la recopilación documental de fuentes bibliográficas como páginas web, artículos de investigación, monografías, proyectos y otros documentos, para realizar un análisis cualitativo y cuantitativo de casos de implementación de equipos de respuesta CSIRT, en organizaciones de diferentes sectores como el gubernamental, académico y empresarial. El presente proyecto aplicado se desarrolla en 3 fases, que se visualizan en la tabla 2 y se describen a continuación:

- **Revisión documental:** Inicialmente se realiza una revisión desde el enfoque cuantitativo y cualitativo para identificar y justificar la problemática del proyecto, adicionalmente se elabora el marco referencial obteniendo información importante para abordar los objetivos específicos del proyecto.

- **Diseño de la documentación del CSIRT:** Esta fase se divide en cuatro partes, donde se aborda un objetivo específico por cada una, como resultados de esta fase se obtienen la taxonomía de ataques, el panorama actual de la ciberseguridad, el catálogo de servicios y las políticas y procedimientos.

- **Conclusiones y recomendaciones:** en esta fase se plasman las conclusiones y recomendaciones por cada uno de los objetivos específicos y de del proyecto en general.

Cuadro 2. Desarrollo del proyecto aplicado

<table>
<tr><th colspan="6">Desarrollo del proyecto aplicado</th></tr>
<tr><th colspan="2">1. Revisión Documental</th><th colspan="4">2. Diseño de la documentación del CSIRT</th></tr>
<tr><td>Introducción</td><td>Marco referencial</td><td>Taxonomía de ataques y ámbito de actuación del CSIRT</td><td>Servicios proactivos y reactivos del CSIRT</td><td>Estructura orgánica y perfiles del equipo del CSIRT</td><td>Políticas y procedimientos del CSIRT</td></tr>
<tr><td>• Objetivos
• Planteamiento del problema
• Justificación</td><td>• Marco teórico
• Marco conceptual
• Marco histórico
• Antecedentes
• Marco científico
• Marco legal</td><td>• Panorama actual de la Ciberseguridad en Colombia
• Ámbito de actuación del CSIRT
• Taxonomía de ataques a partir del documento de panorama actual</td><td>• Catálogo de servicios del CSIRT</td><td>• Caracterización y manual de funciones de los perfiles del equipo de trabajo del CSIRT</td><td>• Manual de Políticas y Procedimientos Operacionales del CSIRT</td></tr>
<tr><th colspan="6">3. Conclusiones - Recomendaciones</th></tr>
</table>

Fuente. El autor

6 DESARROLLO DE LOS OBJETIVOS

6.1 TAXONOMÍA DE ATAQUES Y ÁMBITO DE ACTUACIÓN DEL CSIRT

6.1.1 Ataques informáticos en Colombia

En esta sección se presenta un cuadro descriptivo (tabla 5) con los principales ataques informáticos ocurridos en los últimos 3 años en el territorio colombiano, los cuales se han calificado según su impacto y probabilidad de ocurrencia, tomando como referencia las matrices de las tablas 3 y 4.

Cuadro 3. Matriz de probabilidad

	Nomenclatura	Categoría	Valoración
Probabilidad	PS	Prácticamente seguro	4
	PR	Probable	3
	PP	Poco Probable	2
	MR	Muy raro	1

Fuente. El autor

Cuadro 4. Matriz de impacto

	Nomenclatura	Categoría	Valoración
Impacto	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

Fuente. El autor

Cuadro 5. Principales ataques informáticos en Colombia

Ataques	Descripción	Impacto	Probabilidad
Business Email Compromise BEC	Los Ataques BEC son uno de los principales incidentes que afectan la integridad de los correos electrónicos y servicios de mensajería instantánea. Los cibercriminales engañan a los empleados de las organizaciones por medio de escenarios simulados apoyados en técnicas de phishing y spoofing, con el fin de suplantar la identidad de sus clientes y proveedores para defraudar las empresas.	A	PR
Ransomware	Este tipo de ataque no es reciente y se basa en el secuestro de información con el propósito de liberarla a cambio de dinero. Esta modalidad de ciberataque ha tenido gran concurrencia en Colombia durante los dos últimos años y está ligada al uso de criptomonedas como medio de monetización a nivel mundial.	A	PR
Ddos	Este tipo de ataque se utiliza para inhabilitar los servicios ofrecidos por un sistema de información, haciendo colapsar los recursos del servidor aprovechándose de las vulnerabilidades detectadas por los ciberdelincuentes.	A	PR

Cuadro 5. (Continuación)

Ataques	Descripción	Impacto	Probabilidad
Malware	Este tipo de ataque se utiliza para múltiples finalidades, como extraer información personal y credenciales de sistemas de información para hurtar dinero e información importante, también es utilizado para evitar el acceso a dispositivos y sistemas de información, o para aprovechar los recursos de una red por medio de bootnets.	A	PR
Swapping	Este tipo de ataque aprovecha las vulnerabilidades de las tarjetas SIM, con la ayuda de técnicas de ingeniería social, su finalidad es engañar a los proveedores de telefonía móvil y lograr que transfieran números móviles a tarjetas SIM controladas por los ciberdelincuentes.	M	PR
Cryptojacking	Este ataque aprovecha los recursos de un equipo de cómputo sin la autorización de su propietario, con el propósito de minar criptomonedas. En este caso las páginas visitadas contienen código javascript que transforman el navegador del usuario ene un criptominero de forma pasiva y silenciosa, afectando el rendimiento de los equipos sin ser detectados.	M	PR

Cuadro 5. (Continuación)

Ataques	Descripción	Impacto	Probabilidad
Ingeniería social	Alrededor del 90% de los ataques informáticos que sufren las empresas en Colombia utilizan la ingeniería social como principal medio para su ejecución. A través de diferentes estrategias que involucran a las personas, los cibercriminales obtienen información confidencial, para suplantar identidades, falsificar correos electrónicos y conseguir beneficios económicos a base de engaños a los empresarios, clientes y proveedores[55]	A	PS

Fuente. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Cuadro 6. Equipos y sistemas afectados por los ataques informáticos

Equipo / Sistema	Descripción
Equipos móviles	El acceso a internet desde dispositivos móviles como smartphones y tabletas está en constante crecimiento, por esta razón, es uno de los campos de acción preferidos por los delincuentes informáticos.
Equipos de cómputo convencionales	En la actualidad es el principal objetivo de los delincuentes informáticos, debido a su gran masificación y la facilidad de acceso no autorizado.
Equipos activos de red	El ingreso no autorizado y manipulación de los dispositivos activos de red y servidores son prácticas ilícitas que les generan grandes utilidades a los ciberdelincuentes.

[55] CCIT. Tendencias cibercrimen Colombia 2019-2020 [En línea]. 2019. [Consultado el 17 de marzo de 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Cuadro 6. (Continuación)

Equipo / Sistema	Descripción
Sistemas e infraestructura corporativa	En el 2017 los delitos informáticos afectaron a 446 empresas de todo el territorio nacional, afectando su infraestructura tecnológica.[56]
Sistemas y equipos de hogares	Son ataques dirigidos a los equipos personales de la población, por lo general utilizan cadenas de phising para apropiarse de información bancaria y datos personales.
Sistemas de autenticación	Los sistemas de autenticación son la principal puerta de entrada a los sistemas de información, por tal razón son objetivo predilecto de los ciberdelincuentes.
Tiendas de descarga de aplicaciones	Cada día existen más aplicaciones para dispositivos móviles, las cuales se distribuyen por medio de tiendas de descargas centralizadas, convirtiéndolas en un excelente objetivo para los ciberdelincuentes.
Sistemas del sector financiero	En el 2018 se denunciaron 21.687 casos de ciberdelitos de los cuales el 25% fueron dirigidos a entidades financieras. Adicionalmente los ataques contra tarjetas de crédito aumentaron un 212%
Empresas del sector gobierno	El sector gobierno es el propietario de las bases de datos personales más grandes del país, por lo tanto, es común que muchos ataques informáticos se dirijan hacia este sector.
Internet de las cosas IoT	El internet de las cosas permite la conexión de gran cantidad de dispositivos no convencionales en temas de conectividad, como electrodomésticos, accesorios, automóviles entre otros. Por tal razón en un futuro cercano serán los principales objetivos de ataques informáticos.
Servicios cloud computing	Los servicios cloud y SaaS son la tendencia mundial en temas de servicios tecnológicos para el sector empresarial, donde la seguridad es la principal carta de presentación, por tal razón muchos ataques son dirigidos hacia estas plataformas y servicios.

Fuente. https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

[56] Portafolio. El secuestro de información desangra a las empresas del país. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

6.1.2 Taxonomía de ataques del CSIRT

Tomando como base los principales ataques informáticos ocurridos en Colombia, se clasifican los reportes e incidentes atendidos por el CSIRT de la empresa Cibersecurity de Colombia LTDA, según las siguientes opciones:

- **Contenido abusivo:** Incidentes relacionados con spam que distribuyan contenidos sexuales, pederastas, que inciten a la violencia, el racismo, violación de los derechos humanos, trata de personas, actividades ilícitas, ofensas y contenidos inapropiados que afecten la moral y buenas costumbres.

- **Contenido malicioso:** Incidentes relacionados con malware como, virus, troyanos, gusanos, spyware, bootnets, inyecciones de código, ramsomware.

- **Obtención de información:** Incidentes relacionados con aplicativos de escaneos de puertos e intrusiones, uso de sniffers, exploits, ingeniería social y ataques de fuerza bruta.

- **Acceso no autorizado:** Incidentes relacionados con el acceso sin autorización y escalado de privilegios a sistemas de información, programas y aplicaciones, ataques que afectan los sistemas de autenticación y credenciales de usuarios.

- **Disponibilidad:** Incidentes relacionados con ataques de denegación de servicios, hurto y daño de infraestructura, sabotaje de servicios y aplicaciones, vandalismo, problemas de orden público.

- **Fraude:** Incidentes relacionados con el uso y acceso no autorizado, suplantaciones de identidad, estafas, derechos de autor y licencias.

- **Prevención:** Solicitudes a requerimientos técnicos, mantenimientos preventivos, capacitaciones, sensibilizaciones, asesorías y consultorías.

- **PQRS:** Solicitudes que no tienen clasificación dentro de los incidentes informáticos, pero que se relacionan con la administración, la gestión y el servicio del CSIRT.

La prioridad con la que se catalogan las solicitudes y reportes de incidentes es la siguiente:

- **Emergencia:** Incidentes cuya solución no debe dar espera, para lo cual se utilizarán todos los recursos disponibles, por lo general, son incidentes que suponen riesgo para la vida de las personas, la continuidad del negocio o temas de seguridad y defensa Nacional.

- **Alta:** Incidentes que requieren atención inmediata y aunque se hayan registrado posteriormente se mantienen en una cola de incidentes de prioridad alta, en este caso no serán atendidos incidentes de prioridad inferior hasta no solucionar los de dicha cola.

- **Media:** Incidentes que se atienden por defecto en orden de llegada, siempre y cuando no se registre un incidente de prioridad mayor. Este tipo de incidentes pueden cambiar de prioridad según sus características e impacto.

- **Baja:** Este tipo de incidentes se atienden en orden de siempre y cuando no se registre un incidente de prioridad mayor, por lo general son incidentes donde el atacante no ha conseguido su propósito, y no ha generado impactos negativos aún.

6.1.3 Ámbito de actuación del CSIRT

El CSIRT de la empresa Cibersecurity de Colombia LTDA, está dirigido a los ciudadanos en general, el sector gobierno y las PYMES de todo el territorio Colombiano, ya que los ataques informáticos ocurridos en Colombia no discriminan sectores económicos o regiones, adicionalmente, es poco probable que las pequeñas y medianas empresas cuenten con los recursos y capacidades necesarias para implementar sus propios equipos de respuesta a incidentes cibernéticos. Por lo anterior, surge la necesidad de implementar un CSIRT de ámbito nacional que preste sus servicios en tres grandes grupos organizados de la siguiente manera:

- GOB: Sector Gobierno
- CIG: Ciudadanía en General
- PYM: Sector PYMES

6.1.3.1 Ámbito de actuación sector Gobierno

El CSIRT de la empresa Cibersecurity de Colombia LTDA, tiene la capacidad para ofrecer servicios y brindar respuestas a las solicitudes e incidentes reportados por las diferentes entidades estatales del orden Nacional, para tal fin, cuenta con personal suficiente, desde especialistas en atención al cliente y profesionales en seguridad informática, entrenados para atender todo tipo de requerimientos. Con esta iniciativa el CSIRT contribuye con el fortalecimiento de la política de ciberseguridad y ciberdefensa del país.

6.1.3.2 Ámbito de actuación ciudadanía en general

Otro ámbito importante de atención para el CSIRT, es la ciudadanía en general, abarcando los computadores, dispositivos móviles y equipos IoT de los hogares, estudios de diferentes consultoras de IT, establecen que el internet de las cosas se convertirá en uno de los principales focos de riesgos y amenazas informáticas para los hogares. Según lo anterior, el CSIRT contribuye con el fortalecimiento de la ciberseguridad de las personas, generando confianza en los desarrollos tecnológicos.

6.1.3.3 Ámbito de actuación sector Pymes

En el 2019 se incrementaron los reportes de pequeñas y medianas empresas, que denunciaron incidentes y ataques informáticos que afectaron la continuidad de sus negocios, por tal razón, el sector Pyme le está dando mayor importancia a la ciberseguridad, pero una de sus limitantes es la falta de capacitación y experiencia sobre el tema, adicionalmente la inversión de grandes cantidades de recursos para implementar este tipo de equipos de respuesta, no es factible para sus metas, por lo anterior, el CSIRT de la empresa Cibersecurity de Colombia LTDA, ofrece servicios de tercerización de seguridad informática para este grupo de empresas.

6.2 SERVICIOS DEL CSIRT

6.2.1 Catálogo de servicios del CSIRT

Los servicios del CSIRT de la empresa Cibersecurity de Colombia LTDA, se diseñaron teniendo en cuenta el ámbito de actuación planteado y los principales ataques ocurridos en Colombia en los últimos 3 años. Con sus servicios el CSIRT busca contribuir en la disminución de los riesgos informáticos de las PYMES, el sector Gobierno y la ciudadanía en general. El CSIRT distribuye sus servicios en tres grandes grupos de la siguiente manera:

- SR: Servicios Reactivos
- SP: Servicios Proactivos
- SC: Servicios Complementarios

Cuadro 7. Servicios del CSIRT

Servicios del CSIRT		
Reactivos	**Proactivos**	**Complementarios**
Alertas y advertencias	Observatorio de seguridad	Capacitación
Gestión de incidentes	Auditorias de seguridad	Sensibilización
Detección de intrusiones	Test de Intrusión	Asesoría técnica y legal
Monitoreo WEB	Cuadro de mando de seguridad	Regulación y normalización
	Identificación y análisis de riesgos	Atención al cliente

Fuente. El autor

6.2.1.1 Servicios reactivos

Se activan ante la ocurrencia y reporte de un evento o incidente, como la ejecución de código malicioso, alertas de computadores, vulnerabilidades de software, o alertas emitidas por sistemas de detección de intrusiones. Los servicios reactivos son el principal campo de acción del CSIRT de la empresa Cibersecurity de Colombia LTDA.

Cuadro 8. Servicio de alertas y advertencias

Servicio: Alertas y advertencias	
Tipo	SR
Sector que atiende	GOB, CIU, PYM
Descripción	Servicio que genera alertas y advertencias automáticas en tiempo real sobre amenazas y ataques ocurridos en los sistemas de información. Su objetivo es detectar y registrar en el menor tiempo posible los incidentes en el CSIRT.
Prioridades	Emergencia, Alta, Media, Baja
Código de servicio	SR01

Fuente. El autor

Cuadro 9. Servicio de gestión de incidentes

Servicio: Gestión de incidentes	
Tipo	SR
Sector que atiende	GOB, CIU, PYM
Descripción	Servicios de gestión, análisis y respuesta a los diferentes ataques que sufren los sistemas informáticos.
Prioridades	Emergencia, Alta, Media, Baja
Código de servicio	SR02

Fuente. El autor

Cuadro 10. Servicio de detección de intrusiones

Servicio: Detección de intrusiones	
Tipo	SR
Sector que atiende	GOB, PYM
Descripción	Servicios de control y detección de accesos sin autorización a los sistemas de información, equipos de cómputo e infraestructura de red.
Prioridades	Emergencia, Alta, Media, Baja
Código de servicio	SR03

Fuente. El autor

Cuadro 11. Servicio de monitoreo web

Servicio: Monitoreo web	
Tipo	SR
Sector que atiende	GOB, PYM
Descripción	Servicio de monitorización en tiempo real de páginas y sitios WEB, que tiene el propósito de identificar y alertar a tiempo posibles ataques e incidentes informáticos.
Prioridades	Emergencia, Alta, Media, Baja
Código de servicio	SR04

Fuente. El autor

6.2.1.2 Servicios proactivos

Servicios que brindan asistencia y soporte para prevenir y proteger los sistemas de información de los sectores del ámbito de actuación, con el propósito de anticiparse a los posibles ataques, problemas o incidentes. Los servicios proactivos son de gran importancia ya que influyen positivamente en la cantidad de solicitudes y peticiones futuras del CSIRT.

Cuadro 12. Servicio de observatorio de seguridad

Servicio: Observatorio de seguridad	
Tipo	SP
Sector que atiende	GOB, CIU, PYM
Descripción	Informes y alertas, publicación de información
Prioridades	Alta, Media, Baja
Código de servicio	SP01

Fuente. El autor

Cuadro 13. Servicio de auditorías de seguridad

Servicio: Auditorias de seguridad	
Tipo	SP
Sector que atiende	GOB, PYM
Descripción	Servicio de auditoría interna y externa a sistemas de gestión de seguridad de la información, que tiene el propósito de diagnosticar el estado actual y madurez de la seguridad en las organizaciones.
Prioridades	Alta, Media, Baja
Código de servicio	SP02

Fuente. El autor

Cuadro 14. Servicio de test de intrusiones

Servicio: Test de intrusión	
Tipo	SP
Sector que atiende	GOB, PYM
Descripción	Servicios de pruebas de penetración a sistemas informáticos y redes de datos, con el propósito de identificar las vulnerabilidades y falencias de en seguridad informática de las organizaciones.
Prioridades	Alta, Media, Baja
Código de servicio	SP03

Fuente. El autor

Cuadro 15. Servicio de cuadro de mando de seguridad

Servicio: Cuadro de mando de seguridad	
Tipo	SP
Sector que atiende	GOB
Descripción	Servicios de medición del desempeño de las organizaciones en temas de seguridad de la información.
Prioridades	Alta, Media, Baja
Código de servicio	SP04

Fuente. El autor

Cuadro 16. Servicio de análisis de riesgos

Servicio: Gestión de riesgos	
Tipo	SP
Sector que atiende	GOB
Descripción	Servicios de Identificación, análisis y tratamiento de los riesgos informáticos de las organizaciones.
Prioridades	Alta, Media, Baja
Código de servicio	SP05

Fuente. El autor

6.2.1.3 Servicios complementarios

Complementa los servicios reactivos y proactivos del CSIRT y son independientes de la gestión de incidentes, por lo general son servicios con niveles de prioridad media y baja, ya que atienden incidentes que no ponen en riesgo la vida de las personas o la seguridad nacional. Estos servicios también contribuyen en la reducción de la cantidad de solicitudes e incidentes registrados en el CSIRT.

Cuadro 17. Servicio de capacitación

Servicio: Capacitación	
Tipo	SC
Sector que atiende	GOB, PYM, CIG
Descripción	Servicios de capacitación orientados a grupos de personal del área de informática de las organizaciones, en temas relacionados con la gestión de riesgos informáticos, planes de recuperación ante desastres, auditorías internas.
Prioridades	Media, Baja
Código de servicio	SC01

Fuente. El autor

Cuadro 18. Servicio de sensibilización

Servicio: Sensibilización	
Tipo	SC
Sector que atiende	GOB, PYM, CIG
Descripción	Servicios de sensibilización para organizaciones y personas en temas relacionados con la seguridad de las TICs.
Prioridades	Media, Baja
Código de servicio	SC02

Fuente. El autor

Cuadro 19. Servicio de asesoría técnica y legal

Servicio: Asesoría técnica y legal	
Tipo	SC
Sector que atiende	GOB, PYM
Descripción	Servicios de asesoría en temas de regulación y normativas vigentes relacionadas con la seguridad de la información.
Prioridades	Media, Baja
Código de servicio	SC03

Fuente. El autor

Cuadro 20. Servicio de regulación y normalización

Servicio: Regulación y normalización	
Tipo	SC
Sector que atiende	GOB, PYM, CIG
Descripción	Servicios de consultoría y definición de políticas de seguridad de la información y lineamientos para las empresas y el sector gobierno.
Prioridades	Media, Baja
Código de servicio	SC04

Fuente. El autor

Cuadro 21. Servicio de atención al cliente

Servicio: Atención al cliente	
Tipo	SC
Sector que atiende	GOB
Descripción	Servicios de atención de peticiones, quejas y reclamaciones relacionadas con la operación del CSIRT
Prioridades	Media, Baja
Código de servicio	SC05

Fuente. El autor

6.3 ESTRUCTURA ORGÁNICA Y PERFILES DEL EQUIPO DEL CSIRT

6.3.1 Estructura orgánica del CSIRT

La estructura orgánica de un CSIRT depende directamente de la estructura de la organización y al ámbito al que pertenece, también depende de la disponibilidad de los expertos para cubrir necesidades puntuales y de la capacidad financiera del proyecto. El CSIRT para la empresa CIBERSECURITY DE COLOMBIA LTDA se conforma por los siguientes departamentos y dependencias:[57]

Dirección: La dirección del CSIRT define los lineamientos de la organización y se encarga de la planeación estratégica. Entre sus funciones también establece alianzas de cooperación con otras organizaciones de ciberseguridad. Dentro de la dirección se encuentran las siguientes dependencias:

- Coordinación: Se encarga de desarrollar y supervisar estrategias que permitan el desarrollo normal del CSIRT y el cumplimiento de los objetivos estratégicos de la organización, adicionalmente se encarga de velar por el cumplimiento de las políticas y lineamientos impartidos por la dirección en cada una de las dependencias.

- Auditoría: Se encarga del diagnóstico y supervisión de los sistemas de gestión del CSIRT, con el propósito de obtener información que permita la

[57] ENSIA. CSIRT Setting up Guide in Spanish — ENISA. [En línea]. 2006. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish

toma de decisiones acertadas y la mejora continua de los sistemas de gestión.

- Consultoría: Brinda asesoría especializada a la dirección del CSIRT, con el fin de encontrar soluciones a los problemas y necesidades del equipo de respuestas, sustentándose en la experiencia, habilidades y conocimientos de los consultores.

- Gestión financiera: Dependencia que se ocupa de la gestión de los gastos, rentabilidad, el efectivo y crédito, con el fin de que el CSIRT cuente con los suficientes recursos en todo momento para llevar a cabo su objetivo de una manera satisfactoria.

Operación: El departamento de operaciones es donde se realiza la gestión, el monitoreo y el análisis de las solicitudes e incidentes reportados. Dentro del departamento de operación se encuentran las siguientes dependencias:

- Gestión de solicitudes e incidentes: Define el proceso de solicitudes y respuesta de incidentes de seguridad, con el objetivo de recuperar el funcionamiento de los servicios y minimizar el impacto en el CSIRT y sus clientes, manteniendo unos niveles adecuados de disponibilidad y calidad del servicio.

- Operaciones de seguridad: Esta dependencia garantiza la seguridad de la información, se encarga de supervisar, prevenir y administrar la seguridad de las redes y sistemas informáticos del CSIRT y sus clientes. sus funciones van desde el monitoreo y diagnóstico de vulnerabilidades, respuesta oportuna a incidentes, neutralización de ataques, administración de riesgos, alertas y recuperación ante desastres.[58]

Tecnología: El departamento de tecnología administra todos los servicios, aplicaciones e infraestructura tecnológica del CSIRT, como la red de datos y sus equipos, los servicios de correo electrónico, gestión de tickets, conectividad, seguridad, entre otros. Dentro del departamento de tecnología se encuentra la gestión de servicios e infraestructura tecnológica.

[58] Oracle. ¿Qué es un SOC? [En línea]. 2021. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

- Gestión de servicios e infraestructura tecnológica: Esta dependencia se encarga de alinear los servicios de tecnologías de la información con los objetivos y necesidades del CSIRT, se encarga de ejecutar una adecuada gestión de la calidad, reducir los riesgos asociados a los servicios TI, aumentar la eficiencia y alinear los procesos del negocio con la infraestructura TI.

Investigación y desarrollo: Este departamento se encarga del desarrollo de herramientas y nuevas tecnologías en el ámbito de la ciberseguridad, adicionalmente se encarga de diseñar los planes de capacitación y realizar investigaciones sobre nuevas tendencias y amenazas informáticas. El departamento de I+D estará en mayor medida a cargo de la planificación, capacitación y desarrollo de las soluciones tecnológicas necesarias en el CSIRT. Dentro del departamento de I+D se encuentran las siguientes dependencias:

- Observatorio tecnológico: Es un espacio donde se gestionan las fuentes de conocimiento, transformándolas en información útil, para ser compartida tanto interna como externamente y fortalecer la toma de decisiones estratégicas del CSIRT. Adicionalmente se encarga de diseñar los programas de capacitación para los colaboradores y los clientes del CSIRT.

- Laboratorio de informática forense: Se encarga de la adquisición, preservación y análisis de datos e información que ha sido procesada electrónicamente y que ha sido transportada por una red de comunicaciones o almacenada en un medio computacional. El laboratorio utiliza equipos informáticos y buenas prácticas que permiten catalogar la información obtenida como evidencia válida en un proceso legal o una investigación.

- Desarrollo de sistemas y aplicaciones: Esta dependencia se encarga de la planeación, diseño, implementación, evaluación y mantenimiento de proyectos de desarrollo de sistemas de seguridad para las dependencias y clientes del CSIRT, adicionalmente realiza pruebas de calidad y seguridad de nuevos sistemas informáticos antes de sus lanzamientos.

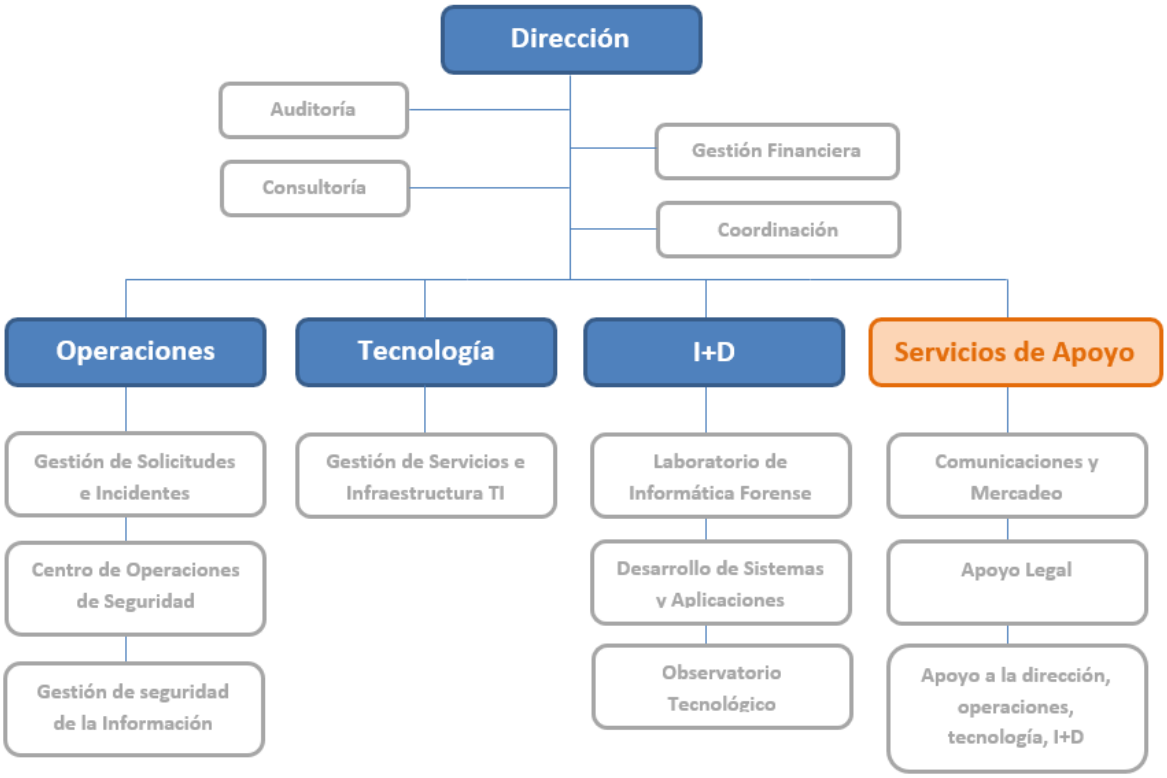
Servicios de apoyo: Este departamento se encarga de prestar apoyo en temas de gestión de comunicaciones, consideraciones legales, gestión financiera y las demás actividades que necesiten de apoyo. Dentro del departamento de servicios de apoyo se encuentran las siguientes dependencias:

- Comunicaciones y mercadeo: Esta dependencia se encarga de la gestión de las comunicaciones internas y externas del CSIRT, mantiene a todos los departamentos y dependencias comunicados para mejorar la coordinación entre los equipos de trabajo, adicionalmente establece los lineamientos y el marco de los contenidos a comunicar, asegurando que los mensajes sean coherentes y entendibles por el público objetivo.

- Apoyo legal: Esta dependencia se encarga de brindar apoyo legal a todos los departamentos y dependencias del CSIRT, interviniendo en los procesos y proyectos que requieran relaciones contractuales con otras personas jurídicas como proveedores, clientes, organizaciones y equipos de respuesta, con el fin de revisar que todo se realice dentro de los marcos y regulaciones del sector.

- Apoyo a la dirección, operaciones, tecnología, I+D: Dependencia encargada de suministrar el apoyo necesario a las demás dependencias y departamentos del CSIRT, está conformada por personal con experiencia y conocimientos en la gestión de procesos necesarios para el funcionamiento de equipos de respuesta CSIRT.

Figura 6. Organigrama CSIRT Cibersecurity de Colombia



Fuente. El autor

6.3.2 Equipo de trabajo del CSIRT

Una vez descritos los servicios que serán prestados por el CSIRT y de haber definido el modelo organizacional del CSIRT, es importante definir el número adecuado de colaboradores calificados que prestaran su apoyo para atender la operación del equipo de respuestas. Por lo general el número de colaboradores depende del ámbito de actuación y el área que pretende abarcar el CSIRT. teniendo en cuenta las buenas prácticas para establecer un CSIRT Nacional recomendadas por la Organización de los Estados Americanos[59], se establece la siguiente estructura de talento humano mínima para las operaciones del CSIRT, que puede crecer con el tiempo según sea necesario:

[59] Organización de los Estados Americanos. Buenas prácticas para establecer un CSIRT nacional. [En línea]. 2016. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Cuadro 22. Personal requerido para las operaciones del CSIRT

Departamento	**Dependencias**	**Personal**
Dirección (1 Director)	Auditoría	1 Auditor
	Consultoría	1 Asesor
	Gestión financiera	1 Contador
	Coordinación	1 Coordinador
Operaciones (1 Líder)	Gestión de solicitudes e incidentes	2 Especialistas en gestión de incidentes
	Centro de operaciones de seguridad	2 Especialistas en ciberseguridad
	Gestión de seguridad de la información	1 Especialista en seguridad de la información
Tecnología (1 Líder)	Gestión de servicios e infraestructura	1 Especialista en servicios e infraestructura TI
Investigación y desarrollo (1 Líder)	Laboratorio de informática forense	2 Especialistas en informática forense
	Desarrollo de sistemas y aplicaciones	2 Especialistas en desarrollo de software
	Observatorio tecnológico	1 Especialista en vigilancia tecnológica
Servicios de Apoyo (1 Líder)	Comunicaciones y mercadeo	1 Especialista en comunicaciones y mercadeo
	Apoyo Legal	1 Abogado
	Apoyo a los departamentos y dependencias	2 Especialistas en administración de CSIRT

Fuente. El autor

6.3.3 Perfiles del equipo de trabajo del CSIRT

Es importante detallar las áreas de conocimiento, habilidades y la experiencia necesaria que deben tener los trabajadores potenciales para ser parte de los departamentos y dependencias del CSIRT. Contratar el personal calificado es uno de los procesos más importantes y difíciles de establecer, ya que una buena definición de los perfiles requeridos es fundamental para garantizar el éxito en los procesos de contratación de personal. A continuación se describen los

requerimientos en cuanto a formación y experiencia de los potenciales trabajadores del CSIRT.[60]

Cuadro 23. Perfiles de trabajo del Departamento de Dirección

Departamento de Dirección	
Los colaboradores pertenecientes al departamento de dirección deben tener experiencia en liderazgo de grandes grupos de personal, adicionalmente deben contar con los suficientes conocimientos técnicos según su área dentro del CSIRT.	
Cargo: Director	
Formación	• Título universitario en áreas de TI • Postgrado en Gerencia de proyectos de tecnología • Certificación en gestión de proyectos PMI
Experiencia	• Siete años de experiencia en gerencia de proyectos de TI • Tres años de experiencia en áreas técnicas de seguridad de la información • Gestión de riesgos • Sistemas de gestión de seguridad de la información
Cargo: Auditor	
Formación	• Título universitario en áreas de TI • Certificación de auditor líder en iso 27001
Experiencia	• Cinco años de Experiencia en Auditoría de sistemas de gestión de seguridad de la información
Cargo: Asesor	
Formación	• Título universitario en áreas de TI • Postgrado en Gerencia de proyectos • Certificaciones en seguridad informática (CEH, CCSP, CISSP)
Experiencia	• Cinco años de experiencia en gestión de proyectos de tecnología • Tres años de experiencia en áreas técnicas de seguridad de la información
Cargo: Contador	
Formación	• Título universitario en contaduría pública • Especialista en gestión financiera
Experiencia	• Cinco años de experiencia en gestión financiera de empresas de tecnología

[60] Organización de los Estados Americanos. Buenas prácticas para establecer un CSIRT nacional. [En línea]. 2016. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Cuadro 23. (Continuación)

Cargo: Coordinador	
Formación	• Título universitario en áreas de TI • Postgrado en Gerencia de proyectos • Certificaciones en seguridad informática (CEH, CCSP, CISSP)
Experiencia	• Cinco años de experiencia en gestión de proyectos de tecnología • Tres años de experiencia en áreas técnicas de seguridad de la información

Fuente. El autor

Cuadro 24. Perfiles de trabajo del Departamento de Operaciones

Departamento de Operaciones	
Para el personal de las áreas de operaciones se requiere eficiencia, organización, dinamismo, adaptación al cambio y trabajo en equipo bajo presión.	
Cargo: Líder de Operaciones	
Formación	• Título universitario en áreas de TI • Postgrado en Gerencia de proyectos de Tecnología • Certificaciones en seguridad informática (CEH, CCSP, CISSP)
Experiencia	• Cinco años de experiencia en áreas técnicas de seguridad de la información • Gestión de incidentes y mesa de servicio • Gestión de proyectos • Administración de sistemas, y ciclo de vida de los servicios de TI bajo el estándar ITIL
Cargo: Especialista en gestión de incidentes	
Formación	• Título universitario en áreas de TI • Especialista en Seguridad Informática
Experiencia	• Tres años de experiencia en áreas técnicas de seguridad de la información • Atención y gestión de incidentes en proyectos de mesa de servicios y soporte técnico.
Cargo: Especialista en ciberseguridad	
Formación	• Título universitario en áreas de TI • Especialista en Seguridad Informática
Experiencia	• Tres años de experiencia en áreas técnicas de seguridad informática • Seguridad de centros de operaciones de red

Cuadro 24. (Continuación)

Cargo: Especialista en seguridad de la información	
Formación	• Título universitario en áreas de TI • Especialista en Seguridad de la información
Experiencia	• Tres años de experiencia en áreas técnicas de seguridad de la información • Experiencia en el diseño e implementación de sistemas de gestión de seguridad de la información

Fuente. El autor

Cuadro 25. Perfiles de trabajo del Departamento de I + D

Departamento de Investigación y Desarrollo	
El personal de Investigación y desarrollo se centra en el análisis de sistemas de información e investigación de las tendencias de ataques y vulnerabilidades para la seguridad de la información. Los especialistas de I+D deben tener conocimientos en diferentes lenguajes de programación y conocer diferentes técnicas de intrusión y ethical hacking.	
Cargo: Líder de investigación y desarrollo	
Formación	• Título universitario en áreas de TI • Especialista en programación y desarrollo de sistemas de información • Certificación Scrum Master • Conocimientos y manejo de lenguajes de programación como Python, PHP, C++, Java • Cursos en informática forense y otras áreas de la seguridad Informática.
Experiencia	• Cinco años de experiencia en áreas técnicas de seguridad de la información • Desarrollo y gestión de proyectos de TI • Investigación y desarrollo. • Metodologías agiles de desarrollo de software • Sistemas criptográficos
Cargo: Especialista en informática forense	
Formación	• Título universitario en áreas de TI • Especialización en informática forense
Experiencia	• Tres años de experiencia técnica en laboratorios de informática forense

Cuadro 25. (Continuación)

Cargo: Especialista en desarrollo de software	
Formación	• Título universitario en áreas de TI • Especialista en programación y desarrollo de sistemas de información • Conocimientos y manejo de lenguajes de programación como Python, PHP, C++, Java
Experiencia	• Tres años de experiencia en desarrollo de software, sistemas de información y aplicaciones. • Desarrollo de proyectos de software con metodología ágiles
Cargo: Especialista en vigilancia tecnológica	
Formación	• Título universitario en áreas de TI • Posgrado en gestión de proyectos
Experiencia	• Tres años de experiencia en proyectos de investigación

Fuente. El autor

Cuadro 26. Perfiles de trabajo del Departamento de TI

Departamento de Tecnologías de la Información	
El personal del departamento de Tecnología debe tener experiencia y conocimientos en gestión, operación y mantenimiento de la infraestructura y servicios de tecnologías de la información, mesa de servicios, seguridad de la información.	
Cargo: Líder de Tecnología	
Formación	• Título universitario en áreas de TI • Posgrado en gestión de proyectos de tecnología • Certificación en ITIL foundation V4
Experiencia	• Cinco años de experiencia en áreas técnicas de seguridad de la información y administración de sistemas • Gestión de proyectos de tecnología • Gestión bajo el estándar ITIL • Gestión de infraestructura y servicios tecnológicos • Diseño de arquitecturas tecnológicas
Cargo: Especialista en servicios e infraestructura TI	
Formación	• Título universitario en áreas de TI • Certificación en ITIL foundation V4
Experiencia	• Tres años de experiencia en administración de infraestructura y servicios tecnológicos • Gestión de servicios tecnológicos bajo el estándar ITIL

Fuente. El autor

Cuadro 27. Perfiles de trabajo del Departamento de Servicios de Apoyo

Departamento de Servicios de Apoyo	
El personal del departamento de servicios de apoyo debe tener habilidades en, adaptación al cambio, comunicación asertiva, dinamismo, y trabajo en equipo bajo presión.	
Cargo: Líder de Servicios de Apoyo	
Formación	• Título universitario en áreas de TI o administración • Posgrado en gestión de proyectos • Especialista en seguridad de la información • Certificación Auditor interno ISO 27001
Experiencia	• Cinco años de experiencia en gestión de proyectos de tecnología • Experiencia en gestión de sistemas de seguridad de la información • Gestión de servicios de TI bajo el estándar ITIL • Gestión de proyectos de tecnología • Gestión de proyectos de software con metodologías ágiles
Cargo: Especialista en comunicaciones y mercadeo	
Formación	• Título universitario en comunicación social • Especialista en comunicaciones corporativas • Especialista en publicidad y mercadeo
Experiencia	• Cinco años de experiencia liderando proyectos de comunicaciones corporativas • Experiencia en publicidad y mercadeo
Cargo: Abogado	
Formación	• Título universitario de abogado • Especialista en derecho laboral
Experiencia	• Tres años de experiencia en procesos de asesoría jurídica para empresas de tecnología • Contratación pública y privada • Derecho laboral
Cargo: Especialista en administración de CSIRT	
Formación	• Título universitario en áreas de TI • Postgrado en Gerencia de proyectos de Tecnología • Certificaciones en seguridad de la información • Certificación en Itil Foundation V4

Cuadro 27. (Continuación)

Cargo: Especialista en administración de CSIRT	
Experiencia	• Tres años de experiencia en áreas técnicas de seguridad de la información • Gestión de incidentes y mesa de servicio • Administración de sistemas, y ciclo de vida de los servicios de TI bajo el estándar ITIL • Gestión de proyectos de tecnología • Gestión de proyectos de software con metodologías ágiles

Fuente. El autor

6.4 POLÍTICAS Y PROCEDIMIENTOS OPERACIONALES DEL CSIRT

Las políticas de un equipo de respuestas a incidentes cibernéticos son fundamentales para su buen funcionamiento, ya que contienen las directrices que deben seguir el personal y las diferentes dependencias del CSIRT, lo anterior, garantiza la integridad, disponibilidad y confidencialidad de los activos de información de la organización y sus los clientes. Adicionalmente las políticas del CSIRT sirven de guía para el cumplimiento de las metas y los objetivos planteados en los planes estratégicos de la empresa. A continuación, se plantean las políticas recomendables para el normal funcionamiento del CSIRT.[61]

6.4.1 Política de clasificación de información[62]

1. Objetivo: Clasificar todos los activos de información para garantizar su adecuada gestión, teniendo en cuenta parámetros de confidencialidad, integridad y disponibilidad.

2. Alcance: Esta política es aplicable a los activos de información de los procesos incluidos en el sistema de gestión de seguridad de la información adoptado por la empresa.

[61] Organización de los Estados Americanos. Buenas prácticas para establecer un CSIRT nacional. [En línea]. 2016. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[62] MINTIC. Guía para la Gestión y Clasificación de Activos de Información. [En línea]. 2016. [Consultado el 14 de Febrero de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

3. Roles y responsabilidades:

- Administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y los líderes de los demás departamentos del CSIRT.

- Propietario de la información: Es una parte designada por la empresa, como un cargo, equipo de trabajo o proceso, que es responsable de garantizar la correcta clasificación de la información y sus activos relacionados.

- Custodio: Es una parte designada por la empresa, como un cargo, equipo de trabajo o proceso, encargado de administrar el cumplimiento de los controles de seguridad definidos por los propietarios de la información.

- Usuario: Puede ser una persona, entidad, cargo o equipo de trabajo que obtenga, almacene, transforme o utilice información física o digital, para propósitos de su labor utilizando las herramientas otorgadas por la empresa.

4. Disposiciones:

a) Inventario de la información: Es importante realizar un inventario de todos los activos de información con los que dispone la empresa, registrando información del activo como el tipo, ubicación, servicios, responsable, estado.

b) Clasificación de la información: Se deben definir los criterios de clasificación para los activos de información, algunos criterios pueden ser:

Por su accesibilidad o confidencialidad:

- Confidencial
- Reservado
- Público

Por su finalidad:

- información para clientes
- información para proveedores
- información financiera
- información de personal
- información de inventarios

Por su impacto ante un incidente:

- Repercusiones legales
- Repercusiones económicas
- paralización de procesos

c) Etiquetado de la información: Se debe diseñar e implementar un procedimiento adecuado para el etiquetado de la información, tomando como referencia los criterios de clasificación definidos por la empresa.

d) Información básica: Hace referencia a las características del activo de información, que debe incluir como mínimo:

- Identificador: Número único que identifica al activo dentro del inventario.
- Proceso: Nombre del proceso al que pertenece el activo de información.
- Nombre Activo: Nombre del activo de información dentro del proceso al que pertenece.
- Descripción: Contiene la descripción de los activos para que se puedan identificar fácilmente.
- Ubicación: Contiene la ubicación física y electrónica del activo de información.
- Criticidad: Cálculo que determina la valoración del activo de información, tomando como referencia la clasificación de la Información.

e) Uso aceptable de la información: Se debe identificar, documentar e implementar procedimientos y reglas para el uso adecuado de la información, incluyendo los activos asociados al almacenamiento y procesamiento.

f) Auditorías: Se deben realizar auditorías de seguridad periódicamente, con el propósito de certificar que los tratamientos y controles se están ejecutando.

6.4.2 Política de protección de datos[63]

1. Objetivo: Definir los lineamientos generales para el tratamiento y protección de datos personales.

2. Alcance: esta política es aplicable a los datos registrados en los sistemas de información y bases de datos de propiedad de la empresa.

3. Roles y responsabilidades:

- Administrador de la política: Esta Política será administrada por un representante de la Dirección General y los líderes de los demás departamentos del CSIRT.

- Líder de Departamento: Los líderes de departamento serán los responsables de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal de la empresa.

- Titular de la información: Los proveedores, asesores y cualquier persona que interactúe con los sistemas de información de la empresa, quedarán sujetos a esta Política.

4. Disposiciones:

a) Principios: La información recibida, almacenada, procesada y transmitida por la empresa será tratada bajo los siguientes principios.

- Confidencialidad: El tratamiento de la información empresarial debe cumplir lineamientos de seguridad de la información que permitan prevenir la divulgación no autorizada de esta.

- Integridad: La información almacenada y procesada por los sistemas de información de la empresa, se debe conservar exacta evitando su modificación o alteración.

[63] Agencia Nacional de Tierras. Lineamientos de seguridad de la información, tratamiento y protección de datos personales. [En línea]. 2017. [Consultado el 14 de Febrero de 2021]. Disponible en: https://www.agenciadetierras.gov.co/wp-content/uploads/2018/04/INTI-Politica-008-LINEAMIENTOS-DE-SEGURIDAD-DE-LA-INFORMACION-TRATAMIENTO-Y-PROTECCION-DE-DATOS-PERSONALES.pdf

- Disponibilidad: Se debe garantizar que la información se encuentre disponible en todo momento, teniendo en cuenta las excepciones y autorizaciones de acceso a la misma.

b) Finalidad de los Datos: La empresa es responsable del tratamiento y protección de los datos personales registrados y almacenados en sus sistemas de información, y podrá hacer uso de estos únicamente para las finalidades que se presentan a continuación:

- Para fines de gestión y administración de la empresa.

- Caracterizar la población para diseñar estrategias que mejoren los tramites y servicios prestados.

- Responder las PQRS presentados.

- Consultar la información personal de los titulares que repose en las bases de datos de la empresa.

- Diseñar y ejecutar encuestas de satisfacción de usuarios.

- Enviar mensajes con contenidos e información relevante sobre los servicios de la empresa.

c) Derechos de los Titulares: La empresa garantiza a los titulares de información los siguientes derechos:

- Conocer, rectificar, actualizar, suprimir y desautorizar la utilización de su información personal.

- Solicitar pruebas sobre la autorización respecto al tratamiento y protección de datos.

- Ser informado sobre el correcto uso y tratamiento de sus datos personales.

- Presentar quejas ante la autoridad competente relacionadas con infracciones a lo dispuesto en la ley de protección de datos personales.

- Acceder gratuitamente a su información personal que haya sido objeto de tratamiento.

d) La empresa garantiza a los titulares el derecho al acceso a sus datos personales registrados en los sistemas de información de la empresa, derecho

que se hace efectivo mediante petición por medio de los canales dispuestos por la empresa.

e) La empresa podrá recopilar, actualizar y rectificar la información de los usuarios que utilicen los sistemas de información y solicitar de manera libre y voluntaria la autorización de tratamiento de datos personales.

f) Datos Personales Sensibles: Es posible que durante la operación de la empresa se obtengan datos personales sensibles, los cuales serán suministrados voluntariamente por sus titulares y su tratamiento se efectuará según la finalidad establecida en esta política.

g) Supresión de Datos: Los titulares de la información personal en cualquier momento pueden solicitar la supresión de los datos que consideren que no estén recibiendo un trato adecuado, o que no sean pertinentes para la finalidad de su recolección.

6.4.3 Política de retención de información[64]

1. Objetivo: Establecer los lineamientos para la conservación y retención de información necesaria para las operaciones del negocio y para el cumplimiento regulatorio.

2. Alcance: Esta Política es aplicable a todos los departamentos y dependencias de la empresa y a todo su personal, no es aplicable a los activos de información de naturaleza personal o que no estén relacionados con el negocio, la información personal no podrá almacenarse en medios de propiedad de la empresa.

3. Roles y responsabilidades:

- Administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y los líderes de los demás departamentos del CSIRT.

- Líder de departamento: Los líderes de departamento serán los responsables de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

[64] CEMEX. Política de Retención de Información de CEMEX. [En línea]. 2009. [Consultado el 20 de Febrero de 2021]. Disponible en: https://www.cemex.com/documents/20143/160085/politica-retencion-informacion.pdf/b2bac2e3-efc8-8f5a-9a5c-fd2679938af4

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal de la empresa.

- Terceros: Los proveedores, asesores y cualquier persona con acceso a los equipos y sistemas informáticos de la empresa, quedarán sujetos a esta Política.

4. Disposiciones:

a) Los documentos e información se deben conservar según los requerimientos de cada proyecto y la operación de las dependencias del CSIRT, los activos de información dispuestos a retención deben ser los estrictamente necesarios para desarrollar los proyectos y permitir la operación de la empresa.

b) Las diferentes dependencias del negocio son responsables de organizar la información para que pueda ser encontrada y accedida posteriormente.

c) Los documentos e información de la operación del negocio y proyectos de la empresa tendrán un periodo de conservación definido, que debe ser aprobado por el equipo administrador de la política de retención de información. Los periodos de retención no podrán superar los 5 años, salvo autorización del equipo administrador de esta política.

d) La información de los proyectos y de la operación del negocio deberá ser revisada cada año, con el propósito de identificar la información que debe ser eliminada a razón de que ya no sea objeto de retención.

e) Toda la información generada en la operación del negocio que no sea objeto de retención debe destruiste de forma segura en un periodo no superior a 30 días.

f) Las versiones preliminares y borradores de la información electrónica deberán conservarse o eliminarse, teniendo en cuenta los mismos procedimientos establecidos para los demás tipos de información.

g) Cada dependencia de la empresa es responsable de cumplir los procedimientos apropiados para la conservación y eliminación de documentos e información.

h) La información electrónica se puede almacenar en diferentes ubicaciones, tales como equipos de cómputo, servidores, discos externos. Cualquier medio de almacenamiento debe permanecer dentro de las instalaciones de la empresa, salvo autorización del equipo administrador de esta política.

6.4.4 Política de destrucción de información[65]

1. Objetivo: El objetivo es definir normas y lineamientos para el borrado seguro de la información y para la destrucción de soportes según las necesidades de la organización

2. Alcance: Esta Política es aplicable a todos los departamentos y dependencias de la empresa y a todo su personal, no es aplicable a los activos de información de naturaleza personal o que no estén relacionados con el negocio, la información personal no podrá almacenarse en medios de propiedad de la empresa.

3. Roles y responsabilidades:

- Administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y los líderes de los demás departamentos del CSIRT.

- Líder de departamento: Los líderes de departamento serán los responsables de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal de la empresa.

4. Disposiciones:

a) Inventario de activos de información: Se debe realizar un seguimiento de los activos de información que están vigentes, conocer sus responsables y la información contenida en ellos, adicionalmente clasificarlos según su criticidad.

b) Gestión de soportes: Es importante supervisar todos los equipos que almacenan información organizacional, especialmente los utilizados para realizar respaldos de información, documentando cualquier actividad realizada sobre estos equipos (mantenimientos preventivos, correctivos, sustituciones).

[65] PCI Hispano. Eliminación destrucción segura de datos y medios de almacenamiento. [En línea]. 2014. [Consultado el 14 de Febrero de 2021]. Disponible en: https://www.pcihispano.com/eliminaciondestruccion-segura-de-datos-y-pci-dss/

c) Eliminación de la información:

- Para soportes magnéticos y no electrónicos como Impresiones, CD, DVD, cintas magnéticas de debe utilizar el triturado como medio seguro de eliminación.

- Para la reutilización de soportes electrónicos se debe utilizar la opción de sobreescritura.

- Antes de desechar un soporte de almacenamiento, se debe tener en cuenta la desmagnetización o destrucción física.

- Tener en cuenta los dispositivos móviles como smartphones y tabletas ya que también son equipos que pueden almacenar información organizacional.

d) Documentación de las operaciones: Se deben utilizar herramientas de borrado seguro que permitan la generación de documentos, que evidencien los procesos de borrado realizados, detallando su información relevante.

e) Destrucción certificada: Revisar la posibilidad de contratar los servicios de empresas especializadas, las cuales llevarían a cabo todo el proceso de eliminación de información y destrucción de los soportes, emitiendo certificados que garantizan la validez de todo el proceso.

6.4.5 Política de divulgación de información[66]

1. Objetivo: Especificar cómo y cuándo se debe distribuir o compartir información al interior o por fuera de la empresa.

2. Alcance: Esta política el aplicable a toda la información que hace parte de las diferentes dependencias de la empresa.

3. Roles y responsabilidades:

- Administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de

[66] PAREX. Política y procedimientos de divulgación de información, confidencialidad, uso lícito de información privilegiada y periodo de bloqueo. [En línea]. 2019. [Consultado el 14 de Febrero de 2021]. Disponible en: https://parexresources.com/wp-content/uploads/2020/07/COL-GRH-RH-PO-007-POL%C3%8DTICA-Y-PROCEDIMIENTOS-DE-DIVULGACI%C3%93N-DE-INF.pdf

comunicaciones y mercadeo y los líderes de los demás departamentos del CSIRT.

- Líder de departamento: Los líderes de departamento serán los responsables de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal de la empresa.

4. Disposiciones:

a) Controles y procedimientos: Los controles y procedimientos de divulgación de información dentro y fuera de la empresa implicaran lo siguiente:

- Seguimiento e identificación de los requisitos de divulgación según las normativas, leyes y decretos expedidos por el gobierno.

- Identificación de las personas y equipos de trabajo responsables de preparar los informes y notificaciones de divulgación.

- Diseño y ejecución de procedimientos para la revisión y preparación de la información objeto de divulgación.

- Obtención de aprobaciones referentes a la divulgación de información empresarial por parte de las diferentes dependencias de la empresa.

- Procedimientos para la presentación de informes oportunos al equipo administrador de esta política.

- Garantizar que se cumplan los procedimientos referentes a la divulgación de información, evaluando continuamente los controles implementados por las diferentes dependencias de la empresa.

b) Información Pública: Toda la información de la empresa catalogada como pública está autorizada para ser difundida, teniendo en cuenta los procedimientos y canales establecidos para tal fin.

c) Información de uso interno: Este tipo de información solo puede ser difundida con la autorización de equipo administrador de esta política.

d) Información Restringida: Este tipo de información solo puede ser divulgada a una dependencia o personas en específico, después de ser autorizadas por el equipo administrador de esta política.

e) Información confidencial: Este tipo de información solo puede ser gestionada por personal exclusivo autorizado por las directivas del CSIRT, en caso de requerir divulgación de este tipo de información al personal exclusivo, es necesaria la autorización de la Dirección del CSIRT, dejando actas de confidencialidad y no divulgación.

f) Información Sensible. Este tipo de información no debe ser divulgada ya que está amparada por la ley.

g) Pedidos de información. La dinámica de trabajo y cooperación entre CSIRT permite la divulgación de información entre diferentes equipos de respuesta, siempre cumpliendo las normas legales y disposiciones expuestas en esta política.

h) Ningún miembro de la empresa está autorizado para divulgar información o brindar declaraciones sobre los procedimientos internos a los medios de comunicación, este tipo de divulgaciones deben realizarse por medio de los representantes de la empresa autorizados para tal fin.

6.4.6 Política de acceso a la información[67]

1. Objetivo: Establecer el personal que puede acceder a la información de la empresa, teniendo en cuenta la clasificación de la información, los permisos y excepciones.

2. Alcance: Esta política es de obligatorio cumplimiento por parte de todo el personal y dependencias del CSIRT.

3. Roles y responsabilidades:

- Comité administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y los líderes de los demás departamentos del CSIRT.

- Líder de departamento: Los líderes de departamento serán los responsables de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal del CSIRT.

[67] OEA. Política de acceso a la información. [En línea]. 2012. [Consultado el 20 de Febrero de 2021]. Disponible en: http://www.oas.org/legal/spanish/gensec/exor1202.pdf

- Terceros: Los proveedores, asesores y cualquier persona con acceso a los equipos y sistemas informáticos del CSIRT, quedarán sujetos a esta Política.

4. Disposiciones:

a) El comité administrador de la política establecerá y clasificará la información por niveles de acceso y determinará la restricciones y procedimientos para acceder a la información.

b) Acceso permanente a la información: Se establecerán medios de comunicación como la página web de la empresa, redes sociales y canales telefónicos con el propósito de compartir información catalogada como publica que pueda ser de interés para los ciudadanos, referente a los servicios de la empresa, atención al cliente, ultimas noticias, ofertas de empleo, entre otros.

c) Restricciones: La información catalogada como confidencial, reservada o sensible no podrá ser publicada a través de los medios de comunicación de acceso permanente, dentro de esta se encuentra la siguiente:

- información que afecte la privacidad de los usuarios, empleados, e interesados.
- Información sobre procesos de licitación y contratación.
- Información sujeta a secreto profesional.
- Información protegida por derechos de propiedad intelectual.
- Información judicial.
- Información que el comité administrador considere como inadecuada para publicar.

d) Solicitudes de información: Para solicitar información que no se encuentre publicada en los medios de comunicación de la empresa, se debe realizar una petición formal que contenga la información personal del peticionario, la descripción del requerimiento y una dirección física o electrónica para recibir respuesta.

6.4.7 Política de uso apropiado de los sistemas del CSIRT[68]

1. Objetivo: Definir el uso aceptable e inaceptable de los recursos y sistemas pertenecientes al CSIRT.

2. Alcance: Esta política es de obligatorio cumplimiento por parte de todo el personal que tenga acceso a los sistemas y recursos del CSIRT, incluyendo contratistas, consultores y pasantes.

3. Roles y responsabilidades:

- Comité administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y los líderes de los demás departamentos del CSIRT.

- Líder de departamento: Los líderes de departamento serán los responsables de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal de la empresa que tenga acceso a los sistemas y recursos de CSIRT.

4. Disposiciones:

a) La operación del CSIRT utiliza dispositivos, redes, sistemas de información y aplicaciones, los cuales deben ser gestionados responsablemente conservando la disponibilidad, integridad y confidencialidad de los activos de información.

b) La administración del CSIRT puede aprobar excepciones que deben ser aprobadas por el comité administrador de esta política.

c) Los empleados del CSIRT son responsables de ejercer el uso apropiado de los recursos y sistemas disponibles, respetando las políticas y procedimientos establecidos para tal fin. Los recursos y sistemas no deben ser utilizados con fines ilícitos que atenten contra las políticas de la empresa.

[68] CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. 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

d) Los empleados son responsables de la seguridad de los activos de información bajo su cargo, manteniendo buenas prácticas de seguridad y aplicando los controles establecidos para tal fin.

f) Está prohibido el almacenamiento y uso de información confidencial en aplicaciones o sistemas no controlados por el CSIRT.

g) Los empleados son responsables de la seguridad y el buen uso de los recursos y sistemas a cargo, queda prohibido el uso de recursos que:

- Generen fallas o vulnerabilidades que afecten la seguridad de los activos de información.
- Generen interrupciones en los servicios y recursos de red del CSIRT.
- Violen las leyes de derechos de autor.
- Apoyen o incentiven actividades ilegales, incluyendo la distribución de contenido que viole las políticas de protección de datos.

h) Protección de los sistemas de información: Los sistema y aplicaciones del CSIRT están expuestos a riesgos que afectan su adecuado funcionamiento, por lo cual se debe:

- Asignar un responsable a cada aplicación y sistema que se encargará de velar por su buen uso y funcionamiento.
- Evitar el acceso de personal no autorizado a los ambientes de producción de software.
- Establecer un sistema de control de cambios para registrar las modificaciones realizadas a los sistemas.
- Contar con la autorización del comité administrador de la política
- Implementar un sistema de protección y respaldo de los códigos fuentes de los sistemas y aplicaciones desarrolladas por la empresa.

6.4.8 Definición de Incidentes de seguridad y política de eventos[69]

1. Objetivo: Establecer los criterios para clasificar los eventos e incidentes de seguridad según su prioridad e impacto.

2. Alcance: Esta política es de obligatorio cumplimiento por parte del personal del departamento de operaciones, quienes se son los encargados de gestionar los incidentes y eventos del CSIRT.

3. Roles y responsabilidades:

- Comité administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y el líder de departamento de operaciones del CSIRT.

- Líder de departamento: El líder del departamento operativo del CSIRT será el responsable de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte del personal encargado de gestionar los incidentes y eventos de seguridad del CSIRT.

4. Disposiciones:

a) Un incidente de seguridad es un evento con consecuencias que afectan la disponibilidad, confidencialidad e integridad de los activos de información de la empresa.

b) La categorización de los incidentes y eventos de seguridad es responsabilidad del departamento operativo del CSIRT, y se realizará teniendo en cuenta los criterios de prioridad e impacto.

c) Impacto.

- Impacto Grave: Incidentes que afectan directamente los recursos necesarios para el correcto funcionamiento del negocio, afectando activos de información críticos para su operación.

"[69] MINTIC. Guía para la Gestión y Clasificación de Activos de Información. [En línea]. 2016. [Consultado el 14 de Febrero de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf"

- Impacto Medio: Incidentes que no afectan directamente los recursos críticos del negocio, pero causan retrasos en los procesos de las diferentes dependencias del CSIRT.

- Impacto Leve: Incidentes que no presentan ninguna afectación para los servicios que presta la empresa,

- pero pueden provocar fallas futuras en la ejecución de los procesos.

d) Prioridad de atención.

- Emergencia: Incidentes cuya solución no debe dar espera, para lo cual se utilizarán todos los recursos disponibles, por lo general, son incidentes que suponen riesgo para la vida de las personas o temas de seguridad Nacional.

- Alta: Incidentes que requieren atención inmediata y aunque se hayan registrado posteriormente se mantienen en una cola de incidentes de prioridad alta, en este caso no serán atendidos incidentes de prioridad inferior hasta no solucionar los de dicha cola.

- Media: Incidentes que se atienden por defecto en serie por orden de llegada, siempre y cuando no se registre un incidente de prioridad mayor. Este tipo de incidentes pueden cambiar de prioridad según sus características e impacto.

- Baja: Este tipo de incidentes se atienden por orden de siempre y cuando no se registre un incidente de prioridad mayor, por lo general son incidentes

6.4.9 Política de gestión de incidentes[70]

1. Objetivo: Definir el proceso de solicitud y respuesta de incidentes de seguridad.

2. Alcance: Es de obligatorio conocimiento y cumplimiento por parte de todo el personal del CSIRT.

3. Roles y responsabilidades:

[70] CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. 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

- Comité administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y los líderes de los demás departamentos del CSIRT.

- Líder de departamento: Los líderes de departamento serán los responsables de informar a la Dirección General sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal de la empresa que tenga acceso a los sistemas y recursos de CSIRT.

4. Disposiciones:

a) Todo el personal del CSIRT debe tener conocimiento sobre el proceso de solicitud y respuesta de incidentes de seguridad teniendo en cuenta los siguientes parámetros:

- El personal de comunicaciones debe enviar a los empleados y clientes del CSIRT información referente a los canales de atención para el reporte de incidentes, adicionalmente debe publicar los protocolos y procedimientos de atención en la página web y redes sociales de la entidad.

- El personal de comunicaciones debe publicar periódicamente información y estadísticas sobre acontecimientos y amenazas de seguridad de la información y compartirá los reportes más relevantes con otros equipos de respuesta de la región.

- El personal de la dependencia de gestión de solicitudes e incidentes debe realizar el registro y categorización de los incidentes reportados por los usuarios.

- Se prohíbe el uso de herramientas y procedimientos no autorizados por el CSIRT para la atención de incidentes.

- La información recolectada en los registros de incidentes se tratará según las políticas de protección de información y datos personales del CSIRT.

- El registro de la información de los incidentes y el tratamiento de datos debe cumplir estándares internacionales, con el propósito de recolectar evidencias digitales y aportarlas en caso de ser requeridas por parte de las autoridades judiciales.

b) Reporte de Incidentes de Seguridad: El personal y los usuarios del CSIRT deben conocer el protocolo para reportar incidentes, el cual contiene los siguientes lineamientos:

- El registro de incidentes de seguridad lo debe realizar el personal de la dependencia de gestión de solicitudes e incidentes, quienes remitirán una respuesta de conocimiento del incidente, notificando que se inicia el proceso de clasificación y asignación para atender el incidente lo más pronto posible.

- El especialista de gestión de solicitudes e incidentes debe analizar el registro del incidente y asignarlo según su clasificación a la dependencia idónea para que ejecute el proceso de solución.

- La dependencia asignada una vez recibido el incidente, debe diagnosticar la situación encontrada y diligenciar un informe con la solución efectuada.

- El líder del departamento de operaciones debe revisar el informe de solución y registrar la información en el sistema de gestión de incidentes, adicionalmente verifica si se requiere una aclaración desde el punto de vista técnico, para darle una respuesta satisfactoria al usuario que solicita el servicio.

c) Detección automática de incidentes: Se deben implementar herramientas y mecanismos de detección automática de intrusiones, que estén en constante monitoreo y generen alertas que detallen lo sucedido en tiempo real.

d) Evaluación incidentes: Después de detectar automáticamente un incidente, debe ser categorizado por el personal de la dependencia de gestión de solicitudes e incidentes, estableciendo el impacto y la prioridad de atención.

f) Resolución de incidentes: Es prioritario desarrollar informes y documentar guías de atención para cada uno de los tipos de incidentes, enfatizando en aquellos incidentes de mayor concurrencia e impacto. Se deben detallar procedimientos para las siguientes actividades:

- Recolección de evidencias tan pronto como sea posible desde la ocurrencia del incidente.

- Definir un tiempo de solución al incidente.

- Realizar análisis forenses en caso de ser necesario.

- En caso de que el incidente no pueda ser solucionado, se debe gestionar su escalamiento al especialista adecuado.

- Ejecutar acciones para tratar de mitigar los daños, causas y consecuencias del incidente.

g) Tratamiento del registro del incidente: El tratamiento efectivo de los incidentes requiere el registro de la siguiente información:

- Fecha y hora de ocurrencia del incidente

- Descripción básica del incidente

- Recursos y áreas afectadas

- Posibles causas del incidente

- Estado actual

- Acciones realizadas hasta el momento para solucionarlo

- Fecha y hora de solución

- Cierre del incidente

6.4.10 Política de cooperación[71]

1. Objetivo: Definir las condiciones mínimas para realizar acuerdos de cooperación entre equipos de respuesta CSIRT.

2. Alcance: Esta política aplica para todos los empleados del CSIRT y los equipos de respuesta aliados con los que se tengan convenios de cooperación.

3. Roles y responsabilidades:

- Comité administrador de la política: Esta Política será administrada por un representante del departamento de Dirección, el especialista de gestión de seguridad de la información y los líderes de los demás departamentos del CSIRT.

[71] ENSIA. CSIRT Setting up Guide in Spanish — ENISA. [En línea]. 2006. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish

- Líder de departamento: Los líderes de departamento serán los responsables de informar a la Dirección sobre el nivel de cumplimiento de esta política.

- Empleados: Esta política es de obligatorio cumplimiento por parte de todo el personal de la empresa que tenga acceso a los sistemas y recursos de CSIRT.

- Aliados: Son todos los equipos de respuesta y organizaciones con los que se tienen convenios de cooperación.

4. Disposiciones:

a) La cooperación entre equipos de respuesta CSIRT, grupos de investigación y empresas de seguridad informática, fortalece las capacidades de respuesta ante eventos que afectan la disponibilidad, confidencialidad e integridad de los activos de información de las empresas, gobiernos y la sociedad.

b) La realización de acuerdos de cooperación con equipos de respuesta, grupos de investigación y empresas de seguridad informática, deben contener los siguientes requisitos mínimos:

- Definición y aprobación de los objetivos del convenio de cooperación

- Análisis del alcance, tiempo y costo del convenio de cooperación

- Definir las cláusulas de terminación del acuerdo

- Definición de los procedimientos y protocolos para el flujo de información y trabajo colaborativo entre las entidades

- Toda la información generada en el marco del convenio de cooperación debe alinearse con las políticas de protección de información de las entidades

7 CONCLUSIONES

El diseño administrativo del CSIRT otorga la hoja de ruta para la adecuada implementación de los procesos necesarios, para iniciar las operaciones del equipo de respuestas de Cibersecurity de Colombia, adicionalmente permite una adecuada gestión de las solicitudes e incidentes de ciberseguridad de la empresa y sus clientes.

Es importante implementar estrategias y mecanismos que permitan asegurar los activos de información frente a los riesgos y amenazas informáticas existentes. Los equipos de respuestas a incidentes cibernéticos (CSIRT), son una excelente alternativa de seguridad, ya que centralizan los especialistas, las herramientas y la tecnología necesaria, para atender cualquier tipo de incidente de ciberseguridad.

La taxonomía de ataques informáticos permite que los equipos de respuesta CSIRT realicen una adecuada planeación y diseño de sus servicios, optimizando sus recursos tecnológicos, financieros y de personal.

El ámbito de actuación de un CSIRT define el alcance que tendrán sus servicios, que pueden ser dirigidos a personas, organizaciones y gobiernos, abarcando áreas locales, campus universitarios, ciudades e inclusive todo un país.

Los servicios de un CSIRT se deben alinear a los avances de las tecnologías de la información y a los delitos informáticos que se producen en su ámbito de actuación. Una constante vigilancia tecnológica y las alianzas con otros CSIRT de la región permiten la mejora continua en la operación de los equipos de respuesta.

8 RECOMENDACIONES

Realizar vigilancia tecnológica y mantener una base de conocimiento actualizada, en temas relacionados con nuevas tecnologías, amenazas informáticas, y proyectos relacionados con la ciberseguridad.

Implementar sistemas de gestión del conocimiento para el CSCIRT e invertir en investigación, desarrollo e innovación.

Establecer alianzas con otros CSIRT de la región, con el propósito de intercambiar conocimientos, recursos y desarrollar planes de trabajo para fortalecer la ciberseguridad y el desarrollo tecnológico de la región.

BIBLIOGRAFÍA

ACIS. Hay escases de personal calificado en la industria de ciberseguridad en Colombia. [En línea]. 2017. [Consultado el 17 de Octubre de 2019]. Disponible en: https://acis.org.co/portal/content/hay-escases-de-personal-calificado-en-la-industria-de-ciberseguridad-en-colombia

Agencia Nacional de Tierras. Lineamientos de seguridad de la información, tratamiento y protección de datos personales. [En línea]. 2017. [Consultado el 14 de Febrero de 2021]. Disponible en: https://www.agenciadetierras.gov.co/wp-content/uploads/2018/04/INTI-Politica-008-LINEAMIENTOS-DE-SEGURIDAD-DE-LA-INFORMACION-TRATAMIENTO-Y-PROTECCION-DE-DATOS-PERSONALES.pdf

Armas, H. andrés. *GESTIÓN DE SEGURIDAD EN LA RED DE DATOS DE LA CORTE CONSTITUCIONAL MEDIANTE EL DISEÑO DE UN CSIRT (EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD)*. [En línea]. 2012. [Consultado el 17 de Octubre de 2019]. Disponible en: https://dspace.ups.edu.ec/handle/123456789/3776

Asociación CATAI. Modelo de Coordinación y Atención de Emergencias en el ámbito de la Sociedad de la Información. [En línea]. 2007. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://catai.net/blog/wp-content/uploads/2009/01/premioacademiacanariaseguridad.pdf

Batista Díaz, C. M. Lujo Aliaga, Z. Cedeño Galindo, L. V. Propuesta e implementación de la arquitectura de la red LAN en la empresa Acinox Las Tunas. [En línea]. 2018. [Consultado el 18 de Diciembre de 2020]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7107368

Bayona, Z. O. Hacia una Taxonomía de Incidentes de Seguridad en Internet. [En Línea]. 2006. [Consultado el 14 de marzo de 2021]. Disponible en: https://revistas.udistrital.edu.co/index.php/reving/article/view/2308/3126

CCIT. Tendencias cibercrimen Colombia 2019-2020 [En línea]. 2019. [Consultado el 17 de marzo de 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. 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

CCOCI. COMANDO CONJUNTO CIBERNÉTICO. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.ccoc.mil.co/quienes_somos/ccoc/que_hacemos

Cedeño Cruz, A. Y. Simulación de una gestión unificada de amenazas para administrar la red de datos de la Empresa FAINCA GROUP utilizando la tecnología OPEN SOURCE. [En línea]. 2018. [Consultado el 17 de Diciembre de 2020]. Disponible en: http://repositorio.ug.edu.ec/handle/redug/27039

CEMEX. Política de Retención de Información de CEMEX. [En línea]. 2009. [Consultado el 20 de Febrero de 2021]. Disponible en: https://www.cemex.com/documents/20143/160085/politica-retencion-informacion.pdf/b2bac2e3-efc8-8f5a-9a5c-fd2679938af4

ColCERT. Grupo de Respuesta a Emergencias Cibernéticas de Colombia. [En línea]. 2017. [Consultado el 17 de Octubre de 2019]. Disponible en: http://www.colcert.gov.co/?q=acerca-de

Colombia, C. de la R. de. Ley 1273 de 05 Enero de 2009. [En línea]. 2009. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Colombia, C. de la R. de. LEY 1928 DE 24 Julio 2018. [En línea]. 2018. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501

CONPES. CONPES 3701 de 2011. [En línea]. 2011. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

CONPES. CONPES 3858 de 2016. [En línea]. 2016. [Consultado el 17 de Octubre de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CORTÉS BORRERO, R. ESTADO ACTUAL DE LA POLÍTICA PÚBLICA DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA. [En línea]. 2015. [Consultado el 5 de Noviembre de 2019]. Disponible en: https://doi.org/10.15425/redecom.14.2015.06

De la Torre Moscoso, H. M., & Parra Rosero, M. A. Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la Universidad de las Fuerzas Armadas ESPE. [En línea]. 2018. [Consultado el 5 de Noviembre de 2019]. Disponible en: http://repositorio.espe.edu.ec/jspui/handle/21000/15071

Delvasto Ramírez, R. A. Modelo de Gestión de incidentes de seguridad de la información para PYMES. [En línea]. 2016. [Consultado el 16 de Diciembre de 2020]. Disponible en: https://repository.unad.edu.co/handle/10596/6170

El Colombiano. La banca estrena bloque de reacción inmediata contra ciberataques. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elcolombiano.com/negocios/innovacion/seguridad-sistema-financiero-ciberataques-HX9213801

El Espectador. Registraduría ha recibido cuatro ataques informáticos a su página web. [En línea]. 2018 [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elespectador.com/economia/se-han-registrado-cuatro-intentos-para-tumbar-la-pagina-de-la-registraduria-mindefensa-articulo-743295

El Espectador. Un oficial del Centro Cibernético Policial de Colombia explica estrategia para elecciones. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elespectador.com/noticias/judicial/un-oficial-del-centro-cibernetico-policial-de-colombia-explica-estrategia-para-elecciones-articulo-737056

El Heraldo. Hackean página de Registraduría a cuatro días del plebiscito. [En línea]. 2016. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elheraldo.co/politica/hackean-pagina-de-registraduria-cuatro-dias-del-plebiscito-288431

El Heraldo. Ciberataque golpeó a 11 empresas y una entidad pública en Colombia. [En línea]. 2017. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.elheraldo.co/ciencia-y-tecnologia/ciberataque-golpeo-11-empresas-y-una-entidad-publica-en-colombia-361747

ENSIA. CSIRT Setting up Guide in Spanish — ENISA. [En línea]. 2006. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish

Fernández, L. Qué son los Advanced Persistent Threats y cómo protegernos de los APT. [En línea]. 2020. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/advanced-persistent-threats-apt-protegernos/

Gerente.com. Ciberseguridad en Colombia tiene pocos expertos. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: http://gerente.com/co/ciberseguridad-expertos-colombia/

Hurtado Vargas, L. F. & Chuquiguanca Vicente, L. R. Implementación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) en la Fiscalía

General del Estado. [En línea]. 2020. [Consultado el 16 de Diciembre de 2020]. Disponible en: https://repositorio.uisek.edu.ec/handle/123456789/3959

Infotecs. IPS: Sistema de Prevención de Intrusos. [En línea]. 2019. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://infotecs.mx/blog/ips-sistema-de-prevencion-de-intrusos.html

Jerez, D. UNP advierte que recibe 500 ataques cibernéticos al día. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.lafm.com.co/colombia/unp-advierte-que-recibe-500-ataques-ciberneticos-al-dia

La República. Asobancaria presenta primer equipo de seguridad cibernética. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.larepublica.co/finanzas/asobancaria-presenta-primer-equipo-de-seguridad-cibernetica-2763005

Luna, R. Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). [En línea]. 2015. [Consultado el 17 de Octubre de 2019]. Disponible en: http://www.revistascientificas.udg.mx/index.php/REC/article/view/5209/4865

Maridueña Carrión, N. E. LA IMPORTANCIA DE LOS IPS Y BYOD EN LAS ORGANIZACIONES: CASO DE ESTUDIOS CONFIDENCIAL S.A. [En línea]. 2017. [Consultado el 18 de Diciembre de 2020]. Disponible en: https://www.bibliotecasdelecuador.com/Record/oai:localhost:123456789-1436

MINTIC. Colombia y Chile suscriben memorando de cooperación en ciberseguridad, ciberdefensa y cibercriminalidad. [En línea]. 2019. [Consultado el 25 de Noviembre de 2019]. Disponible en: https://mintic.gov.co/portal/604/w3-article-92617.html?_noredirect=1

MINTIC. Guía para la Gestión y Clasificación de Activos de Información. [En línea]. 2016. [Consultado el 14 de Febrero de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Miranda, J. M., & Ramirez, H. Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (17), 1–15. 2016. https://doi.org/10.17013/risti.17.1-15

Novoa, H. A., & Barrera, C. R. Metodologías para el análisis de riesgos en los sgsi. [En línea]. 2015. [Consultado el 17 de Octubre de 2019]. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

OEA. Política de acceso a la información. [En línea]. 2012. [Consultado el 20 de Febrero de 2021]. Disponible en: http://www.oas.org/legal/spanish/gensec/exor1202.pdf

OEA. Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. [En línea]. 2013. [Consultado el 16 de Diciembre de 2020]. Disponible en: http://technoint.weebly.com/uploads/2/1/2/9/21297584/tendencias_del_cibercrimen_hecho_por_la_oea.pdf

Oracle. ¿Qué es un SOC? [En línea]. 2021. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.oracle.com/es/database/security/que-es-un-soc.html

Organización de los Estados Americanos. Buenas prácticas para establecer un CSIRT nacional. [En línea]. 2016. [Consultado el 14 de Febrero de 2019]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Pachón Ramírez, J. A. Gestión de incidentes de seguridad de la información para la superintendencia financiera de Colombia. [En línea]. 2016. [Consultado el 16 de Diciembre de 2020]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2773

Palacios Santamaría, P. A., & Andrés, P. Equipo de respuesta ante incidentes informáticos para La Universidad Regional Autónoma de Los Andes. [En línea]. 2018. [Consultado el 17 de Octubre de 2019]. Disponible en: http://dspace.uniandes.edu.ec/handle/123456789/8158

PAREX. Política y procedimientos de divulgación de información, confidencialidad, uso lícito de información privilegiada y periodo de bloqueo. [En línea]. 2019. [Consultado el 14 de Febrero de 2021]. Disponible en: https://parexresources.com/wp-content/uploads/2020/07/COL-GRH-RH-PO-007-POL%C3%8DTICA-Y-PROCEDIMIENTOS-DE-DIVULGACI%C3%93N-DE-INF.pdf

PCI Hispano. Eliminación destrucción segura de datos y medios de almacenamiento. [En línea]. 2014. [Consultado el 14 de Febrero de 2021]. Disponible en: https://www.pcihispano.com/eliminaciondestruccion-segura-de-datos-y-pci-dss/

Portafolio. El secuestro de información desangra a las empresas del país. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

Revista Dinero. Ciberseguridad en el 2019 en Colombia. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

Revista Dinero. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [En línea]. 2019. [Consultado el 5 de Octubre de 2019]. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

Revista Semana. Así está Colombia en el ranking de ciberseguridad mundial. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

Secretaría del senado. Ley 1978 de 2019. [En línea]. 2019. [Consultado el 25 de Noviembre de 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1978_2019.html

UNAM. Firewall de Aplicación Web - Parte I. [En línea]. 2018. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://revista.seguridad.unam.mx/numero-16/firewall-de-aplicación-web-parte-i

UNAM. Firewall de bases de datos. [En línea]. 2018. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

Uyana García, M. A. Propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos, CSIRT. [En línea]. 2014. [Consultado el 17 de Octubre de 2019]. Disponible en: http://repositorio.espe.edu.ec/jspui/handle/21000/8063

Tecnozero.¿Qué es un EDR? ¿Por qué es diferente de un antivirus?. [En línea]. 2020. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/

Vega Barbosa, C. Las pymes como blanco para los ciberdelincuentes. [En línea]. 2018. [Consultado el 5 de Octubre de 2019]. Disponible en: https://www.elespectador.com/tecnologia/las-pymes-como-blanco-para-los-ciberdelincuentes-articulo-828209

Velasquez, A. M. Principales ataques de cibercriminales en Colombia. [En línea]. 2019. [Consultado el 17 de Octubre de 2019]. Disponible en:

https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-ataques-de-cibercriminales-en-colombia-371096

Villagómez, C. Sistema de detección de intrusiones (IDS). [En línea]. 2017. [Consultado el 17 de Diciembre de 2020]. Disponible en: https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

William R. Cheswick y Steven M. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Publishing Company, Estados Unidos, 1994.

Resumen Analítico Especializado (RAE)	
Tema	Infraestructura Tecnológica y Seguridad en Redes
Título	DISEÑO ADMINISTRATIVO DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA
Autor	Jorge Luis Flórez Benavides
Fuente Bibliográfica	• Organization of American States. Best Practices for Establishing a National CSIRT. [En línea]. 2016. [Consultado el 14 de febrero de 2019]. Disponible en: https://cutt.ly/JnaMmYu • CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de octubre de 2019]. Disponible en: https://cutt.ly/VyIwzLr • De la Torre Moscoso, H. M., & Parra Rosero, M. A. Estrategia y diseño de un CSIRT académico para la Universidad de las Fuerzas Armadas ESPE. [En línea]. 2018. [Consultado el 5 de noviembre de 2019]. Disponible en: https://cutt.ly/gyIwlKn
Año	2021
Resumen	Según informes de las multinacionales CISCO[72] y FORTINET[73], en Colombia existen importantes brechas de ciberseguridad, que afectan principalmente al sector empresarial y gubernamental, adicionalmente afirman que los índices de ataques informáticos en el país son alarmantes, generando potenciales problemas para la seguridad de las empresas. Una de las causas de los elevados índices de ciberataques, es el constante desarrollo de herramientas y técnicas cada vez más sofisticadas para vulnerar las redes y los sistemas, por lo tanto, las empresas requieren de una constante actualización, especialización e implementación de nuevas estrategias para asegurar sus activos de información. Este proyecto aplicado se desarrolla sobre el escenario hipotético, de una empresa que presta servicios de seguridad de la Información llamada “Cibersecurity de Colombia LTDA”, que tiene como objetivo consolidarse como un Centro de Respuesta CSIRT, para fortalecer la respuesta a incidentes y la gestión de vulnerabilidades según los servicios contratados por sus clientes.

[72] Vega Barbosa, C. Las pymes como blanco para los ciberdelincuentes. [En línea]. 2018. [Consultado el 5 de octubre de 2019]. Disponible en: https://www.elespectador.com/tecnologia/las-pymes-como-blanco-para-los-ciberdelincuentes-articulo-828209

[73] Revista Dinero. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. [En línea]. 2019. [Consultado el 5 de octubre de 2019]. Disponible en: https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556

	El objetivo del proyecto es el diseño de la documentación administrativa de un Equipo de Respuesta a Incidentes Cibernéticos (CSIRT) para la empresa Cibersecurity de Colombia LTDA, su desarrollo se fundamenta en una metodología de investigación documental descriptiva, que comprende la selección, análisis e interpretación de documentos y material de consulta, referente a los procesos administrativos y funcionamiento de diferentes equipos de respuesta CSIRT.
Palabras Claves	Amenaza informática, riesgo informático, ciberdefensa, ciberdelincuentes, ciberseguridad, CSIRT, seguridad de la información, seguridad informática.
Contenidos	1. DEFINICIÓN DEL PROBLEMA 1.1 ANTECEDENTES DEL PROBLEMA 1.2 FORMULACIÓN DEL PROBLEMA 2. JUSTIFICACIÓN 3. OBJETIVOS 3.1 OBJETIVOS GENERAL 3.2 OBJETIVOS ESPECÍFICOS 4. MARCO REFERNCIAL 4.1 MARCO TEÓRICO 4.2 MARCO CONCEPTUAL 4.3 MARCO HISTÓRICO 4.4 ANTECEDENTES O ESTADO ACTUAL 4.5 MARCO CIENTÍFICO O TECNOLÓGICO 4.6 MARCO LEGAL 5. DISEÑO METODOLÓGICO 6. DESARROLLO DE LOS OBJETIVOS 6.1 TAXONOMÍA DE ATAQUES Y ÁMBITO DE ACTUACIÓN DEL CSIRT 6.2 SERVICIOS DEL CSIRT 6.3 ESTRUCTURA ORGÁNICA Y PERFILES DEL EQUIPO DEL CSIRT 6.4 POLÍTICAS Y PROCEDIMIENTOS OPERACIONALES DEL CSIRT 7. CONCLUSIONES 8. RECOMENDACIONES
Descripción del problema de investigación	La multinacional CISCO Systems estima que más de la mitad de las PYMES de Latinoamérica tienen importantes brechas de seguridad, a razón de que los ciberataques no solo están dirigidos a las grandes empresas y al sector gobierno, las organizaciones de menor escala también son el objetivo de este tipo de delincuentes. Según estudios de CISCO, el 53%

	de las pymes latinoamericanas reportaron brechas de seguridad aludiendo que es un problema muy costoso, pues en el 40% de los casos de ataques cibernéticos, se generaron tiempos de inactividad empresarial de alrededor de ocho horas, lo cual generó impactos negativos en la productividad y prestación de los servicios. Adicionalmente en el 39% de los ataques se generaron daños en más del 50% de los sistemas de información y equipos, provocando pérdidas que oscilan entre los 320 millones y 8.000 millones de pesos por empresa damnificada.[74] Las estadísticas demuestran que los ciberataques están en constante crecimiento y evolución, diariamente los delincuentes informáticos trabajan para aprovechar las vulnerabilidades de las redes y aplicaciones, desarrollando nuevas versiones de ataques y técnicas más sofisticadas para lograr sus objetivos. En Colombia diferentes empresas han reportado brechas de seguridad, confirmando que los índices de ciberataques son alarmantes, según lo anterior, se plantea la siguiente pregunta: ¿Cómo ayuda el diseño administrativo de un CSIRT en la gestión de incidentes informáticos para la empresa Cibersecurity de Colombia?
Objetivo general	Diseñar la documentación desde el enfoque directivo administrativo, que permita dar desarrollo a las actividades propias de un CSIRT para la empresa Cibersecurity de Colombia Ltda.
Objetivos específicos	• Establecer la taxonomía de ataques y el ámbito de actuación del CSIRT. • Elaborar el catálogo de servicios proactivos, reactivos y complementarios del CSIRT. • Proponer la estructura orgánica y los perfiles del equipo de trabajo para la conformación del CSIRT. • Formular las políticas y procedimientos operacionales del CSIRT.
Metodología	Para el desarrollo del proyecto aplicado se utiliza una metodología de revisión documental descriptiva, que comprende la selección, análisis e interpretación de documentos y material de consulta referente a los procesos

[74] Vega Barbosa, C. Las pymes como blanco para los ciberdelincuentes. [En línea]. 2018. [Consultado el 5 de octubre de 2019]. Disponible en: https://www.elespectador.com/tecnologia/las-pymes-como-blanco-para-los-ciberdelincuentes-articulo-828209

	administrativos y funcionamiento de diferentes equipos de respuesta CSIRT. La metodología tiene un componente cuantitativo, ya que uno de los objetivos específicos es la cuantificación y medición del impacto de los ataques y amenazas informáticas en Colombia, permitiendo definir la taxonomía de ataques y ámbito de actuación del CSIRT. Adicionalmente la metodología cuenta con un componente cualitativo, en el cual se realiza la indagación y análisis de las características y funcionalidades de los equipos de respuesta CSIRT, con el propósito de definir los servicios y establecer los procedimientos necesarios para la operación de un equipo de respuestas a incidentes cibernéticos.
Principales referentes teóricos y conceptuales	• Organization of American States. Best Practices for Establishing a National CSIRT. [En línea]. 2016. [Consultado el 14 de febrero de 2019]. Disponible en: https://cutt.ly/JnaMmYu • CCN. GUÍA DE CREACIÓN DE UN CERT / CSIRT. [En línea]. 2011. [Consultado el 17 de octubre de 2019]. Disponible en: https://cutt.ly/VyIwzLr • De la Torre Moscoso, H. M., & Parra Rosero, M. A. Estrategia y diseño de un CSIRT académico para la Universidad de las Fuerzas Armadas ESPE. [En línea]. 2018. [Consultado el 5 de noviembre de 2019]. Disponible en: https://cutt.ly/gyIwlKn
Resultados	Como resultado se obtuvo la documentación administrativa que permite el funcionamiento de un CSIRT, incluyendo el ámbito de actuación del equipo de respuestas, la taxonomía de ataques, el catálogo de servicios, los requisitos y perfiles del equipo de trabajo, las políticas y procedimientos operacionales y la estructura orgánica del CSIRT.
Conclusiones	• El diseño administrativo del CSIRT otorga la hoja de ruta para la adecuada implementación de los procesos necesarios, para iniciar las operaciones del equipo de respuestas de Cibersecurity de Colombia, adicionalmente permite una adecuada gestión de las solicitudes e incidentes de ciberseguridad de la empresa y sus clientes. • Es importante implementar estrategias y mecanismos que permitan asegurar los activos de información frente a los riesgos y amenazas informáticas existentes. Los equipos de respuestas a incidentes cibernéticos (CSIRT), son una excelente alternativa de seguridad, ya que centralizan los especialistas, las herramientas y la tecnología necesaria, para atender cualquier tipo de incidente de ciberseguridad. • La taxonomía de ataques informáticos permite que los equipos de respuesta CSIRT realicen una adecuada planeación y diseño de sus servicios, optimizando sus

	recursos tecnológicos, financieros y de personal. • El ámbito de actuación de un CSIRT define el alcance que tendrán sus servicios, que pueden ser dirigidos a personas, organizaciones y gobiernos, abarcando áreas locales, campus universitarios, ciudades e inclusive todo un país. • Los servicios de un CSIRT se deben alinear a los avances de las tecnologías de la información y a los delitos informáticos que se producen en su ámbito de actuación. Una constante vigilancia tecnológica y las alianzas con otros CSIRT de la región permiten la mejora continua en la operación de los equipos de respuesta.