DISEÑO TÉCNICO DE UN CSIRT COMO MEDIO DE ANÁLISIS Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

IVÁN DARÍO MONTES DÍAZ

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

DISEÑO TÉCNICO DE UN CSIRT COMO MEDIO DE ANÁLISIS Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

IVÁN DARÍO MONTES DÍAZ

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

Ing. Yenny Stella Núñez Alvarez
Asesor

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

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Fecha sustentación

DEDICATORIA

A Dios.

Por darme gusto y pasión por el conocimiento, por acompañarme en este proceso y por brindarme una nueva oportunidad para avanzar.

A mi esposa.

Por tantos días y noches de paciencia infinita y apoyo incondicional, por ser el más grande motor que me impulsa a continuar en la consecución de este nuevo logro académico.

AGRADECIMIENTOS

Gracias a Dios por brindarme una nueva oportunidad para crecer profesionalmente, por no permitirme desfallecer ante tantas horas de dedicación al estudio, a mi esposa por estar siempre a mi lado animándome a continuar y por su paciencia infinita ante tantos días y noches de trabajo y esfuerzo.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Amenaza: Circunstancia que puede ocurrir en cualquier momento y que puede generar indisponibilidad de los sistemas, mal funcionamiento o pérdida de información. [1]

Análisis: Distinción y separación de las partes de algo para conocer su composición.[2]

Confidencialidad: Significa que la información solo está disponible para los usuarios autorizados para disponer y trabajar sobre ella.[3]

CSIRT: Grupo de expertos en seguridad informática, encargados de realizar monitoreo y análisis de incidentes de seguridad y responder de manera oportuna a ellas.[4]

Diseño: Definición de la arquitectura tecnológica, junto con la descripción detallada de los requisitos de los componentes del sistema.[5]

Disponibilidad: Significa que la información está disponible en todo momento para los usuarios autorizados.[6]

Implementación: Es la realización de procesos y desarrollo de estructuras en un sistema.[7]

[1]INCIBE. «Glosario de términos de ciberseguridad.» 2016. [en linea] (https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridadguia-aproximacion-el-empresario).
[2]Ibid P 9
[3]Ibid P 17
[4]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.
[5]Ibid P 33
[6]Ibid P 21
[7]Ibid P 24

Incidente de seguridad: Cualquier evento o suceso que afecta los activos de información de la entidad.[8]

Infraestructura: Conjunto de hardware y software sobre el cual funcionan los servicios de una organización.[9]

Integridad: Significa que la información no ha sido modificada ni parcial ni totalmente y que se mantiene control de los usuarios que pueden modificar la información.[10]

Políticas de seguridad de la información: Conjunto de reglas o directrices establecidas e implementadas para determinar el rumbo y funcionamiento de los sistemas de información de una organización.[11]

Proactivo: Defensa que se efectúa antes de cualquier ataque informático, buscando prevenir daños a la infraestructura.[12]

Reactivo: Defensa que se efectúa durante o cuando el ataque informático ya ha ocurrido y tratar de solucionarlo.[13]

Riesgo informático: Se define como toda acción que puede afectar un sistema informático, en cualquier momento, ya sea por vulnerabilidades del sistema o aplicaciones, configuraciones mal aplicadas o por amenazas internas o externas.[14]

Seguridad informática: Se define como cualquier procedimiento que impida la ejecución de procesos que han sido autorizados sobre un sistema.[15]

[8]INCIBE. «Glosario de términos de ciberseguridad.» 2016. (https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridadguia-aproximacion-el-empresario).
[9]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.
[10]Ibid P 25
[11]Ibid P 33
[12]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.
[13]Ibid P 25
[14]Ibid P 29
[15]Universidad Internacional de Valencia. «¿Qué es la seguridad informática y cómo puede ayudarme?» 2020. [en linea] https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme.

RESUMEN

El siguiente proyecto aplicado establece la delimitación técnica de un CSIRT como medio de análisis y respuesta ante los ataques y vulnerabilidades informáticas que se presenten dentro de la comunidad de entidades que atiende la empresa Cibersecurity de Colombia LTDA, de forma reactiva y proactiva, ayudando a las entidades a aplicar estrategias y métodos para detectar, mitigar y eliminar las amenazas, aplicar manuales de operación y procedimientos que permitan servir de apoyo para ante incidentes o amenazas de seguridad informática, detectando y/o realizando las correcciones y reparaciones del sistema a las que haya lugar.

El proyecto incluye en su primera parte, la documentación de todo el proceso técnico del CSIRT iniciando por las consideraciones necesarias para su funcionamiento, normas legales, políticas de seguridad informática, servicios vitales de operación, nivel de prestación de los servicios, procedimientos de análisis, monitoreo y reporte, métricas de evaluación de los ANS (acuerdos de nivel de servicio), criterios de evaluación y clasificación de incidentes, estructura jerárquica con que debe contar el CSIRT, tipos de herramientas de software necesarias y se finaliza con la identificación de hardware e infraestructura con que puede trabajar el CSIRT.

En la segunda parte, se realizan laboratorios bajo máquinas virtuales para identificar el funcionamiento en conjunto de las herramientas seleccionadas y la forma de aplicar salvaguardas ante incidentes o amenazas de seguridad informática.

Entre los resultados obtenidos, se espera contar al terminar el proyecto con una guía completa para el funcionamiento de un CSIRT, con sus correspondientes requisitos para una futura implementación y puesta en marcha, además de pruebas de funcionamiento que demuestren su efectividad.

PALABRAS CLAVE: Análisis, Amenaza, CSIRT, Incidente de seguridad, Principios de seguridad informática.

ABSTRACT

The following applied project establishes the technical delimitation of a CSIRT as a means of analysis and response to attacks and computer vulnerabilities that occur within the community of entities served by the company Cibersecurity de Colombia LTDA, reactively and proactively, helping the entities to apply strategies and methods to detect, mitigate and eliminate threats, apply operation manuals and procedures that allow to serve as support for incidents or computer security threats, detecting and / or carrying out corrections and repairs of the system to which there are place.

The project includes in its first part, the documentation of the entire technical process of the CSIRT starting with the considerations necessary for its operation, legal regulations, IT security policies, vital operating services, level of service provision, analysis procedures, monitoring and reporting, evaluation metrics of the ANS (service level agreements), evaluation criteria and classification of incidents, hierarchical structure that the CSIRT must have, types of necessary software tools and ends with the identification of hardware and infrastructure that the CSIRT can work with.

In the second part, laboratories are carried out under virtual machines to identify the overall operation of the selected tools and how to apply safeguards against incidents or computer security threats.

Among the results obtained, it is expected to have at the end of the project a complete guide for the operation of a CSIRT, with its corresponding requirements for future implementation and commissioning, as well as operational tests that demonstrate its effectiveness.

KEY WORDS: Analysis, Threat, CSIRT, Security Incident, Computer Security Principles.

INTRODUCCIÓN

En el presente trabajo se realiza el análisis del diseño técnico para el desarrollo de un CSIRT para la empresa Cibersecurity de Colombia LTDA, identificando sus componentes, estructura e infraestructura necesaria para funcionar al igual que el personal que es requerido para brindar un óptimo nivel de servicio, ante las amenazas de seguridad informática y de seguridad de la información a las que puedan estar sometidas las entidades a las cuales les brinda sus servicios.

Se fundamenta en la necesidad de crear un centro especializado de atención a incidentes de seguridad informática en Colombia, debido al aumento desproporcionado de los ataques informáticos a los que se han venido enfrentado las entidades tanto públicas como privadas a nivel nacional, durante los primeros 6 meses del 2020 se detectaron 6.340 casos más de phishing con respecto al 2019 lo que implica un aumento del 640% y en casos de malware el aumento fue de 125% en lo que respecta a suplantación de páginas web fueron reportados 2103 casos[16] y aunque existen sistemas CSIRT en el país para control de estos incidentes, es necesario contar con más sistemas de protección debido al número de ataques[17], entre sus objetivos se establecen la delimitación tecnológica de un CSIRT funcional, con procesos y procedimientos claros para su funcionamiento, la selección de las herramientas tecnológicas necesarias para los análisis de seguridad y respuesta con los que se trabajarán, desarrollo de los acuerdos de nivel de servicios entre otros.

En las siguientes páginas se encontrará la relación detallada de los elementos necesarios para el funcionamiento de un CSIRT, abarcando no solo el aspecto técnico, sino también legal, humano y lógico a nivel del software que se puede utilizar para la identificación de amenazas y su respuesta, ya sea de tipo reactiva o proactiva.

[16]Vanguardia. «Los delitos cibernéticos se dispararon en Colombia durante la pandemia.» 20220. [en linea] https://www.vanguardia.com/area-metropolitana/bucaramanga/los-delitos-ciberneticos-se-dispararon-en-colombia-durante-la-pandemia-KJ2685268.

[17]LatinPyme. «SEGURIDAD INFORMÁTICA EN COLOMBIA POR BUEN CAMINO.» 2020. [en linea] https://www.latinpymes.com/?p=4507.

1. DEFINICIÓN DEL PROBLEMA

1.1. Antecedentes del problema.

Dado el aumento de los ataques informáticos ocurridos en el país durante el último año, donde se registraron más de 40 billones de intentos de ciberataques tanto a entidades públicas como privadas en 2019 y dentro de los cuales se ha detectado la masificación de ataques con software malicioso por medio de correo electrónico bajo la modalidad de Phishing[18], para el año 2019, la policía nacional recibió un total de 28.827 registros de ataques informático a través de los canales de atención a ciudadanos y empresas, los ataques informáticos más comunes en el país son Phishing con un 42%, suplantación de identidad con un 28%, malware con 14% y fraudes en medios de pago con el 16%, esto representa un aumento del 54% en ataques en comparación al 2018 en donde se atendieron 8.363 casos, por otra parte, uno de los delitos informáticos más denunciados en el país es el hurto a través de medios informáticos con 31.058 casos reportados seguido por la violación de datos personales con 8.037 casos, acceso abusivo a sistemas informáticos con 7.994 casos y transferencia de activos no consentido con 3.425 casos.

Las ciudades con mayor número de ataques son Bogotá con 5.308 casos, Cali con 1.190 casos, Medellín con 1.186 casos[19], para el año 2014 el 92% de incidentes cibernéticos reportados a la policía nacional estaban destinados a las personas del común, mientras que los años 2015 y 2016 fue de 63% y 57% respectivamente, mientras que los incidentes cibernéticos a entidades privadas o públicas aumentó de 5% al 28%, esto indica un aumento marcado de ataques a las entidades debido a que los cibercriminales comprendieron que era mejor a nivel de ganancias realizar un ataque más sofisticado, con mayor grado de conocimientos informáticos que un ataque más simple pero poco productivo a personas del común.[20]

Es de resaltar que, aunque existen varias entidades públicas y privadas efectuando monitoreo y atención de incidentes cibernéticos[21] Colombia todavía no está preparada para detectar un ataque de forma oportuna y enfrentar la avalancha de ciberdelitos que se presentan a diario y es necesario contar con más empresas que desarrollen métodos efectivos de detección y control.

[18]El tiempo.com. «Colombia sufrió 42 billones de intentos de ciberataques en 3 meses.» 2019. [en linea] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666.

[19]ccit.org.co. «Tendencia de cibercrimen en Colombia 2019 -2020.» 2020. [en linea] https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf.

[20]caivirtual.policia.gov.co. «Amenazas del cibercrimen en Colombia 2016 -2017.» 2017. [en linea] https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.

[21]gobierno digital. «ENTRA EN OPERACIÓN EL CSIRT DE GOBIERNO.» 2018. [en linea] https://gobiernodigital.mintic.gov.co/portal/Noticias/77743:Entra-en-operacion-el-CSIRT-de-Gobierno.

La empresa Cibersecurity de Colombia LTDA, como una organización que presta servicios de seguridad para la protección de información en el territorio nacional a entidades tanto privadas como públicas y en su afán de garantizar la seguridad de la información de sus clientes, está interesado en la creación de un centro de respuesta a incidentes cibernéticos CSIRT para responder oportunamente a los incidentes ocurridos y también para poder efectuar control de vulnerabilidades.

1.2. Formulación del problema.

Actualmente la empresa Cibersecurity de Colombia LTDA no cuenta con la plataforma tecnológica ni la infraestructura necesaria para la implementación de un CSIRT, lo que no le ha permitido prestar este servicio a sus clientes, ya sea de forma reactiva o proactiva, lo cual a su vez ha generado la no mitigación y control de las vulnerabilidades de seguridad presentes en las organizaciones y ha causado que la empresa deba enfrentar un aumento significado en los ataques informáticos a sus clientes por fallas de seguridad que se podrían evitar.

Teniendo en cuenta lo anterior se plantea la siguiente pregunta como eje temático del proyecto ¿Como elaborar el diseño técnico funcional de un CSIRT, que permita la gestión de incidentes cibernéticos para la empresa Cibersecurity de Colombia LTDA a partir del uso de la infraestructura tecnológica y herramientas lógicas necesarias?

2. JUSTIFICACIÓN

Debido al aumento de los ataques informáticos y constantes vulnerabilidades presentes en los sistemas de las organizaciones clientes de la empresa Cibersecurity de Colombia LTDA, la falta de un sistema que permita responder oportunamente a estas demandas constantes de seguridad y la necesidad inherente de proteger la información, se hace indispensable que la empresa empiece a desarrollar un plan de trabajo para la creación de un equipo de respuesta a incidentes de seguridad (CSIRT) con la capacidad de detectar ataques cibernéticos en tiempo real y que brinde herramientas de monitoreo y control para todas las entidades a nivel país.

Esto con el fin de ampliar la capacidad de reacción y disminuir el tiempo de respuesta ante un eventual ataque, que pudiera afectar las infraestructuras críticas cibernéticas de cada organización teniendo en cuenta que son sistemas fundamentales para la operación de las entidades y que pueden afectar la integridad, confidencialidad y/o disponibilidad de la información y/o que puedan hacer que los sistemas queden inutilizados, entre estos servicios se destacan, servidores, servidores de archivos, controladores de dominio, copias de respaldo de los sistemas, bases de datos y procesos del Core de negocios entre otros.

3. OBJETIVOS

3.1. Objetivo general.

Realizar el diseño técnico de un CSIRT que permita efectuar un oportuno análisis y respuesta ante incidentes cibernéticos, a través del uso de infraestructura tecnológica y herramientas lógicas dentro de la empresa Cibersecurity de Colombia LTDA.

3.2. Objetivos específicos.

Establecer los lineamientos de operación de un CISRT que permita garantizar la gestión de los incidentes de seguridad Informática presentados.

Establecer las métricas de evaluación de los posibles incidentes identificados por el CSIRT y establecer controles para una adecuada gestión.

Proponer una estructura operativa y una infraestructura funcional que permita abordar las actividades propias del CSIRT.

Diseñar ambientes controlados con una propuesta de arquitectura funcional para el desarrollo de actividades de monitoreo y control por parte del CSIRT.

4. MARCO REFERENCIAL

El presente proyecto está enfocado en establecer el diseño técnico de un CSIRT mediante el análisis de las necesidades propias de la empresa Cibersecurity de Colombia LTDA y el desarrollo de los diferentes procesos para el funcionamiento del centro de control de incidentes.

4.1. Marco teórico.

Una vez establecido la propuesta de trabajo, se tomaron algunos artículos y trabajos como referencia al proceso de diseño técnico de un CSIRT, los cuales se relacionan a continuación:

Hoy en día la seguridad de la información es un aspecto fundamental en todas las áreas de la informática, por lo que es de vital importancia establecer centros de control de amenazas y crear las condiciones de confianza para el uso de las tecnologías de la información en el país, es por esto que desde el año 2008 el ministerio de las comunicaciones (en aquel entonces) empezó a diseñar el programa de implementación de un CSIRT, tal como se plantea en el documento "diseño de un CSIRT de Colombia para la estrategia de gobierno en línea"[22] desarrollado por el área de investigación y planeación, esto demuestra el interés gubernamental por establecer métodos de control y prevención a nivel país para defenderse de forma proactiva y reactiva ante ataques a las infraestructuras críticas cibernéticas, para el año 2018 entró en funcionamiento el CSIRT diseñado e implementado por Colombia dirigido por la Policía Nacional en un complejo custodiado llamado C4 (Centro de Comando, Control, Comunicaciones y Cómputo), otras entidades que también hacen parte del sistema de monitoreo de la seguridad cibernética en el país son: el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Comando Conjunto Cibernético (CCOC), el Centro Cibernético Policial (CCP), el CSIRT de la Policía Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), su campo de acción empezó sobre 144 entidades de orden nacional.[23]

En el año 2016 Colombia adopta su segunda política de seguridad cibernética, en donde busca fortalecer las capacidades de defensa por parte del estado ante ciberataques, bajo esta nueva política se crea el rol del coordinador nacional de seguridad digital, este rol está bajo el control de la presidencia de la república, se

[22] Ministerio de comunicaciones de Colombia. «Seguridad y privacidad de la información.» 2016. [en linea] https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf.

[23] gobierno digital. «ENTRA EN OPERACIÓN EL CSIRT DE GOBIERNO.» 2018. [en linea] https://gobiernodigital.mintic.gov.co/portal/Noticias/77743:Entra-en-operacion-el-CSIRT-de-Gobierno.

crea el comité de seguridad digital y se agrega la política de ciberseguridad como parte de las operaciones estratégicas de las entidades tanto públicas como privadas.[24]

A nivel de Suramérica se destaca el BA-CSIRT de Argentina como un centro de control ante incidentes cibernéticos enfocado a los usuarios y al gobierno de la ciudad de Buenos Aires, brindando servicios proactivos y reactivos además de capacitaciones al público en general. [25]

En Perú, el PECERT o Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional creado bajo resolución ministerial RM 360-2009-PCM, sus funciones son las de coordinar en todas las entidades públicas nacionales de Perú las actividades de prevención, manejo, detección, actualización y recopilación de datos además de la puesta en marcha de soluciones ante los incidentes de ciberseguridad detectados, debe asesorar a las entidades sobre herramientas, procesos, procedimientos y técnicas de protección, debe servir como eje central de los reportes de ciber incidentes reportados y facilitar el acceso a esta información por parte de cualquier entidad además de emitir información y alertas que ayuden a mitigar los incidentes de seguridad.[26]

En Uruguay, CERTuy o Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay, su función es la protección de la infraestructura critica de del país, entre sus objetivos se destacan el centralizar, optimizar y coordinar los procesos de respuesta a los incidentes de ciber seguridad detectados. Fue creado bajo la ley No.18362 del 6 de octubre de 2008, Articulo 73, el cual crea específicamente el "Centro Nacional de Respuesta a Incidentes de Seguridad Informática" [27]

En Bolivia, se estableció en el año 2017 la ley de estrategia nacional de seguridad cibernética del país, y bajo el decreto Supremo N.º 2514 de septiembre de 2015 se crea la Agencia de Gobierno Electrónico y Tecnologías de Información y comunicación (AGETIC) cuya función principal es la implementación de las TIC y e-gobierno en el país, por otra parte bajo el mismo Decreto Supremo, se crea el Centro de Gestión de Incidentes Informáticos (CGII) para proteger los activos de

[24]BID - OEA. «RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE .» 2020. [en linea] https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.
[25]BA-CSIRT. «¿QUÉ ES BA-CSIRT?» 2020. [en linea] https://www.ba-csirt.gob.ar/index.php?u=quienes-somos.
[26]PECERT. «¿Que es el PECERT?» 2020. [En linea] https://www.pecert.gob.pe/index.php/acerca-de-nosotros/que-es-el-pe-cert.
[27]Centro Nacional de Respuesta a Incidentes de Seguridad Informática. «gub.uy.» 2020. [en Linea] https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-el-certuy.

información críticos, responder ante los ciberataques detectados y generar conciencia sobre la seguridad informática, a pesar de todo esto, Bolivia no cuenta con una legislación fuerte y específica sobre protección de datos y/o seguridad de la información.[28]

A nivel de Latinoamérica se destacan la reciente implementación del CSIRT de LACNIC (Registro de Direcciones de Internet de América Latina y Caribe), que entró en operaciones en 2020, su función es servir como un hub para la coordinación de respuestas ante incidentes cibernéticos en América latina y el caribe brindando la experiencia adquirida durando 5 años por el WARP (Warning, Advice and Reporting Point) cuya función era ser un grupo especializado en incidentes de seguridad, en este tiempo logro la capacitación de 800 profesionales en el área de la seguridad informática y atendió más de 600 incidentes de seguridad en América latina y el caribe. [29]

LACNIC debido a su función y experiencia en la región ha ingresado a formar parte de las entidades de nivel mundial con mayor renombre en el campo de la seguridad informática.[30]

Bajo el modelo de la Alianza del pacifico, el 19 de mayo de 2019, ColcERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) desarrollo y lanzo el proyecto MISP (Malware Information Sharing Platform), plataforma de intercambio de información de amenazas cibernéticas en conjunto con la OEA, el punto central de esta red está bajo gestión del CSIRT Américas de la OEA quien es el encargado de recibir y entregar información a los CSIRT nacionales, los cuales reciben información a su vez de los CSIRT sectoriales.[31]

A nivel mundial los CSIRT más importantes son:

FIRST: nace en 1990 para resolver el inconveniente de comunicación y falta de estandarización entre los diferentes CSIRT del mundo, su función es reunir la mayor cantidad de CSIRT de forma que se pueda lograr un internet seguro y confiable para

[28]BID - OEA. «RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE .» 2020. [en linea] https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.
[29]Lacnic. «LACNIC anuncia la constitución de su CSIRT.» 2020. [en linea] https://www.lacnic.net/4463/1/lacnic/lacnic-anuncia-la-constitucion-de-su-csirt.
[30]Ibid P 1
[31]ASOBANCARIA. «Alianza del pacifico: fomentando la seguridad digital a través de la cooperación.» 2019. [en linea] https://www.csirtasobancaria.com/sala-de-prensa/alianza-del-pacifico-fomentando-la-seguridad-digital-a-atraves-de-la-cooperacion.

todos, la organización FIRST proporciona recursos, plataformas, herramientas y medios para que los CSIRT puedan colaborar de forma eficiente, teniendo en cuenta su ámbito global, también brinda capacitación y un conjunto de políticas a aplicar libremente para lograr una mayor madurez a la hora de enfrentar ciberataques.[32]

FIRTS cuenta con 566 equipos CSIRT reconocidos, a nivel Colombia se encuentran los CSIRT: BS-CSIRT Centro operativo de ciberseguridad B-SECURE, C-DOC Centro de Operaciones de Defensa Cibernética, CGCSD Centro de Gobierno de Ciberseguridad y Seguridad Digital, el Grupo Evolution Technologies CGCSD, CSIRT Asobancaria CSIRT Financiero Asobancaria, CSIRT Olimpia equipo de respuesta a incidentes de seguridad informática de olimpia digital, CSIRT-CCIT Equipo de Respuesta a Incidentes de Seguridad Informática de la Cámara Colombiana de Informática y Telecomunicaciones, CSIRT-ETB Equipo de Respuesta a Incidentes de Seguridad Informática - Empresa de Telecomunicaciones de Bogotá S.A. ESP, CSIRT-MOC Newnet Equipo de respuesta a incidentes de seguridad informática de NewNet, CSIRTPONAL Equipo de Respuesta Incidente de Seguridad Informática de la Policía Nacional de Colombia, CSVD-A3Sec CSVD-A3Sec, DigiCSIRT Equipo de respuesta a incidentes de seguridad informática de DigiSOC entre otros.[33]

ENISA: European Union Agency For Cybersecurity, nace en 2004, siendo su sede principal Heraklion (Grecia), su función es ayudar a los países de la unión europea en la atención, solución y prevención a incidentes de seguridad informática, también ofrece asesoramiento a entidades públicas y privadas de la UE, incluyendo organizar ejercicios de gestión de crisis, fomentar la cooperación entre los distintos CSIRT, contribuir al desarrollo de mejores estrategias de ciberseguridad, también forma parte activa en la elaboración de las políticas y leyes de la unión europea sobre seguridad informática y de las redes.[34]

INCIBE: Instituto Nacional de Ciberseguridad de España, es una organización que depende directamente del Ministerio de Asuntos Económicos y Transformación Digital de España, es considerada un referente en temas de ciberseguridad y trasformación digital, cuenta con el INCIBE-CERT como centro de respuesta a incidentes de seguridad tanto para ciudadanos como para entidades, su misión es mejorar la seguridad, la confianza y la protección de la información desde la seguridad informática.[35]

[32]FIRST. «FIRST History.» 2020. [en linea] https://www.first.org/about/history.
[33]FIRST. «FIRST Teams.» 2020. [en linea] https://www.first.org/members/teams/.
[34]europa.eu. «gencia de la Unión Europea para la Ciberseguridad (ENISA).» 2019. [en linea] https://europa.eu/european-union/about-eu/agencies/enisa_es.
[35]Instituto Nacional de Ciberseguridad. «Que es INCIBE.» 2019. [en linea] https://www.incibe.es/que-es-incibe.

4.2. Marco conceptual.

Como se ha venido mencionando, la gestión de incidentes de seguridad está conformada por CSIRT sectorizados dentro de cada país, lo que permite que los esfuerzos requeridos para gestionar un incidente sean enfocados a un área específica, se pueden establecer diferentes CSIRT según su área de enfoque:

CSIRT para pymes: Presta servicios de seguridad de la información y asesoría a empresas pequeñas o emergentes que no tienen capacidad de crear sus propios CSIRT.[36]

CSIRT para entidades de educación: Diseñado para prestar servicios a las universidades, a sus campus virtuales y centros de desarrollo e investigación, su tamaño puede varias dependiendo del conjunto de instituciones que abarque siendo una o varias instituciones a la vez.[37]

CSIRT comercial: Diseñado para brindar servicios a empresas prestadoras de servicios comerciales, se presta el servicio a cambio de una contra prestación, se establece una relación mediante convenios llamados acuerdos de nivel de servicios.[38]

CSIRT de infraestructuras críticas: Diseñados para la protección de los activos de información vitales para una nación, no se hace distinción entre operadores públicos o privados o su área productiva, como son de distintos sectores, más de un CSIRT puede ofrecer servicios por lo que es importante establecer protocolos de comunicación entre todos los equipos relacionados.[39]

CSIRT nacionales: Se encarga de la coordinación nacional y de puente ante organizaciones internacionales para la defensa de incidentes de ciberseguridad.[40]

CSIRT de proveedores: Son CSIRT destinados a la prestación de servicios de productos específicos.[41]

[36]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.
[37]Ibid P 15
[38]Ibid P 15
[39]Ibid P 15
[40]Ibid P 15
[41]Ibid P 15

CSIRT gubernamentales: Están destinados a la protección de las entidades públicas de una nación, protegiendo tanto la infraestructura como los servicios que se prestan a los ciudadanos, estos CSIRT se adaptan a las necesidades nacionales, regionales o locales.[42]

CSIRT del sector militar: Encargados de la seguridad cibernética de las entidades militares de una nación, deben contar con conocimiento especifico de TIC para uso militar.[43]

4.3. Marco histórico.

En este apartado se presentará una breve descripción de los ataques informáticos más importantes de los últimos años y una recopilación de las amenazas más importantes a nivel de ciberseguridad.

Ataques informáticos en los últimos años.

Wikileaks: En 2010 a través de la página WikiLeaks fueron publicados más de 240.000 telegramas diplomáticos entre 250 embajadas de Estados Unidos y el Departamento de Estado de este país, exponiendo información confidencial del gobierno de Estados Unidos y sus actividades.[44]

Sony PlayStation Network: En 2011 debido a una brecha de seguridad de los servidores de Sony, fueron expuestos los datos personales y posiblemente bancarios de cerca de 77 millones de usuarios de este sistema de compra online.[45]

Stuxnet: Fue un código malicioso que afecto a la industria nuclear de Irán, este código tomó control de algunos sistemas de las plantas nucleares del país, fue tan sigiloso que solo fue posible neutralizarlo un año después.[46]

[42]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.
[43]Ibid P 1
[44]Computing. «Los 10 ciberataques más grandes de la década.» 2020. [en linea] https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-mas-grandes-de-decada.1.html.
[45]Ibid P 1
[46]IT Masters MAG. «Ciberataques que marcaron esta década.» 2019. [en linea] https://itmastersmag.com/noticias-analisis/ciberataques-que-marcaron-esta-decada/.

CtiBank: En 2011el banco informo de un ataque cibernético que comprometió las cuentas bancarias de 200.000 usuarios, los atacantes lograron acceso a la información personal de los usuarios incluyendo números de cuentas, números de tarjetas y números de seguro social.[47]

Dropbox: En 2012 el gigante de almacenamiento en la nube sufrió un ataque que dejo expuestos los correos de sus usuarios, pero hasta el 2016 se conoció que también las contraseñas de estos usuarios fueron robadas, en total fueron cerca de 68 millones de usuarios los afectados.[48]

Mirai: En 2016 el programa maligno Mirai ataco routers, cámaras IP y grabadoras digitales del proveedor de servicios Dyn esto causo un ataque de denegación de servicios masivos, afecto servicios como Twitter, PayPal, PlayStation entre otros.[49]

Amenazas a nivel de ciberseguridad.

Phishing: Los ataques de suplantación de identidad son muy comunes hoy en día, su modo de operación radica en el envío masivo de correos electrónicos falsos, estos correos tienen la apariencia de ser correos legítimos para que los usuarios no duden en abrirlos y diligenciar los datos que son solicitados, en otros casos se descarga al equipo software malicioso que permite a un atacante recopilar la información del usuario.[50]

MitM: Ataque del Hombre en el Medio, consiste en interceptar la comunicación entre dos fuentes, de esta forma el atacante puede capturar los datos e información enviados por el canal.[51]

DoS: Ataques de denegación de servicios: Estos ataques consisten en realizar múltiples solicitudes a un recurso (servidor) de esta forma se sobrepasa la capacidad del recurso para responder a las peticiones y el servicio es puesto fuera de servicio.[52]

---

[47]IT Masters MAG. «Ciberataques que marcaron esta década.» 2019. [en linea] https://itmastersmag.com/noticias-analisis/ciberataques-que-marcaron-esta-decada/.
[48]Computing. «Los 10 ciberataques más grandes de la década.» 2020. [en linea] https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-mas-grandes-de-decada.1.html.
[49]IT Masters MAG. «Ciberataques que marcaron esta década.» 2019. [en linea] https://itmastersmag.com/noticias-analisis/ciberataques-que-marcaron-esta-decada/.
[50]Infocyte. «Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks.» 2021. [en linea] https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/.
[51]Ibid P 1
[52]Ibid P 1

SQL Injection: Este tipo de ataque consiste en insertar código arbitrario en una consulta legitima de SQL que no ha sido debidamente optimizada, de esta forma el atacante obtiene información relevante para un ataque mayor o para ingresar a los datos almacenados en las tablas de la base de datos.[53]

Explotación de día 0: Consiste en explotar una vulnerabilidad que no ha sido reportada o que fue reportada pero aún no cuenta con un parche de seguridad para solucionarla por lo que estos ataques solo pueden ser prevenidos por una supervisión constante.[54]

Rootkits: Se alojan dentro de software legal, al descargarse al equipo, se instala automáticamente y permanece en estado inactivo hasta que el atacante envía una instrucción para activarlo, una vez activo permite el acceso a la información contenida en el equipo.[55]

4.4. Marco legal.

Para el diseño del CSIRT se tomaron en cuenta las normas y leyes siguientes para determinar el marco legal a aplicar.

La ley 1273 de 2009 "de la protección de la información y de los datos".

Establece la reglamentación legal para los delitos que se cometan contra los tres pilares de la seguridad de la información, estos son: integridad, disponibilidad y confidencialidad.[56]

Establece los siguientes delitos:

Artículo 269A: Acceso abusivo a un sistema informático: Determina la pena privativa de la libertad en 48 a 96 meses y una sanción económica de 100 a 1000 salarios mínimos legales vigentes para aquellas personas que ingresen de forma fraudulenta y/o sin autorización a un sistema informático o se mantenga dentro del sistema sin autorización expresa del dueño del sistema.

[53]Infocyte. «Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks.» 2021. [en linea] https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/.
[54]Ibid P 1
[55]Infocyte. «Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks.» 2021. [en linea] https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/
[56]Secretaria del Senado. «LEY 1273 DE 2009.» 2021. [en linea] http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: Determina la pena privativa de la libertad en 48 a 96 meses y una sanción económica de 100 a 1000 salarios mínimos legales vigentes para aquellas personas que de forma deliberada se interpongan al correcto y normal funcionamiento, acceso a un sistema informático o de telecomunicación y a la información contenida en él

Artículo 269C: Interceptación de datos informáticos: Determina la pena privativa de la libertad en 36 a 72 meses para aquellas personas que sin autorización judicial logren interceptar información desde, hacia o en el interior de un sistema de información o en su defecto intercepte las ondas electromagnéticas que provienen de un sistema informático

Artículo 269D: Daño Informático: Determina la pena privativa de la libertad en 48 a 96 meses y una sanción económica de 100 a 1000 salarios mínimos legales vigentes para aquellas personas que destruyan, modifiquen o borren al grado de dejar inutilizable la información o un sistema informático.

Artículo 269E: Uso de software malicioso: Determina la pena privativa de la libertad en 48 a 96 meses y una sanción económica de 100 a 1000 salarios mínimos legales vigentes para aquellas personas que se encarguen de diseñar, destruir, enviar o vender software malicioso o cualquier otro tipo de software que pueda producir daños a un sistema informático o de telecomunicaciones.

Artículo 269F: Violación de datos personales: Determina la pena privativa de la libertad en 48 a 96 meses y una sanción económica de 100 a 1000 salarios mínimos legales vigentes para aquellas personas que sin previa autorización obtengan, manipulen, vendan, compren o publiquen la información personal contenida en sistemas informáticos, archivos, bases de datos y/o cualquier otro medio de transmisión.

Artículo 269G: Suplantación de sitios web para capturar datos personales: Determina la pena privativa de la libertad en 48 a 96 meses y una sanción económica de 100 a 1000 salarios mínimos legales vigentes para aquellas personas que diseñan páginas web, correos, enlaces o cualquier tipo de herramienta que capture datos confidenciales de los usuarios sin su autorización para fines extorsivos o fraude.

Establece varios agravantes que aumentan las penas privativas de la libertad y establece sanciones de inhabilidad para cargos competentes a la profesión.

Las penas impuestas serán aumentadas en una tercera parte cuando los recursos tecnológicos o de telecomunicaciones afectados pertenezcan al estado, al Sena o entidades oficiales, grupos financieros, entidades o estados extranjeros y nacionales. Cuando el directamente responsable es un funcionario público que se encuentra laborando, en condiciones cuando se demuestre abuso de confianza hacia el dueño de la información, cuando se revele información de tipo personal o confidencial y que cause daño o perjuicio a otro o cuando se genere una alarma de seguridad nacional o se use la información o los ataques con fines terroristas.[57]

Bajo el capítulo 2, se regulan los atentados informáticos:

Artículo 269I: Hurto por medios informáticos y semejantes: Uso de la tecnología para hurtar información, datos privados o de cualquier clase manipulando sistemas informáticos, redes, sistemas de autenticación o suplantando usuarios.

Artículo 269J: Transferencia no consentida de activos: Determina la pena privativa de la libertad en 48 y 120 meses y una sanción económica de 200 a 1500 salarios mínimos legales vigentes para aquellas personas que mediante el uso o manipulación de un sistema informático puedan realizar transferencia sin permiso de cualquier dato o información de valor en perjuicio de otra persona y con fines lucrativos.

Ley 1266 de 2008: "ley de Habeas Data", permite a los ciudadanos conocer y actualizar la información que las entidades tienen sobre ellos mismos, su ámbito se refiere a la recolección, tratamiento y circulación de los datos personales, así como al derecho a la información consagrado en el artículo 20 de la constitución política de Colombia.[58]

Circular 007 de 2018: Por la cual la superintendencia financiera establece a las entidades sobre las cuales hace control la obligación de informar a sus usuarios sobre todo tipo de incidente de seguridad informática en sus plataformas de pago.[59]

Ley 1928 de 2018: Por la cual el Congreso de la republica ratifica el convenio firmado en la ciudad de Bucarest sobre ciberdelincuencia, este convenio compromete a los estados firmantes a establecer políticas y normas penales,

[57]Secretaria del Senado. «LEY 1273 DE 2009.» 2021. [en linea] http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.
[58]Secretaria del Senado. «LEY ESTATUTARIA 1266 DE 2008.» 2008. [en linea] http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.
[59]Superfinanciera. «Superfinanciera fortalece la protección de la información .» 2018. [en linea] https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00.

además de cooperación internacional en temas relacionados con la ciberdelincuencia.[60]

Documento CONPES 3854 de 2016: Establece la política de seguridad digital a aplicar por el gobierno de Colombia, tanto para los ciudadanos como para las entidades en donde deben realizar un análisis de riesgos de seguridad informática de modo que puedan responder ante un ataque.[61]

A partir de esta información se establece la importancia de la creación de un CSIRT que permita dar atención oportuna a los incidentes de seguridad informática para la empresa Cibersecurity de Colombia.

[60]Secretaria del Senado. «LEY 1928 DE 2018.» 2018. [en linea] http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html.
[61]DEPARTAMENTO NACIONAL DE PLANEACIÓN . 2017. [en linea] https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf.

5. DISEÑO METODOLÓGICO

El proyecto se desarrollará de forma teórico/práctico con la elaboración de la documentación sobre el proceso de delimitación técnica de un CSIRT, y de forma práctica con la aplicación de algunas pruebas de laboratorio en máquinas virtuales, las cuales permitirán el desarrollo de algunas de las funcionalidades técnicas más importantes de un CSIRT.

Se emplea Metodología para evaluación, diagnóstico y diseño de procesos, en la cual se abarcan 4 ejes fundamentales:[62]

Conocimiento, interpretación, análisis y diseño.[63]

Etapa 1, Conocimiento: En esta etapa se realiza la consulta en fuentes documentales y de internet sobre los CSIRT, como nacen, cuáles son los más importantes, como funcionan, como están conformados, se realiza consulta sobre las diferentes normas y leyes que pueden ser aplicadas al funcionamiento de un CSIRT en Colombia, también se examina el estado de los CSIRT en América latina y el caribe.

Etapa 2, interpretación: En esta etapa se validan las fuentes de información seleccionando las más relevantes, se contrapone la información con otras fuentes y de ser necesario se realizan nuevas búsquedas que permitan ampliar el horizonte de información de manera tal que se tengan todos los datos y criterios para el desarrollo del trabajo.

Etapa 3, análisis: En esta etapa se verifica que información es pertinente aplicarla en el desarrollo del trabajo, teniendo en cuenta a que pertenecen a otros países, se aplican otras leyes, la metodología de trabajo es distinta, se busca tener un punto intermedio entre los CSIRT internacionales y los requerimientos propios de un CSIRT para las entidades del país.

Etapa 4, Diseño: En esta etapa se establece el alcance del CSIRT, diseño funcional, lógico, esquemas de red, políticas, servicios y procedimientos además de los requisitos de software y hardware con los que trabajara el CSIRT, se realizan los laboratorios controlados para verificar la funcionalidad del software seleccionado.

[62]Herrera Monterroso, Harold Eduardo. «gestiopolis.» *Metodología para evaluación, diagnóstico y diseño de procesos.* 2007. [en linea] https://www.gestiopolis.com/metodologia-para-evaluacion-diagnostico-y-diseno-de-procesos/.
[63]Ibid P 1

6. LINEAMIENTOS DE OPERACIÓN DE UN CISRT

6.1. Función de un CSIRT.

Antes de entrar en materia con el diseño técnico del CSIRT, es importante saber que es un CSIRT, la Agencia Europea para la seguridad cibernética (ENISA) define un CSIRT como “Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática)”, es decir, un grupo de especialistas en seguridad informática capaz de dar respuesta a incidentes de seguridad informática.

Debido a que existen diferentes tipos de CSIRT, es necesario decir que el alcance está definido por su ámbito, es decir un CSIRT académico se limitara a dar apoyo y soporte proactivo y reactivo solo a centros de educación.

Adicional a la gestión que prestan sobre los incidentes de seguridad también ofrecen servicios como la asistencia para identificar, mitigar y controlar riesgos, prestan servicios de análisis forense luego de registrarse un problema de seguridad de la información.

Entre las ventajas del uso de los CSIRT se encuentran la siguientes:

Tener un equipo especializado en cuestiones de seguridad de la información en periodos 7x24.

Tener servicios especializados en cuestiones de seguridad de la información.

Tener reacción inmediata ante incidentes de seguridad de la información.

Coordinación centralizada de las acciones correctivas o preventivas como respuesta a los incidentes ocurridos.

Establece un control sobre las normas y legislación vigente sobre seguridad de la información.

Mejora la forma en que se enfrentan los incidentes de seguridad de la información.[64]

6.2. Alcance del CSIRT.

El alcance del CSIRT para la empresa Cibersecurity de Colombia LTDA está dada como un CSIRT comercial, siendo una entidad prestadora de servicios bajo modalidad de acuerdos de servicios o ANS, tanto para entidades públicos y/o privadas, grandes, medianas y pequeñas empresas.

Esto debido a que el CSIRT estará en capacidad de atender de forma proactiva y/o reactiva los incidentes de ciberseguridad que se puedan presentar, como parte del servicio ofrecido la empresa Cibersecurity de Colombia LTDA deberá trabajar en conjunto con las áreas de tecnología de la información de las diferentes entidades contratantes en temas sobre seguridad informática y de esta forma contribuir a la mejora de la seguridad limitando los incidentes presentados.

También se presenta dentro del alcance el catálogo de servicios ya sean de tipo proactivo o reactivo, estema de red inicial de operación del CSIRT, esquema organizacional, políticas y procedimientos de operación básicos teniendo en cuenta que las políticas y procedimientos se adaptan al modelo estratégico de cada entidad y por último se desarrollan laboratorios para verificar la funcionalidad del software base seleccionado para el inicio del operativo del CSIRT.

6.3. Políticas y procedimientos del CSIRT.

Todo CSIRT debe estar alineado bajo políticas institucionales que definan cómo y bajo qué principios operar, estas directrices son de cumplimiento estricto por el personal que operará el CSIRT y deben garantizar que la información está resguardada bajo los tres pilares de la seguridad informática, estos son confidencialidad, disponibilidad e integridad.

Para todos los CSIRT en el mundo existen un conjunto de políticas mínimas que han sido establecidas por la organización FIRST, entre ellas se establecen:

[64]enisa csirt. «Cómo crear un CSIRT paso a paso.» 2006. [en linea]. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-n9P4muDvAhXwEVkFHfN3A_4QFjAAegQIAxAD&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcsirt-setting-up-guide-in-spanish%2Fat_download%2FfullReport&usg=AOvVaw2F8Wp_02LEvZ-NMA.

Políticas de clasificación de información: La OEA define esta política como" la forma en que el CSIRT clasifica la información basada en distintos niveles de criticidad".[65]

Política de protección de datos: Definido por la OEA como "la forma de proteger la información de acuerdo con su criticidad"[66]

Política de retención de información: Definido por la OEA como "el tiempo que el CSIRT debe mantener registros u otra información de que disponga".[67]

Política de destrucción de información: Definido por la OEA como "cómo el CSIRT destruye información, registros, medios, dispositivos, etc., para garantizar que la información esté protegida cuando su ciclo de vida o los medios que lo contienen llegan a su fin".[68]

Política de divulgación de información: La OEA la define como "la especificación de cómo y cuándo el CSIRT puede compartir o distribuir la información interna o externamente".[69]

Política sobre el acceso a la información: Esta política está definida por la OEA como "quién puede acceder a la información del CSIRT, teniendo en cuenta el personal, miembros de la comunidad objetivo o el personal de la organización matriz del CSIRT (si lo tiene)".[70]

Políticas de uso apropiado de los sistemas del CSIRT: En esta política la OEA define "el uso aceptable de los sistemas y recursos del CSIRT".[71]

Definición de incidentes de seguridad y política de eventos: Según la OEA esta política debe "describir los criterios que determinan la definición de un evento o incidente de seguridad y la clasificación de cada uno según el tipo y la gravedad".[72]

---

[65]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.
[66]Ibid P 81
[67]Ibid P 81
[68]Ibid P 81
[69]Ibid P 81
[70]Ibid P 81
[71]Ibid P 81
[72]Ibid P 81

Política de gestión de incidentes: La OEA la establece como “la definición de cómo se lleva a cabo la gestión de incidentes, incluyendo el tipo de incidentes a los que el CSIRT responderá, el tiempo de respuesta aceptables, los procedimientos que se van a aplicar, etcétera”.[73]

Política de cooperación: La OEA establece que esta política “define las otras entidades con las que cooperará el CSIRT y cómo lo harán, particularmente otros equipos de respuesta a incidentes”.[74]

Políticas adicionales para implementar:

Política de gestión de riesgo: Esta política establece que se debe identificar la probabilidad de que un riesgo se materialice y así poder minimizarlo sin afectar procesos críticos.[75]

Política de responsabilidad de la información: Establece mecanismos de control de la información para garantizar el acceso a la misma por los usuarios debidamente autorizados.[76]

Política de seguridad en comunicaciones: Debe garantizar la confidencialidad, disponibilidad e integridad de la información enviada o recibida por redes privadas o públicas.[77]

Política de control de acceso: Encargada de definir los controles de acceso a todos los sistemas, define tipo de contraseña, periodo de caducidad entre otros.[78]

Política de gestión de incidentes: Establece procesos y procedimientos para el reporte de los incidentes de seguridad detectados.[79]

[73]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2006. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.
[74]Ibid P 81
[75]Universidad Técnica Particular de Loja. «Manual de Políticas Institucionales.» 2011. [en linea] https://csirt.utpl.edu.ec/sites/default/files/files/ManualPoliticas.pdf.
[76]Ibid P 81
[77]Ibid P 81
[78]Ibid P 81
[79]Universidad Técnica Particular de Loja. «Manual de Políticas Institucionales.» 2011. [en linea] https://csirt.utpl.edu.ec/sites/default/files/files/ManualPoliticas.pdf.

Política de cumplimiento: Establece el cumplimiento con la normatividad legal y obligaciones contractuales.[80]

Otras políticas:

Política de uso de Internet.[81]
Política de notificación de incidentes.[82]
Política de comunicación del CSIRT.[83]
Política de capacitación y entrenamiento.[84]
Política de seguridad de computador personal.[85]
Política de seguridad de la red. [86]
Política de uso de correo electrónico.[87]
Política de uso de dispositivos móviles.[88]
Política de seguridad de equipo de telecomunicaciones.[89]
Política de copias de seguridad.[90]
Política de segregación de funciones.[91]
Política de control de cambio.[92]
Política de contraseñas.[93]

Todas estas políticas deben ser aplicadas por el CSIRT una vez esté operando para garantizar el manejo de la información, además se deben crear nuevas políticas o adaptarse a las políticas de seguridad establecidas por cada entidad miembro del grupo a las que se les prestara servicio.

Dentro de los procesos y procedimientos establecidos para el CSIRT se encuentran:

Monitoreo de la red corporativa verificando el correcto uso de los recursos, se solicitará reportes de eventos a los encargados de administrar los sistemas de la organización.

[80] Ibid P 114
[81]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2006. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.
[82]Ibid P 81
[83]Ibid P 81
[84]Ibid P 81
[85]Ibid P 81
[86]Ibid P 81
[87]Ibid P 81
[88]Ibid P 81
[89]Ibid P 81
[90]Ibid P 81
[91]Ibid P 81
[92]Ibid P 81
[93]Ibid P 81

Revisión de registros de auditoría de la infraestructura buscando posibles eventos de seguridad.

Aplicación de actualizaciones mensuales y desinstalación de aplicaciones obsoletas que generen riesgos de seguridad.

Control de acceso a datacenter.

Control de cambios en el datacenter.[94]

Proceso de capacitación de los funcionarios en temas relacionados con la seguridad de la información, estableciendo periodicidad mensual.[95]

Verificación, control y auditoría de los procesos internos de las organizaciones para la desactivación de usuarios en DA (directorio activo) y en los sistemas de información.

Centralización de las peticiones de soporte de seguridad informática para su correcta asignación en el CSIRT.

Establecimiento de los canales de solicitud de incidentes.

Establecimiento de los niveles de advertencia según riesgo, peligrosidad e impacto, estableciendo advertencias de tipo crítico, muy alto. Alto, medio y bajo.

Creación del equipo CSIRT determinando los miembros de la dirección y el personal necesario para su operación.[96]

[94]Contraloria de Bogotá. «PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMATICA.» 2018 [en linea] . http://www.contraloriabogota.gov.co/sites/default/files/Contenido/Normatividad/Resoluciones/2018/RR_047_2018%20Adopta%20y%20Actualiza%20Procedimientos%20que%20Conforman%20el%20PGTI%20en%20la%20Contralor%C3%ADa%20de%20Bogot%C3%A1%20D.C/PGTI-06%20Proced%20G.

[95]Estado Libre Asociado de Puerto Rico. «Políticas y Procedimientos de Seguridad Informática.» 2015. [en linea] https://www.de.pr.gov/wp-content/uploads/2014/09/Politicas_y_procedimientos_de_seguridad_PUBLICADO.pdf.

[96]Contraloria de Bogotá. «PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMATICA.» 2018 [en linea] . http://www.contraloriabogota.gov.co/sites/default/files/Contenido/Normatividad/Resoluciones/2018/RR_047_2018%20Adopta%20y%20Actualiza%20Procedimientos%20que%20Conforman%20el%20PGTI%20en%20la%20Contralor%C3%ADa%20de%20Bogot%C3%A1%20D.C/PGTI-06%20Proced%20G.

Se establece tarea automatizada de copia de respaldo de la información que se encuentra en las bases de datos.

6.4. Relaciones entre diferentes CSIRT y medios de comunicación.

Debido a la cantidad de CSIRT que existen, es importante establecer relaciones de confianza que permitan mejorar el manejo de los incidentes de ciberseguridad, en este sentido, en el país existen cerca de 12 CSIRT activos, de los cuales se establecerá relación con los más importantes, estos son:

Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT)

Comando Conjunto Cibernético (CCOC)

Centro Cibernético Policial (CCP)

Equipo de Respuesta Incidente de Seguridad Informática de la Policía Nacional de Colombia (CSIRTPONAL)

CSIRT Financiero

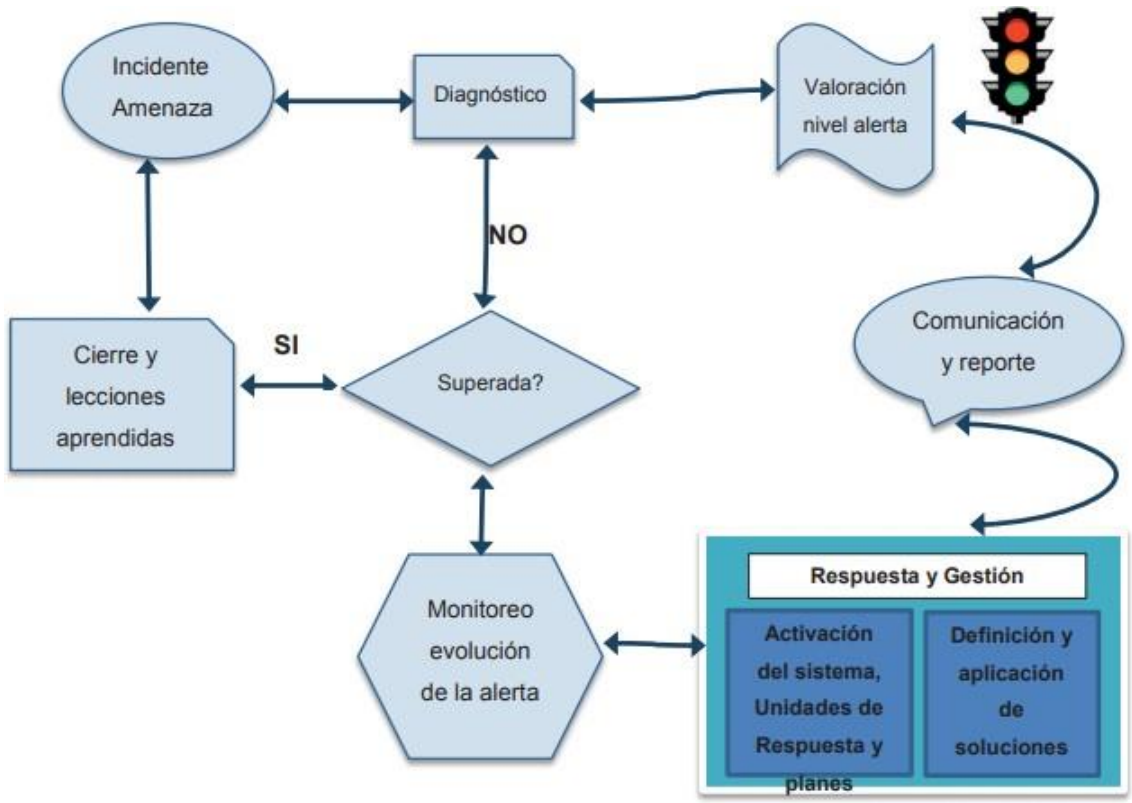
Además, se forma alianzas estratégicas con los siguientes CSIRT especializados por ser proveedores de servicios de internet:

Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-ETB)

SOC Team Claro Colombia

Todo proceso de detección, atención y declaración de una emergencia de seguridad cibernética es considerado de tipo cíclico, lo que permite establecer el nivel de atención al incidente y activar los recursos necesarios para su atención.

Ilustración 1 Pasos del proceso de atención de un incidente.



Fuente: MINISTERIO DE DEFENSA. Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia.[97]

Como punto de coordinación ante estos ataques, se debe realizar comunicación con ColCERT que forma parte del ministerio de defensa, al igual que con los CSIRT de la policía nacional para que realicen las investigaciones necesarias.

6.5. Servicios que prestara el CSIRT.

Los servicios del CSIRT están divididos en 3 grandes grupos, estos son: servicios reactivos, servicios proactivos y servicios de valor agregado.[98]

[97]Ministerio de defensa. «Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia.» 2017. [en linea] file:///C:/Users/Ivan/AppData/Local/Temp/MicrosoftEdgeDownloads/8e193f78-95bf-4dce-8122-c6a23dd82fff/PLAN_PUBLICO.pdf.
[98]Lanfranco, Lic. Einar. «CSIRTs, ¿De qué se trata?, modelos posibles» 2016. [en linea] https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf.

Servicios reactivos: Estos servicios son los encargados de responder ante una petición de un incidente o cualquier amenaza de seguridad cibernética, es posible iniciar el proceso por solicitud de terceras partes, por la revisión de los controles implementados o por sistemas de detección de intrusos.[99]

Servicios proactivos: Son los diseñados para mejorar la infraestructura de la organización al igual que los procesos de seguridad antes de que se detecte o produzca un incidente, su objetivo principal es reducir el impacto y alcance del incidente.[100]

Los servicios proactivos se configuran en dos niveles:

Nivel 1: Dentro de este nivel se presta el servicio de monitoreo y generación de alertas, aplicación de herramientas para identificar eventos en los sistemas de las organizaciones a las que se les presta servicio.[101]

Nivel 2: Seguimiento constante a la infraestructura de las organizaciones por medio de controles configurados.[102]

Servicios de valor agregado: Planes de capacitación y concientización de los usuarios.

Alertas y advertencias: Son los encargados de la difusión de la información sobre un ataque, vulnerabilidad o alerta y recomienda acciones para tener en cuenta, esta información puede ser creada por otros CSIRT o por el mismo prestador del servicio.[103]

A continuación, se especifican los servicios que prestará el CSIRT

[99]Enisa csirt. «Cómo crear un CSIRT paso a paso.» 2006. [en linea]. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-n9P4muDvAhXwEVkFHfN3A_4QFjAAegQIAxAD&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcsirt-setting-up-guide-in-spanish%2Fat_download%2FfullReport&usg=AOvVaw2F8Wp_02LEvZ-NMA.
[100]Ibid P 72
[101]OEA. «Buenas Prácticas para establecer un CSIRT nacional .» 2006. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.
[102]Ibid P 72
[103]OEA. «Buenas Prácticas para establecer un CSIRT nacional .» 2006. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

Tabla 1 Listado de Servicios a prestar en el CSIRT.

Servicios reactivos	Servicios proactivos	Manejo de instancias	Servicios de valor agregado
*Alertas y advertencias * Tratamiento de incidentes *Análisis de incidentes Respuesta a incidentes in situ *Apoyo a la respuesta a incidentes *Apoyo a la respuesta a incidentes *Apoyo a la respuesta a incidentes * Análisis de la vulnerabilidad * Respuesta a la vulnerabilidad * Coordinación de la respuesta a la vulnerabilidad	*Comunicados *Observatorio de tecnología *Evaluaciones o auditorías de la seguridad * Configuración y mantenimiento de la seguridad * Desarrollo de herramientas de seguridad * Servicios de detección de intrusos * Difusión de información relacionada con la seguridad	*Análisis de instancias * Respuesta a las instancias * Coordinación de la respuesta a las instancias	* Análisis de riesgos respuesta a las instancias * Continuidad del negocio y recuperación tras un desastre * Consultoría de seguridad * Sensibilización * Educación / Formación * Evaluación o certificación de productos

Fuente: Guía de seguridad. Guía de creación de un CERT/CSIRT. {En línea}. {consultado el 12 de enero de 2020} disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Guia_Creacion_CERT-CSIRT.pdf.

Dentro del manual de buenas prácticas de la OEA se establece que los servicios reactivos son considerados como los más importantes, esto es debido a que estos servicios son los encargados de responder ante cualquier tipo de ataque.[104]

[104]OEA. «Buenas Prácticas para establecer un CSIRT nacional .» 2006. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

6.6. Notificación de Incidentes.

La gestión de los incidentes y de respuesta es considerada como la actividad principal de todo CSIRT y en este caso no será la excepción, es por esto por lo que se establecieron los siguientes procesos:

Identificación de eventos relacionados con incidentes de seguridad y que estén alineados con los acuerdos de nivel de servicios, estos eventos pueden ser el resultado del monitoreo constante de los sistemas o reportados por distintos medios.[105]

Capacidad para determinar qué incidente de seguridad es considerado falso positivo, interesante o irrelevante.[106]

Llevar control de los incidentes registrados en la plataforma destinada para tal fin teniendo control de quien reporta el incidente, área, nombre, cargo.[107]

Se establece proceso para determinar qué acciones seguir en nivel dos de soporte:[108]

Hay que confirmar que no se trata de un falso positivo.

Verificar la información recibida con la información de los sistemas.

Crear servicios padre-hijo o uno nuevo según sea el caso.

Clasificar el incidente según la clasificación establecida.

[105]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.
[106]Ibid P 27
[107]Ibid P 27
[108]Ibid P 27

Asignación del servicio (caso) al personal correspondiente.

priorización según sea el caso.

Una vez el incidente sea atendido, se procederá a realizar seguimiento y cierre, durante la fase de seguimiento se hará contención de los posibles daños, si el incidente de seguridad lo amerita se deberá notificar a los distintos CSIRT con que se tiene comunicación para reportar el evento.

Todo incidente debe estar asociado a un nivel de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Tabla 2 Criterios de advertencia de incidentes según su impacto.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES		
Nivel	**Clasificación**	**Tipo de incidente**
CRÍTICO	Otros	APT
MUY ALTO		Distribución de malware
	Código dañino	Configuración de malware
	Intrusión	Robo
		Sabotaje
	Disponibilidad	Interrupciones
ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones
		Compromiso de cuentas con privilegios
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información

		Pérdida de datos
	Fraude	Phishing
MEDIO	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas
		Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas sin privilegios
	Disponibilidad	Mala configuración
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
BAJO	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)
	Otros	Otros

Fuente: Guía de seguridad. Guía de creación de un CERT/CSIRT. {En línea}. {consultado el 12 de enero de 2020} disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Guia_Creacion_CERT-CSIRT.pdf.

El CSIRT debe realizar análisis de vulnerabilidades constantemente tanto de hardware como de software, esto con el fin de encontrar las vulnerabilidades y repararlas lo más pronto posible, es función del CSIRT realizar evaluaciones constantes de infraestructura, prueba de penetración, escaneo de la red y auditorías internas de seguridad de la información.[109]

[109]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.

Los incidentes que estén clasificados dentro de los niveles CRÍTICO, MUY ALTO, ALTO deben tener notificación automática obligatoria para su atención inmediata, para facilitar su identificación y clasificación, los incidentes cuentan con una taxonomía.

Ilustración 2 Clasificación/taxonomía de los ciberincidentes

CLASIFICACIÓN/TAXONOMÍA DE LOS CIBERINCIDENTES		
Clasificación	**Tipo de incidente**	**Descripción y ejemplos prácticos**
	Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
Contenido abusivo	Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
Contenido dañino	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
	Sistema infectado	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit.
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.
Obtención de información	Escaneo de redes (scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.

	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Intrusión	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
	Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.
Disponibilidad	DoS (Denegación de servicio)	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural.
Compromiso de la información	Acceso no autorizado a información	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.
Vulnerable	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
	Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de

		ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Fuente: Guía de seguridad. Guía de creación de un CERT/CSIRT. {En línea}. {consultado el 12 de enero de 2020} disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Guia_Creacion_CERT-CSIRT.pdf.

El CSIRT debe realizar análisis de vulnerabilidades constantemente tanto de hardware como de software, esto con el fin de encontrar las fallas y posibles incidentes de seguridad lo más pronto posible, también debe realizar evaluaciones constantes de infraestructura, pruebas de penetración, escaneo de la red y auditorías internas de seguridad de la información.[110]

[110]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.

7. METRICAS DE EVALUACIÓN Y ESTABLECIMIENTO DE CONTROLES.

Para evaluar la capacidad de respuesta del CSIRT se establecen las siguientes tablas de métricas e indicadores, estas tablas pertenecen a la Guía Nacional de Notificación y gestión de ciber incidentes de España[111] y son tomadas como referencia para su uso.

La función de las métricas es permitir contar con información cuantificable sobre el estado de implantación del sistema de gestión de incidentes dentro del CSIRT, esto para obtener una imagen real sobre la capacidad que se tiene para atender efectivamente los incidentes de seguridad reportados y descubiertos en las organizaciones a las que se les prestara servicio.

7.1. Métrica de Implantación.

La métrica de implantación es una de las más importantes al permitir determinar el estado real de implantación del sistema de gestión de incidentes dentro del CSIRT, esto permite brindar la atención requerida a los incidentes reportados y descubiertos durante los análisis realizados.

Esta métrica busca como objetivo identificar si todos los sistemas de información forman parte del servicio mediante el conteo de los servicios que se encuentran controlados.

[111]INCIBE. «Guía nacional de notificación y gestión de ciberincidentes.» 2020. [en linea] https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes.

Tabla 3 Descripción de la métrica de implantación

M1	**Indicador**	Alcance del sistema de gestión de incidentes	
	Objetivo	Saber si todos los sistemas de información están adscritos al servicio.	
	Método	Se cuentan cuántos servicios están bajo control. (Si se conociera cuántos servicios hay en total, se podría calcular un porcentaje). # servicios imprescindibles para la organización.# servicios importantes para la organización.	
	Caracterización	Objeto	100%
		Umbral amarillo	Imprescindibles: 4/5 (80%) Importantes: 2/3 (67%)
		Umbral rojo	Imprescindibles: 2/3 (67%) Importantes: 1/2 (50%)
		Frecuencia medición	Trimestral
		Frecuencia reporte	Anual

Fuente: Guía de seguridad. Guía de creación de un CERT/CSIRT. {En línea}. {consultado el 12 de enero de 2020} disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Gui

7.2. Métricas de resolución de incidentes.

Esta métrica mide el comportamiento sobre la gestión de incidentes clasificados con impacto ALTO / MUY ALTO / CRITICO que han sido resueltos.

Tabla 4 Métrica de resolución

M2	**Indicador**	Resolución de ciberincidentes de nivel de impacto ALTO / MUY ALTO / CRÍTICO	
	Objetivo	Ser capaces de resolver prontamente incidentes de alto impacto.	
	Método	Se mide el tiempo que se tarda en resolver un incidente con un alto impactoen sistemas de la organización: desde que se notifica hasta que se resuelve. T(50) tiempo que se tarda en cerrar el 50% de los incidentesT (90) tiempo que se tarda en cerrar el 90% de los incidentes	
	Caracterización	Objeto	T(50) = 0 && T(90) = 0
		Umbral amarillo	T(50) > 4d || T(90) > 5d
		Umbral rojo	T(50) > 14d || T(90) > 18d
		Frecuencia mediación	Anual
		Frecuencia reporte	Anual

M3	**Indicador**	Resolución de ciberincidentes de nivel de impacto BAJO / MEDIO	
	Objetivo	Ser capaces de resolver prontamente incidentes de impacto medio.	
	Método	Se mide el tiempo que se tarda en resolver un incidente con un impacto en sistemas de la organización: desde que se notifica hasta que se resuelve. T(50) tiempo que se tarda en cerrar el 50% de los incidentes T(90) tiempo que se tarda en cerrar el 90% de los incidentes	
	Caracterización	Objeto	T(50) = 0 && T(90) = 0
		Umbral amarillo	T(50) > 10d || T(90) > 30d
		Umbral rojo	T(50) > 15d || T(90) > 45d
		Frecuencia medición	Anual
		Frecuencia de reporte	Anual

Fuente: Guía de seguridad. Guía de creación de un CERT/CSIRT. {En línea}. {consultado el 12 de enero de 2020} disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Gui

7.3. Métricas de gestión de incidentes.

Esta métrica mide el comportamiento de los incidentes cerrados indicando el tiempo que se demoró en su cierre, su objeto es garantizar la gestión sobre los incidentes de alta peligrosidad.

Tabla 5 Métricas gestión de incidentes

M5	**Indicador**	Estado de cierre los incidentes	
	Objetivo	Ser capaces de gestionar incidentes de seguridad	
	Método	Se mide el número de incidentes que han sido cerrados sin respuesta. Fórmula: # incidentes de seguridad cerrados sin respuesta / # total de incidentes notificados	
	Caracterización	Objeto	<10%
		Umbral amarillo	20%
		Umbral rojo	50%
		Frecuencia mediación	Trimestral
		Frecuencia reporte	Anual
	Indicador	Estado de cierre los incidentes de peligrosidad MUY ALTA/ CRÍTICA	
	Objetivo	Ser capaces de gestionar incidentes de seguridad de alta peligrosidad	

M6	**Método**	Se mide el número de incidentes que han sido cerrados sin respuesta. Fórmula: # incidentes de seguridad cerrados sin respuesta / # total deincidentes notificados	
	Caracterización	Objeto	0%
		Umbral amarillo	5%
		Umbral rojo	20%
		Frecuencia medición	Trimestral
		Frecuencia reporte	Anual

Fuente: Guía de seguridad. Guía de creación de un CERT/CSIRT. {En línea}. {consultado el 12 de enero de 2020} disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Gui

Existen varias métricas que también pueden ser implementadas como parte del proceso de control y seguimiento sobre la gestión de incidentes de seguridad, a continuación, se relacionan algunas de ellas.

Tabla 6 Métricas de evaluación

Descripción	Métrica
Mantenimiento de la Calidad del Servicio	Número de incidentes de severidad Alta (total y por categoría) Número de incidentes severidad Mediana y Baja
	Número de otros incidentes
	Número de incidentes incorrectamente categorizados Número de incidentes incorrectamente escalado Número de incidentes que no pasaron por el Help Desk
	Número de incidentes que no fueron cerrados/resueltos sobre las horas
	Número de incidentes resueltos antes de que el usuario notifique Número de incidentes abiertos nuevamente.
Mantenimiento de satisfacción al cliente	Número de usuarios/clientes encuestas enviadas Número de encuestas respondidas
	Promedio de puntaje encuesta a usuario (total o por categoría de pregunta)
	Promedio de tiempo de espera antes de la respuesta al incidente
Resolución de incidentes en los tiempos establecidos	Número de incidentes registrados
	Número de incidentes resueltos por Help Desk

	Número de incidentes intensificados por Help Desk
	Tiempo promedio para restablecer el servicio desde la primera llamada Tiempo promedio para restaurar la severidad del incidente
	Tiempo promedio para restaurar la urgencia del incidente

Fuente: Roberto, Andrade. Fuertes, Walter. «DISEÑO Y DIMENSIONAMIENTO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT). CASO DE ESTUDIO: ESCUELA POLITÉCNICA DEL EJÉRCITO.» -. [en linea] https://repositorio.espe.edu.ec/bitstream/21000/6972/1/AC-GRT-ESPE-047091.pdf.

7.4. Establecimiento de controles.

Los controles para implementar están definidos sobre norma ISO 27001, la cual será el marco de referencia de operación del CSIRT.

A continuación, se especifican los criterios utilizados para clasificar las vulnerabilidades encontradas.

Integridad: Vulnerabilidades de las aplicaciones que permiten el acceso a la información, modificación y/o eliminación, partiendo desde ataques SQL injection en las bases de datos por la no implementación de controles apropiados.

Autenticación: Vulnerabilidades de las aplicaciones que permiten capturar los datos de Login de los usuarios, fallas en la validación de los datos de acceso concediendo acceso a usuarios no autorizados, backdoor de acceso no autorizado, mala encriptación de los datos de inicio de sesión que pueden ser capturados y desencriptados por la no utilización de sistemas de encriptación fuertes.

Permisos y acceso a recursos: Vulnerabilidad de uso de las aplicaciones permitiendo accesos a otras aplicaciones y a información confidencial. También se debe tener en cuenta la versión del sistema operativo y los parches de seguridad instalados.[112]

[112]Cuervo Álvarez, Sara. «Implementacion ISO 27001.» -. [en linea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/10/scuervoTFM0617presentaci%C3%B3n.pdf.

Recomendaciones:

Identificar los responsables de la seguridad de la información de cada organización a la que se le presta servicio, al igual que los responsables de los sistemas de información, los administradores de las bases de datos y todos los usuarios con acceso a la información contenida para establecer responsables y niveles de acceso tanto al sistema como a la información.

Clasificar la información contenida en los sistemas de información y bases de datos según su valor para la organización.

Controles para implementar:

Inventario de dispositivos: Identificar e inventariar los equipos que pueden tener acceso al sistema de información y administración sobre la base y motor de base de datos.[113]

Inventario de software: Mantener inventario del software, versión del sistema operativo y estado de actualizaciones del servidor donde está instalado el motor de base de datos y la base de datos, mantener listas blancas y negras de software, mantener inventario de las ubicaciones de las instancias de las bases de datos que hacen parte del sistema de información.[114]

Gestión continua de vulnerabilidades: Mantener listado de vulnerabilidades conocidas que puedan afectar el sistema de información, el servidor de base de datos y la base de datos.[115]

Uso controlado de privilegios administrativos: Establecer los usuarios administradores que tendrán acceso al servidor y establecer el nivel de permisos sobre la base de datos para controlar las posibles modificaciones, modificar el nombre de la cuenta de administración local del servidor y mantenerla con clave segura.

[113]Ministerio de comunicaciones de Colombia. «Seguridad y privacidad de la información.» 2016. [en linea] https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf.
[114]ICONTEC. «NORMA TÉCNICA NTC-ISO/IEC NORMA TÉCNICA NTC-ISO/IEC.» 2006. [en linea] http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.
[115]Cuervo Álvarez, Sara. «Implementacion ISO 27001.» -. [en linea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/10/scuervoTFM0617presentaci%C3%B3n.pdf.

Configuración segura para equipos y dispositivos: Realizar control sobre los equipos que tendrán acceso remoto, verificando que estén actualizados tanto en software como versión de sistema operativo y programa antivirus, establecer línea de software base.

Log de auditoría: mantener logs de eventos tanto para los servidores como para las bases de datos y mantenerlos almacenados en un repositorio independiente mediante tareas programadas automatizadas.

Control sobre puertos de red: realizar monitoreo y rastreo regularmente de los puertos de red, protocolos y servicios utilizados para la conexión a los servidores y motores de base de datos (puertos 1433, 1434, 2382, 4022) uso de Firewall para realizar filtrado de puerto y denegación de acceso.

Protección del correo electrónico y navegadores web: mantener monitoreo del correo electrónico de los equipos que tienen acceso a la base de datos y sistemas de información, filtrado de spam y de phishing, limitar la navegación web para evitar ingresar a páginas que contengan software malicioso que pueda propagarse por la red y afecta la información de las bases de datos.

Defensa contra software malintencionado: manteniendo instalado y actualizado un software antivirus en todos los equipos, se recomienda que la instalación y actualización sea por medio de una política de dominio para garantizar la instalación y actualización en los equipos, mantener la administración centralizada para el despliegue de actualizaciones de la base de virus y del propio agente de protección, mantener estadísticas de posibles amenazas detectadas.

Capacidad de recuperación de datos: mantener versiones de las bases de datos, copias de respaldo completos, diferenciales y transaccionales de las bases de datos, mantener las copias de respaldo en ubicaciones distintas al servidor de base de datos.

Configuración segura de equipos de red: realizar monitoreo y gestión sobre los parámetros de configuración de los diferentes dispositivos de red que se tiene, cambiar todos los usuarios administradores y claves de acceso, implementación del

Modelo de defensa en profundidad (basado en capas): Implementar ambientes aislados de ejecución con el fin de separar los componentes de las aplicaciones.[116] Protección de datos, mantener inventarios de datos importantes, su ubicación y nivel de prioridad, cifrar las máquinas desde donde se ingresa a los servidores de base de datos y/o el acceso al motor de base de datos, bloqueo de puertos USB, implementar sistemas DLP (data lost protección).[117]

Control de acceso: Restringir el acceso a la información de la base de datos y del sistema de información basado en el nivel de necesidad de conocimiento de la información mediante el control de los usuarios autorizados y de los equipos con acceso a los sistemas, para el sistema de login de la aplicación, se recomienda el uso de permisos de firma digital, estos permisos son transparentes para los usuarios y garantizan el acceso autorizado a elementos firmados dentro de la aplicación, implementar un servicio de autenticación por token y uso de protocolo de transmisión de datos seguro (HTTPS) para agregar cifrado al canal de transmisión, además permite el control sobre el flujo de datos por el puerto 443, en el caso de uso de redes públicas por parte de los usuarios se recomienda el uso de SSL Socket y la implementación de servicios de notificación de inicio de múltiples sesiones.

Control de cuentas: crear cuentas de dominio relacionadas a cada usuario de la organización con acceso a los sistemas, con el fin de evitar el acceso desde las cuentas normales de dominio, y tener control de las actividades de la cuenta mediante los logs de auditoría.[118]

Se recomienda el uso y aplicación de la norma ISO/IEC 27002:2013 ya que esta norma gestiona la seguridad de la información en las organizaciones, el CSIRT por ser un organismo de control debe aplicar en ISO/IEC 27002:2013 y de esta forma contar con controles estandarizados a nivel mundial.

[116]Cuervo Álvarez, Sara. «Implementacion ISO 27001.» -. [en linea] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/10/scuervoTFM0617presentaci%C3%B3n.pdf.
[117]Ministerio de comunicaciones de Colombia. «Seguridad y privacidad de la información.» 2016. [en linea] https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf.
[118]ICONTEC. «NORMA TÉCNICA NTC-ISO/IEC NORMA TÉCNICA NTC-ISO/IEC.» 2006. [en linea] http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

Tabla 7 Controles Norma ISO/IEC 27002:2013

5. POLÍTICAS DE SEGURIDAD.	10. CIFRADO.	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
5.1 Directrices de la Dirección en seguridad de la información.	10.1 Controles criptográficos.	14.1 Requisitos de seguridad de los sistemas de información.
5.1.1 Conjunto de políticas para la seguridad de la información.	10.1.1 Política de uso de los controles criptográficos.	14.1.1 Análisis y especificación de los requisitos de seguridad.
5.1.2 Revisión de las políticas para la seguridad de la información.	10.1.2 Gestión de claves.	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	11. SEGURIDAD FÍSICA Y AMBIENTAL.	14.1.3 Protección de las transacciones por redes telemáticas.
6.1 Organización interna.	11.1 Áreas seguras.	14.2 Seguridad en los procesos de desarrollo y soporte.
6.1.1 Asignación de responsabilidades para la segur. de la información.	11.1.1 Perímetro de seguridad física.	14.2.1 Política de desarrollo seguro de software.
6.1.2 Segregación de tareas.	11.1.2 Controles físicos de entrada.	14.2.2 Procedimientos de control de cambios en los sistemas.
6.1.3 Contacto con las autoridades.	11.1.3 Seguridad de oficinas, despachos y recursos.	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
6.1.4 Contacto con grupos de interés especial.	11.1.4 Protección contra las amenazas externas y ambientales.	14.2.4 Restricciones a los cambios en los paquetes de software.
6.1.5 Seguridad de la información en la gestión de proyectos.	11.1.5 El trabajo en áreas seguras.	14.2.5 Uso de principios de ingeniería en protección de sistemas.
6.2 Dispositivos para movilidad y teletrabajo.	11.1.6 Áreas de acceso público, carga y descarga.	14.2.6 Seguridad en entornos de desarrollo.
6.2.1 Política de uso de dispositivos para movilidad.	11.2 Seguridad de los equipos.	14.2.7 Externalización del desarrollo de software.

6.2.2 Teletrabajo.	11.2.1 Emplazamiento y protección de equipos.	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	11.2.2 Instalaciones de suministro.	14.2.9 Pruebas de aceptación.
7.1 Antes de la contratación.	11.2.3 Seguridad del cableado.	14.3 Datos de prueba.
7.1.1 Investigación de antecedentes.	11.2.4 Mantenimiento de los equipos.	14.3.1 Protección de los datos utilizados en pruebas.
7.1.2 Términos y condiciones de contratación.	11.2.5 Salida de activos fuera de las dependencias de la empresa.	15. RELACIONES CON SUMINISTRADORES.
7.2 Durante la contratación.	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	15.1 Seguridad de la información en las relaciones con suministradores.
7.2.1 Responsabilidades de gestión.	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	15.1.1 Política de seguridad de la información para suministradores.
7.2.2 Concienciación, educación y capacitación en segur. de la información.	11.2.8 Equipo informático de usuario desatendido.	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
7.2.3 Proceso disciplinario.	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
7.3 Cese o cambio de puesto de trabajo.	12. SEGURIDAD EN LA OPERATIVA.	15.2 Gestión de la prestación del servicio por suministradores.
7.3.1 Cese o cambio de puesto de trabajo.	12.1 Responsabilidades y procedimientos de operación.	15.2.1 Supervisión y revisión de los servicios prestados por terceros.
8. GESTIÓN DE ACTIVOS.	12.1.1 Documentación de procedimientos de operación.	15.2.2 Gestión de cambios en los servicios prestados por terceros.

8.1 Responsabilidad sobre los activos.	12.1.2 Gestión de cambios.	16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
8.1.1 Inventario de activos.	12.1.3 Gestión de capacidades.	16.1 Gestión de incidentes de seguridad de la información y mejoras.
8.1.2 Propiedad de los activos.	12.1.4 Separación de entornos de desarrollo, prueba y producción.	16.1.1 Responsabilidades y procedimientos.
8.1.3 Uso aceptable de los activos.	12.2 Protección contra código malicioso.	16.1.2 Notificación de los eventos de seguridad de la información.
8.1.4 Devolución de activos.	12.2.1 Controles contra el código malicioso.	16.1.3 Notificación de puntos débiles de la seguridad.
8.2 Clasificación de la información.	12.3 Copias de seguridad.	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
8.2.1 Directrices de clasificación.	12.3.1 Copias de seguridad de la información.	16.1.5 Respuesta a los incidentes de seguridad.
8.2.2 Etiquetado y manipulado de la información.	12.4 Registro de actividad y supervisión.	16.1.6 Aprendizaje de los incidentes de seguridad de la información.
8.2.3 Manipulación de activos.	12.4.1 Registro y gestión de eventos de actividad.	16.1.7 Recopilación de evidencias.
8.3 Manejo de los soportes de almacenamiento.	12.4.2 Protección de los registros de información.	17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓNDE LA CONTINUIDAD DEL NEGOCIO.
8.3.1 Gestión de soportes extraíbles.	12.4.3 Registros de actividad del administrador y operador del sistema.	17.1 Continuidad de la seguridad de la información.
8.3.2 Eliminación de soportes.	12.4.4 Sincronización de relojes.	17.1.1 Planificación de la continuidad de la seguridad de la información.
8.3.3 Soportes físicos en tránsito.	12.5 Control del software en explotación.	17.1.2 Implantación de la continuidad de la seguridad de la información.

9. CONTROL DE ACCESOS.	12.5.1 Instalación del software en sistemas en producción.	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
9.1 Requisitos de negocio para el control de accesos.	12.6 Gestión de la vulnerabilidad técnica.	17.2 Redundancias.
9.1.1 Política de control de accesos.	12.6.1 Gestión de las vulnerabilidades técnicas.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
9.1.2 Control de acceso a las redes y servicios asociados.	12.6.2 Restricciones en la instalación de software.	18. CUMPLIMIENTO.
9.2 Gestión de acceso de usuario.	12.7 Consideraciones de las auditorías de los sistemas de información.	18.1 Cumplimiento de los requisitos legales y contractuales.
9.2.1 Gestión de altas/bajas en el registro de usuarios.	12.7.1 Controles de auditoría de los sistemas de información.	18.1.1 Identificación de la legislación aplicable.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	13. SEGURIDAD EN LAS TELECOMUNICACIONES.	18.1.2 Derechos de propiedad intelectual (DPI).
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	13.1 Gestión de la seguridad en las redes.	18.1.3 Protección de los registros de la organización.
9.2.4 Gestión de información confidencial de autenticación de usuarios.	13.1.1 Controles de red.	18.1.4 Protección de datos y privacidad de la información personal.
9.2.5 Revisión de los derechos de acceso de los usuarios.	13.1.2 Mecanismos de seguridad asociados a servicios en red.	18.1.5 Regulación de los controles criptográficos.
9.2.6 Retirada o adaptación de los derechos de acceso	13.1.3 Segregación de redes.	18.2 Revisiones de la seguridad de la información.
9.3 Responsabilidades del usuario.	13.2 Intercambio de información con partes externas.	18.2.1 Revisión independiente de la seguridad de la información.

9.3.1 Uso de información confidencial para la autenticación.	13.2.1 Políticas y procedimientos de intercambio de información.	18.2.2 Cumplimiento de las políticas y normas de seguridad.
9.4 Control de acceso a sistemas y aplicaciones.	13.2.2 Acuerdos de intercambio.	18.2.3 Comprobación del cumplimiento.
9.4.1 Restricción del acceso a la información.	13.2.3 Mensajería electrónica.	
9.4.2 Procedimientos seguros de inicio de sesión.	13.2.4 Acuerdos de confidencialidad y secreto.	
9.4.3 Gestión de contraseñas de usuario.		
9.4.4 Uso de herramientas de administración de sistemas.		
9.4.5 Control de acceso al código fuente de los programas.		

Fuente: ISO 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES. {En línea}. {consultado el 10 de noviembre de 2020} disponible en: https://www.efectus.cl/wp-content/uploads/2018/12/Controles_ISO27002-2013.pdf

EL CSIRT debe establecer tres tipos de controles:

Controles de configuración: los cuales están destinados a mitigar los ataques informáticos realizados sobre la infraestructura de la organización, su función es realizar la evaluación y control sobre los cambios en las configuraciones de los activos.

Controles de acceso: Su función principal es limitar el acceso de los usuarios y de usuarios externos a la red y los recursos de las organizaciones.

Controles de ocurrencia: Están diseñados para evitar la ocurrencia de incidentes de seguridad informática y se determinan luego de la evaluación de riesgos realizada sobre los activos de las organizaciones.

8. ESTRCUTURA OPERATIVA E INFRAESTRUCTURA FUNCIONAL DEL CSIRT.

Es importante establecer que, para el funcionamiento de un CSIRT, existen varios modelos organizativos, estos modelos dependen tanto del CSIRT mismo como de las organizaciones a las que está orientado.[119]

Los modelos más comunes son:

Modelo de organización independiente: En este modelo el CSIRT es totalmente independiente, cuenta con su propia estructura organizacional, directivos y empleados.[120]

Modelo integrado en una organización preexistente: Bajo este modelo, el CSIRT funciona como un área o dependencia más de una organización, cuenta con un director o jefe de equipo responsable de las actividades realizadas, cuenta con personal técnico y profesional para atender los incidentes de ciberseguridad y también puede solicitar apoyo a otras áreas de la organización.[121]

Modelo "Campus": En este modelo existe una sede principal y varias subsedes con un nivel reducido de autonomía en su actuar.

Modelo Basado en el voluntariado: Son grupos de apoyo voluntario en donde se reúnen especialistas para brindar asesoría y apoyo dentro de comunidades.[122]

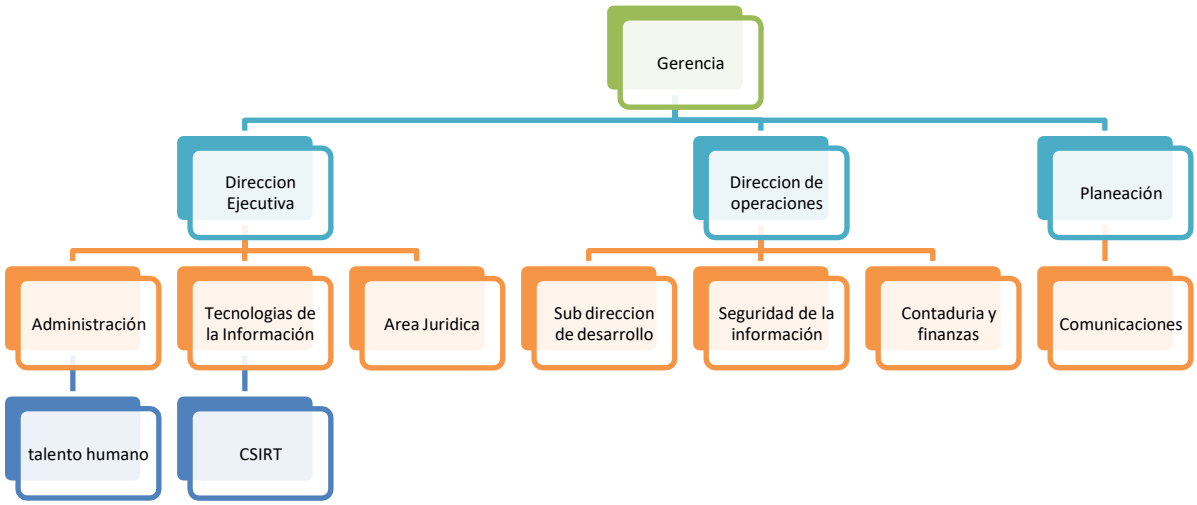
[119]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.
[120]Ibid P 21
[121]Ibid P 21
[122]Ibid P 21

Teniendo en cuenta los modelos anteriores, se establece que el CSIRT para la empresa Cibersecurity de Colombia Ltda, por ser parte de una empresa ya existente aplica el modelo integrado en una organización preexistente.

8.1. Modelo Organizacional.

Es siguiente modelo organizacional representa la estructura jerárquica de la organización.

Ilustración 3 Organigrama



Fuente: Elaboración del autor.

8.2. Misión.

Cibersecurity de Colombia Ltda mediante su CSIRT busca brindar servicios de calidad frente a la atención de incidentes de ciberseguridad en entidades de orden público y privado con el ánimo de garantizar la prestación de los servicios, el mantenimiento de la infraestructura y responder de manera ágil y eficaz a las necesidades actuales de seguridad.

8.3. Visión.

Cibersecurity de Colombia Ltda mediante su CSIRT busca para el año 2024 ser líder nacional y referente internacional en la prestación de servicios destinados a garantizar la seguridad cibernética en las organizaciones

8.4. Estructura del CSIRT.

Para la prestación de servicios básicos de seguridad se requiere un estimado de 4 funcionarios a jornada completa, para la prestación de servicios completos se requiere un mínimo de 8 funcionarios a jornada completa y para turnos 24x7 se debe contar con mínimo 12 funcionarios.

El CSIRT está conformado por los siguientes actores:

Director: Se encarga de tomar las decisiones administrativas, supervisa el equipo de trabajo, miembro permanente del comité asesor de seguridad[123], encargado de la planeación y control de las actividades propias del CSIRT, debe ser especialista en seguridad informática, con experiencia en gestión de crisis y recuperación del negocio.[124]

[123]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.

[124]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

Jefe equipo técnico: Encargado del equipo técnico además funciona como enlace entre las organizaciones a las que les presta servicio en CSIRT, coordinar la actividad de grupo técnico, debe ejercer control sobre los activos de información y coordinar el proceso de respuesta de incidentes.[125]

Técnicos CSIRT: Personal calificado para prestar servicios de seguridad de la información, deben estar capacitados para analizar incidentes, realizar monitoreo, registro y respuesta, de ser necesario debe interactuar con otros grupos para resolver el incidente[126]

Personal de investigación: Personal que realiza investigación forense y análisis destinados a mitigar vulnerabilidades, desarrolla material técnico para uso interno y realiza monitoreo.[127]

Gestores de incidentes: Encargado del análisis, monitoreo y gestión de los incidentes reportados, se encarga de coordinar la respuesta ante el incidente.[128]

Analista: Encargado de investigación dentro de las organizaciones a la que se les presta servicio para identificar necesidades de capacitación de los usuarios.[129]

Clasificador de incidentes: Encargado de brindar asistencia inicial, luego cataloga en incidente y lo escala de ser necesario.[130]

Administrador de red: Encargado de monitorear y controlar la red del CSIRT y da solución a incidentes de red de las organizaciones a las que se les presta servicio.[131]

[125]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.
[126]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
[127]Ibid P 49
[128]Ibid P 49
[129]Ibid P 49
[130]Ibid P 49
[131]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Administrador de sistemas: Encargado de administrar los sistemas que forman parte del CSIRT, gestiona el acceso a la información según los niveles de acceso de los usuarios y según las políticas de clasificación de la información.[132]

Ilustración 4 Estructura CSIRT

Fuente: Elaboración del autor.

[132]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Los técnicos y especialistas deben contar con conocimientos en:

Conocimiento de sistemas Linux y Windows.[133]

Conocimiento de infraestructura de red.[134]

Conocimiento de protocolos de internet.[135]

Conocimiento de seguridad informática.[136]

Conocimiento sobre evaluación de riesgo.[137]

Conocimiento sobre amenazas de seguridad informática.[138]

Conocimiento sobre servidores web.[139]

8.5. Esquema inicial de red.

El esquema inicial de red establece las diferentes áreas establecidas para el CSIRT, estas dependencias son las mínimas posibles para implementar, la cantidad de áreas depende del tamaño del CSIRT y de su alcance operativo, las áreas funcionales son:

Centro de Datos

Centro de Operaciones

Soporte TI

[133]Enisa csirt. «Cómo crear un CSIRT paso a paso.» 2006. [en linea]. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-n9P4muDvAhXwEVkFHfN3A_4QFjAAegQIAxAD&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcsirt-setting-up-guide-in-spanish%2Fat_download%2FfullReport&usg=AOvVaw2F8Wp_02LEvZ-NMA
[134]Ibid P 26
[135]Ibid P 26
[136]Ibid P 26
[137]Ibid P 26
[138]Ibid P 26
[139]Ibid P 26

Coordinaciones

Área Logística

Salón de Formación

Salón de crisis

Para la creación de la red interna del CSIRT se creó direccionamiento para cada área en segmentos de red diferentes.

Tabla 8 Descripción direccionamiento IP.

Ubicación	VLAN	Red
Centro de Datos	10 - 16	192.168.10.0/24
Centro de Operaciones	11	192.168.11.0/24
Soporte TI	12	192.168.12.0/24
Coordinaciones	13	192.168.13.0/24
Salón de Formación	14	192.168.14.0/24
Salón de crisis	15	192.168.15.0/24

Fuente: Elaboración del autor.

Los switches empleados están demarcados según el área correspondiente con su direccionamiento especifico.

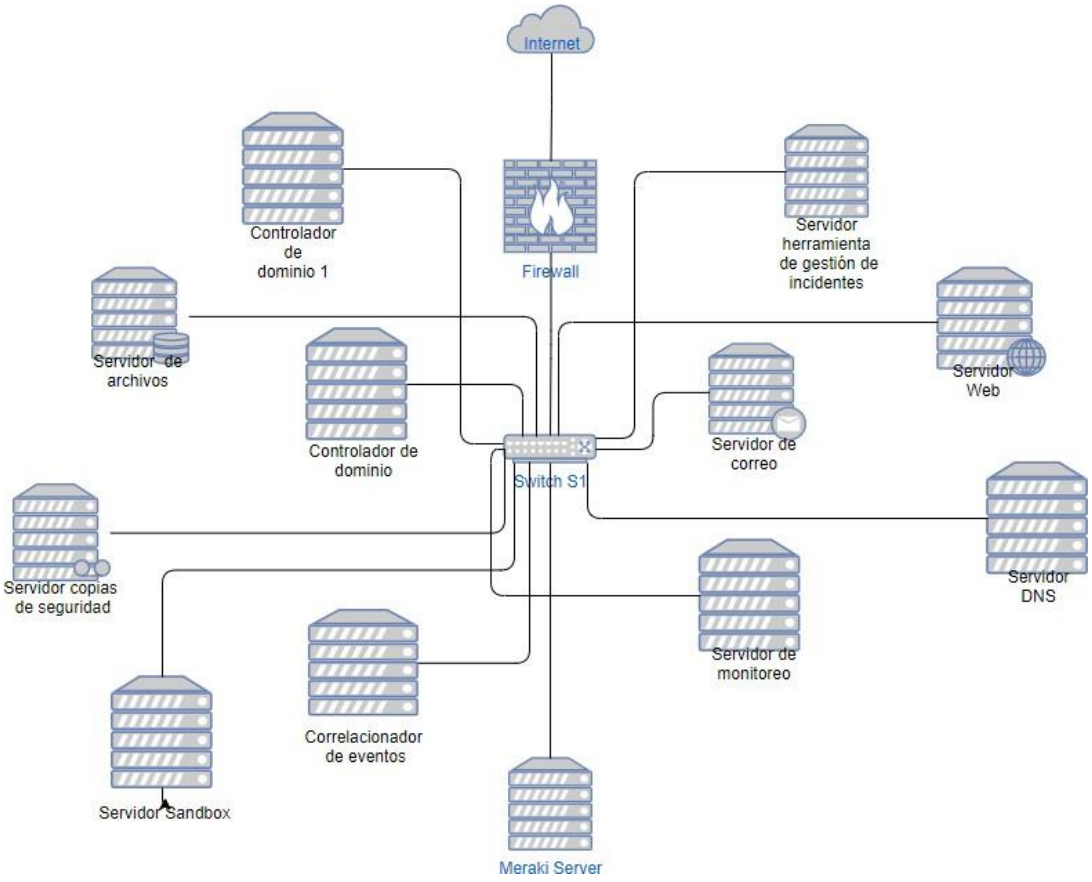
Tabla 9 Direccionamiento IP administración Switches.

Ubicación	Nombre	VLAN	Red
Centro de Datos	Servidores 1	10	192.168.10.1
Centro de Operaciones	Centro de operaciones 1	11	192.168.11.1
Soporte TI	IT1	12	192.168.12.1
Coordinaciones	Gerencias	13	192.168.13.1
Salón de Formación	CF1	14	192.168.14.1
Salón de crisis	Centro de crisis 1	15	192.168.15.1

Fuente: Elaboración del autor.

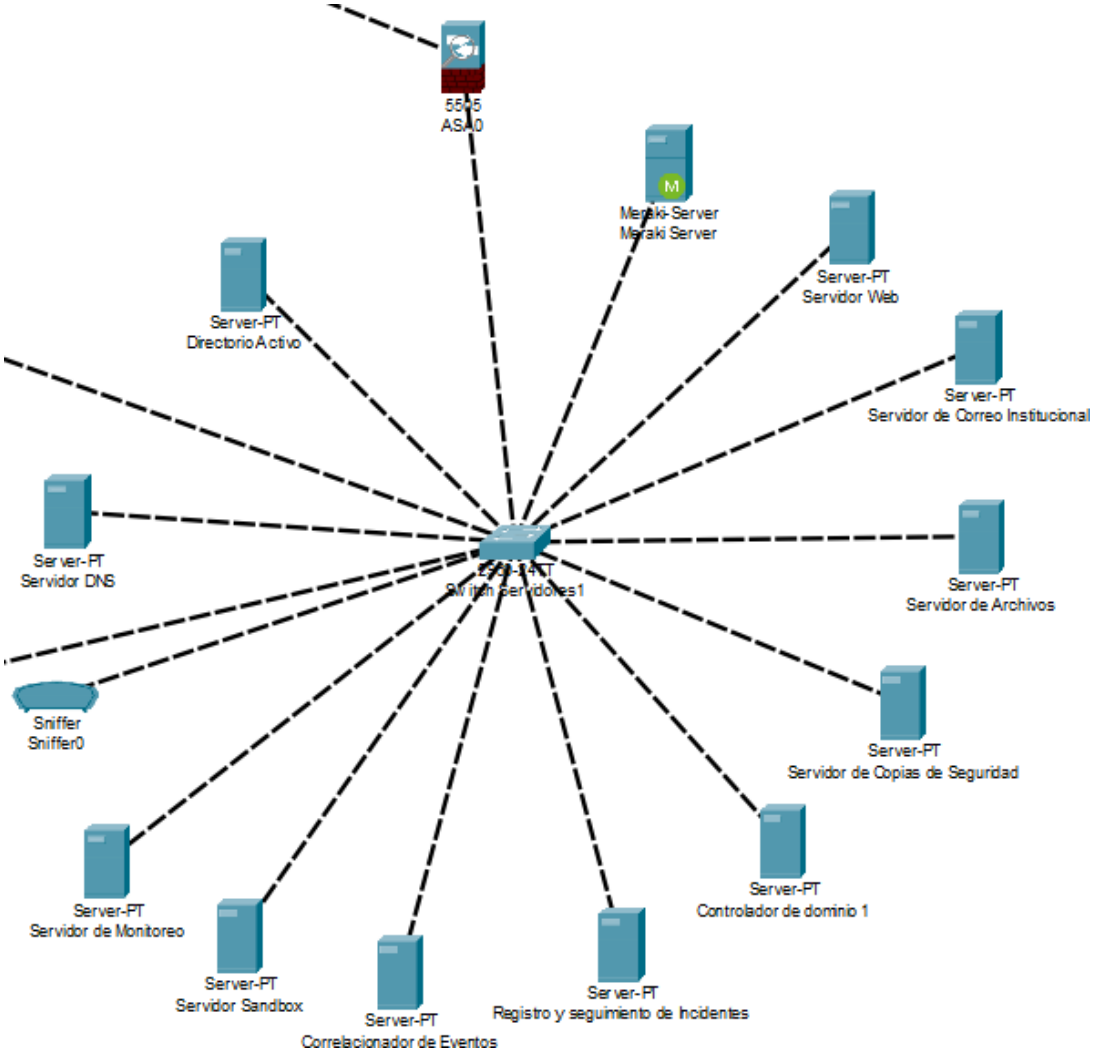
8.6. Esquema centro de datos.

Ilustración 5 Esquema pictografico centro de datos.



Fuente: Elaboración del autor.

Ilustración 6 Esquema de red creado desde Cisco Packet tracer.



Fuente: Elaboración del autor.

El centro de datos este compuesto por los siguientes servidores:

Servidor Web

Servidor de Correo Institucional

Servidor de Intranet

Servidor de Archivos

Servidor de Copias de Seguridad

Servidor DNS

Servidor de Monitoreo

Servidor Sandbox

Correlacionador de Eventos

Registro y seguimiento de Incidentes

Su función es mantener centralizados los principales servicios de protección y monitoreo del CSIRT, está configurado sobre una VLAN independiente bajo el principio de segmentación de la red y protegido bajo su propio firewall.

Los servidores se encuentran en segmento de red Vlan 10 y 16, los servidores de respaldo se encuentran en segmento de Vlan 12.

Tabla 10 Direccionamiento IP de los servidores.

Clase	IP
Servidor Web	192.168.10.10
Servidor de Correo Institucional	192.168.10.12
Servidor de Intranet	192.168.10.15
Directorio Activo	192.168.10.17
Servidor de Archivos	192.168.10.18
Servidor de Copias de Seguridad	192.168.10.21
Servidor DNS	192.168.16.11
Servidor de Monitoreo	192.168.16.13
Servidor Sandbox	192.168.16.14
Correlacionador de Eventos	192.168.16.20
Registro y seguimiento de Incidentes	192.168.16.22
Servidor de archivos - respaldo	192.168.12.11
Directorio Activo 2	192.168.12.13

Fuente: Elaboración del autor.

A continuación, se presentan las características técnicas de los servidores (hardware).

Tabla 11 Características de los servidores.

Clase	Servidor	Características	Procesador	RAM	HDD
Servidor Web	Dell PowerEdge en rack R930	Servidor de 4 sockets, para aplicaciones empresariales con alto consumo interno.	Intel Xeon E7- 4800 de 18 núcleos	hasta 96 DIMM DDR4, 1866 MT/s	24 unidades HDD o SAS
Servidor de Correo Institucional	Dell PowerEdge en rack R530	Servidor de 2 sockets, diseñado para base de datos y aplicaciones.	Intel Xeon E5- 2600 v3 de 18 núcleos por socket	hasta 12 DIMM DDR4.	8 unidades de HDD
Servidor de Intranet	Dell PowerEdge en rack R530	Servidor de 2 sockets, diseñado para base de datos y aplicaciones.	Intel Xeon E5- 2600 v3 de 18 núcleos por socket	hasta 12 DIMM DDR4.	8 unidades de HDD
Directorio Activo	Dell PowerEdge en rack R530	Servidor de 2 sockets, diseñado para base de datos y aplicaciones.	Intel Xeon E5- 2600 v3 de 18 núcleos por socket	hasta 12 DIMM DDR4.	8 unidades de HDD
Servidor de Archivos	Dell PowerEdge en rack R730xd	Servidor de 2 sockets, para almacenamiento de alta densidad flexible.	Intel Xeon E5- 2600 de 22 núcleos por socket	hasta 24 DIMM DDR4, 2400 MT/s	24 unidades HDD o SAS
Servidor de Copias de Seguridad	Dell PowerEdge en rack R730xd	Servidor de 2 sockets, para almacenamiento de alta densidad flexible.	Intel Xeon E5- 2600 de 22 núcleos por socket	hasta 24 DIMM DDR4, 2400 MT/s	24 unidades HDD o SAS

Servidor DNS	Dell PowerEdge en rack R820	Servidor de 4 sockets, para aplicaciones y bases de datos escalables	Intel Xeon E5- 4600 v3 de 8 núcleos por socket	hasta 48 DIMM, 1866 MT/s	16 unidades SSD
Servidor de Monitoreo	Dell PowerEdge en rack	Servidor de 4 sockets, para aplicaciones y bases de datos escalables	Intel Xeon E5- 4600 v3 de 8 núcleos por socket	hasta 48 DIMM, 1866 MT/s	16 unidades SSD
Servidor Sandbox	Dell PowerEdge en rack	Servidor de 4 sockets, para aplicaciones y bases de datos escalables	Intel Xeon E5- 4600 v3 de 8 núcleos por socket	hasta 48 DIMM, 1866 MT/s	16 unidades SSD
Correlacionador de Eventos	Dell PowerEdge en rack R530	Servidor de 2 sockets, diseñado para base de datos y aplicaciones.	Intel Xeon E5- 2600 v3 de 18 núcleos por socket	hasta 12 DIMM DDR4.	8 unidades de HDD
Registro y seguimiento de Incidentes	Dell PowerEdge en rack	Servidor de 4 sockets, para aplicaciones y bases de datos escalables	Intel Xeon E5- 4600 v3 de 8 núcleos por socket	hasta 48 DIMM, 1866 MT/s	16 unidades SSD
Servidor de archivos - respaldo	Dell PowerEdge en rack R730xd	Servidor de 2 sockets, para almacenamiento de alta densidad flexible.	Intel Xeon E5- 2600 de 22 núcleos por socket	hasta 24 DIMM DDR4, 2400 MT/s	24 unidades HDD o SAS
Directorio Activo 2	Dell PowerEdge en rack R530	Servidor de 2 sockets, diseñado para base de datos y aplicaciones.	Intel Xeon E5- 2600 v3 de 18 núcleos por socket	hasta 12 DIMM DDR4.	8 unidades de HDD

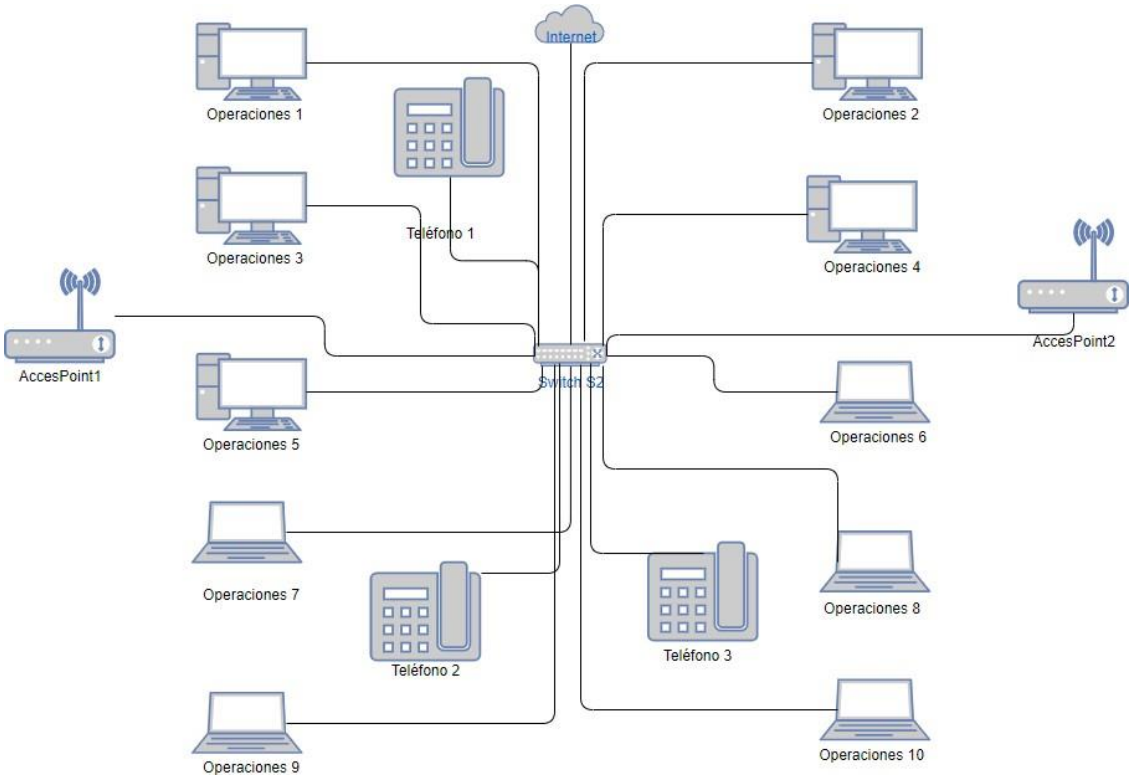
Fuente: Elaboración del autor.

Los servidores están planificados para el uso de la tecnología existente en la empresa Cibersecurity de Colombia Ltda, sin embargo, también es posible utilizar servidores virtualizados sobre plataformas Microsoft Azure o AWS de Amazon.

8.7. Esquema centro de operaciones.

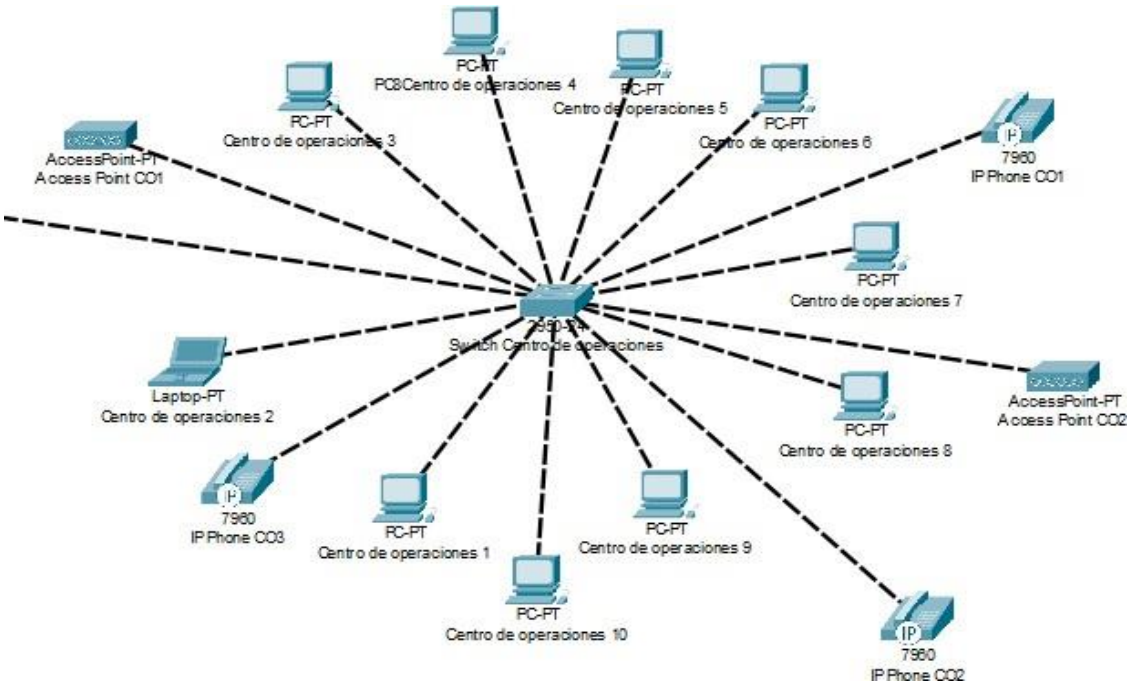
El centro de operaciones cuenta con 10 equipos de cómputo, dos Access points y tres teléfonos IP, su función es brindar un punto de control y monitoreo de los incidentes de seguridad detectados y reportados, cuenta con acceso a todos los sistemas y herramientas que permitan dar una respuesta oportuna al incidente.

Ilustración 7 Esquema pictográfico centro de operaciones



Fuente: Elaboración del autor.

Ilustración 8 Esquema de red creado desde Cisco Packet tracer.



Fuente: Elaboración del autor.

El centro de operaciones se encuentra bajo la Vlan 11, a continuación, se especifica el direccionamiento para cada dispositivo.

Tabla 12 Direccionamiento IP de los dispositivos.

Ubicación	Nombre	Tipo	Red
Centro de Operaciones	Operaciones1	Desktop	192.168.11.3
Centro de Operaciones	Operaciones2	Desktop	192.168.11.4
Centro de Operaciones	Operaciones3	Desktop	192.168.11.5
Centro de Operaciones	Operaciones4	Desktop	192.168.11.6
Centro de Operaciones	Operaciones5	Desktop	192.168.11.7

Centro de Operaciones	Operaciones6	Desktop	192.168.11.8
Centro de Operaciones	Operaciones7	Laptop	192.168.11.9
Centro de Operaciones	Operaciones8	Laptop	192.168.11.10
Centro de Operaciones	Operaciones9	Laptop	192.168.11.11
Centro de Operaciones	Operaciones10	Laptop	192.168.11.12
Centro de Operaciones	Telefono1	teléfono IP	192.168.11.14
Centro de Operaciones	Telefono2	teléfono IP	192.168.11.15
Centro de Operaciones	Telefono3	teléfono IP	192.168.11.16
Centro de Operaciones	AccesPoint1	Enrutador inalámbrico	192.168.11.18
Centro de Operaciones	AccesPoint2	Enrutador inalámbrico	192.168.11.19

Fuente: Elaboración del autor.

A continuación, se presentan las características técnicas de los equipos (hardware).

Tabla 13 Características de los equipos.

Clase	Equipo	Características	procesador	RAM	HDD
Equipos de cómputo de escritorio	HP All-in-One PC 21-b0017la	Equipo de cómputo de alto rendimiento todo en uno marca HP	procesador Intel Core i3 de 10.ª generación o procesador Intel Core i3-1005G1 a 1,2 GHz, hasta 3,4 GHz	4 GB de SDRAM DDR4-3200 (1 x 4 GB)	Unidad interna Disco duro-SATA de 1 TB y 7200 rpm

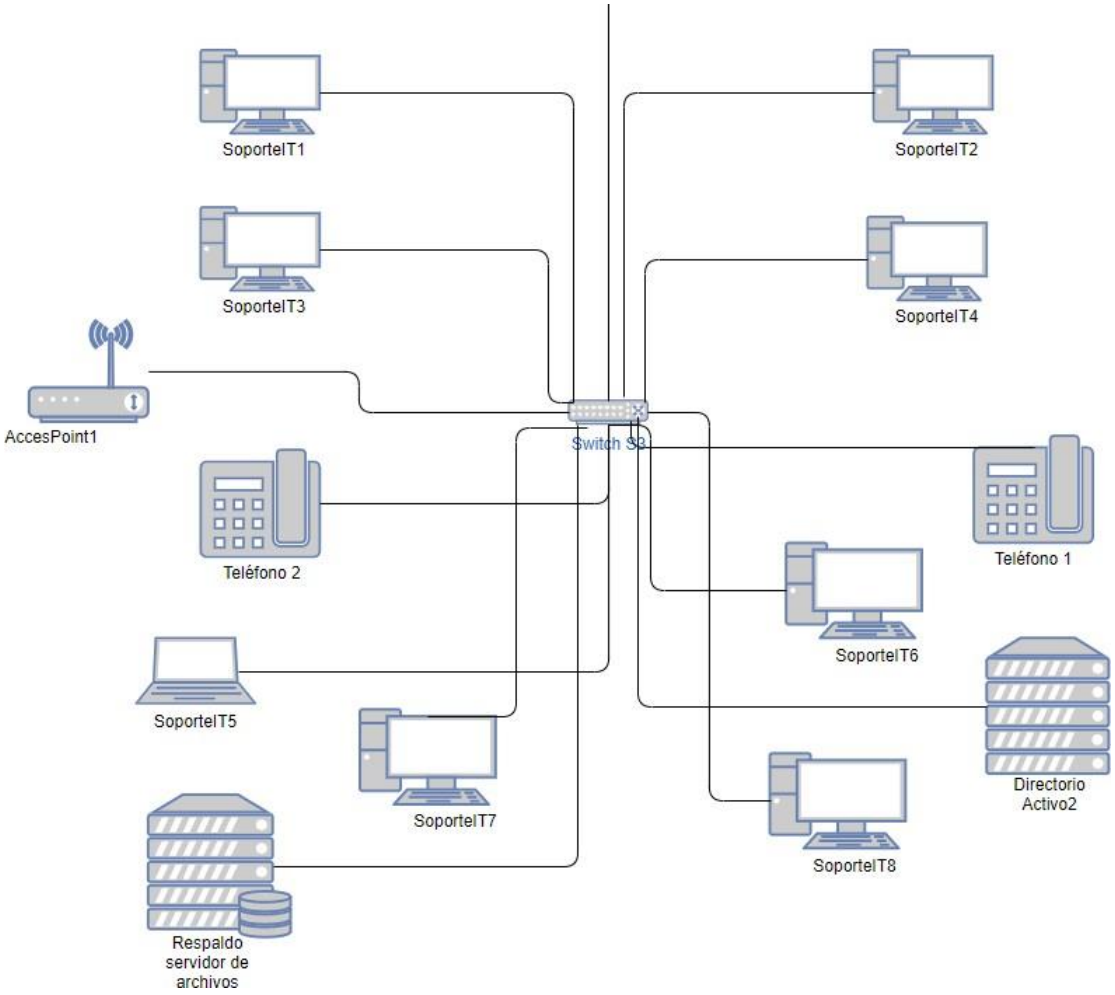
Portátiles	Portátil HP 14-cf3034la	Equipo portátil de alto rendimiento.	Intel Core i3-1005G1	4 GB de SDRAM DDR4-2666	512 GB SSD

Fuente: Elaboración del autor.

8.8. Esquema centro de soporte IT.

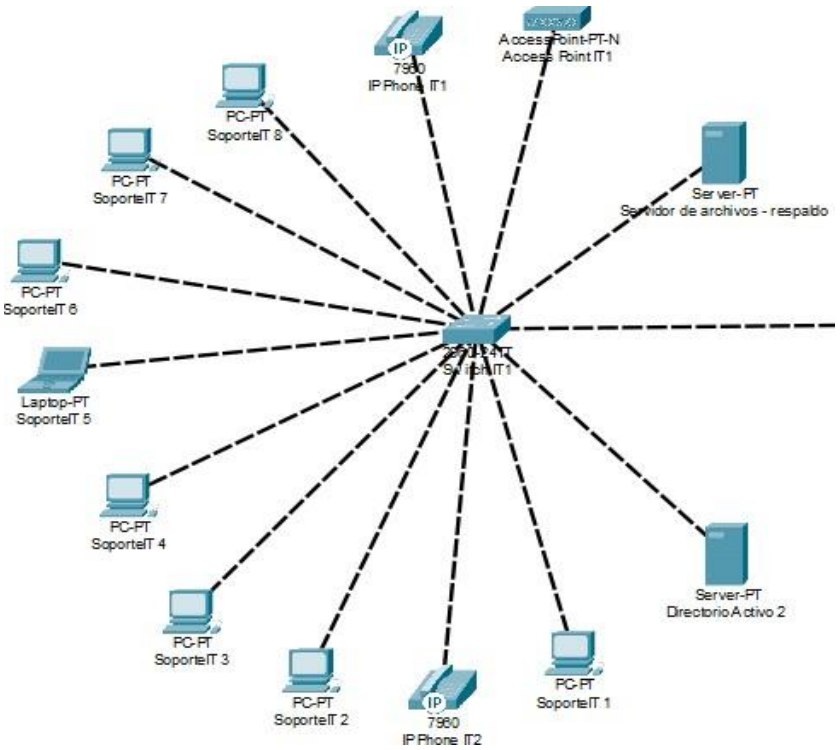
El área de soporte IT cuenta con 7 equipo de cómputo, un equipo portátil, dos teléfonos IP y un Access Point dentro de esta red se ha establecido un respaldo del servidor de archivos y un respaldo del controlador de dominio del CSIRT, su función es servir como punto de recepción de incidentes y de atención técnica de nivel 1, desde esta área se escalan los incidentes cuando no pueden ser solucionados inicialmente.

Ilustración 9 Esquema pictográfico centro de Soporte IT.



Fuente: Elaboración del autor.

Ilustración 10 Esquema de red creado desde Cisco Packet tracer.



Fuente: Elaboración del autor.

El centro de soporte IT se encuentra bajo la Vlan 12, a continuación, se especifica el direccionamiento para cada dispositivo.

Tabla 14 Direccionamiento IP de los dispositivos.

Ubicación	Nombre	Tipo	Red
Centro de Soporte IT	SoporteIT 1	Desktop	192.168.12.3
Centro de Soporte IT	SoporteIT 2	Desktop	192.168.12.4
Centro de Soporte IT	SoporteIT 3	Desktop	192.168.12.5
Centro de Soporte IT	SoporteIT 4	Desktop	192.168.12.6
Centro de Soporte IT	SoporteIT 5	Laptop	192.168.12.7
Centro de Soporte IT	SoporteIT 6	Desktop	192.168.12.8

Centro de Soporte IT	SoporteIT 7	Desktop	192.168.12.9
Centro de Soporte IT	SoporteIT 8	Desktop	192.168.12.10
Centro de Soporte IT	Telefono1	teléfono IP	192.168.12.12
Centro de Soporte IT	Telefono2	teléfono IP	192.168.12.14
Centro de Soporte IT	AccesPoint1	Enrutador inalámbrico	192.168.12.15
Centro de Soporte IT	Respaldo servidor de archivos	Servidor	192.168.12.11
Centro de Soporte IT	Respaldo Directorio activo	Servidor	192.168.12.13

Fuente: Elaboración del autor.

A continuación, se presentan las características técnicas de los equipos (hardware).

Tabla 15 Características de los equipos.

Clase	Equipo	Características	procesador	RAM	HDD
Equipos de cómputo de escritorio	HP All-in-One PC 21-b0017la	Equipo de cómputo de alto rendimiento todo en uno marca HP	procesador Intel Core i3 de 10.ª generación o procesador Intel Core i3-1005G1 a 1,2 GHz, hasta 3,4 GHz	4 GB de SDRAM DDR4-3200 (1 x 4 GB)	Unidad interna Disco duro-SATA de 1 TB y 7200 rpm
Portátiles	Portátil HP 14-cf3034la	Equipo portátil de alto rendimiento.	Intel Core i3-1005G1	4 GB de SDRAM DDR4-2666	512 GB SSD
Servidor de archivos - respaldo	Dell PowerEdge en rack R730xd	Servidor de 2 sockets, para almacenamiento de alta densidad flexible.	Intel Xeon E5- 2600 de 22 núcleos por socket	hasta 24 DIMM DDR4, 2400 MT/s	24 unidades HDD o SAS

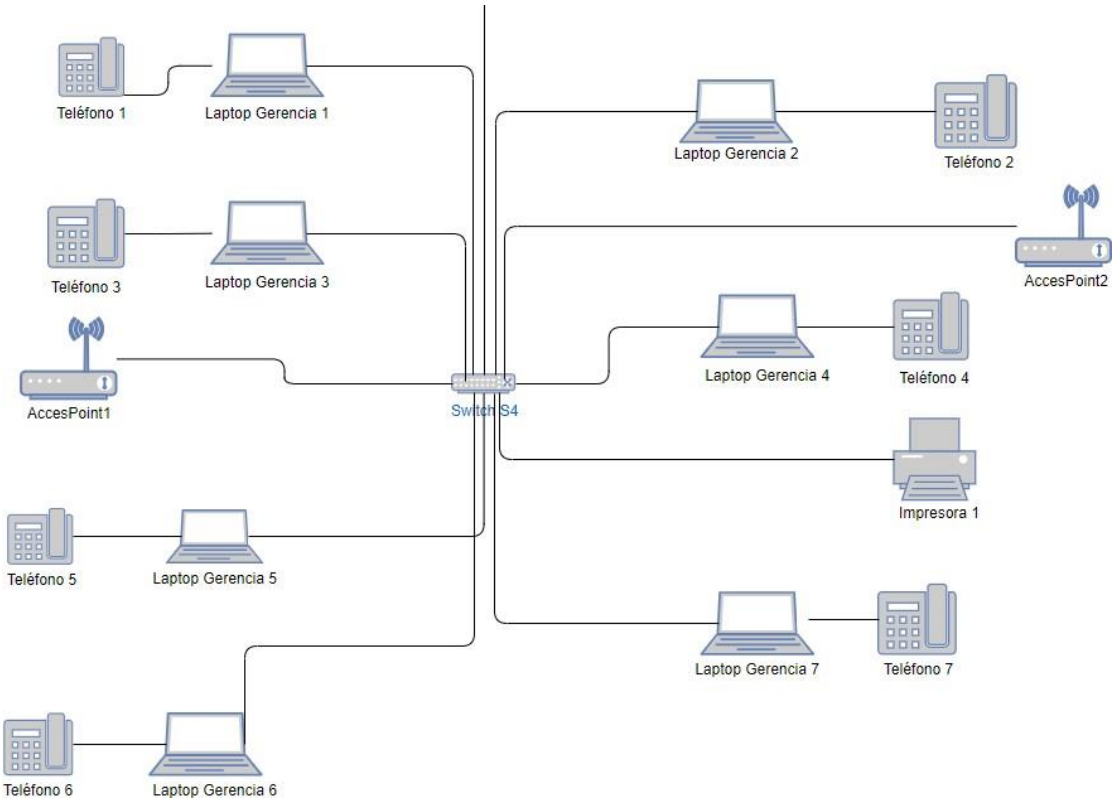
Directorio Activo 2	Dell PowerEdge en rack R530	Servidor de 2 sockets, diseñado para base de datos y aplicaciones.	Intel Xeon E5- 2600 v3 de 18 núcleos por socket	hasta 12 DIMM DDR4.	8 unidades de HDD

Fuente: Elaboración del autor.

8.9. Esquema centro Coordinadores.

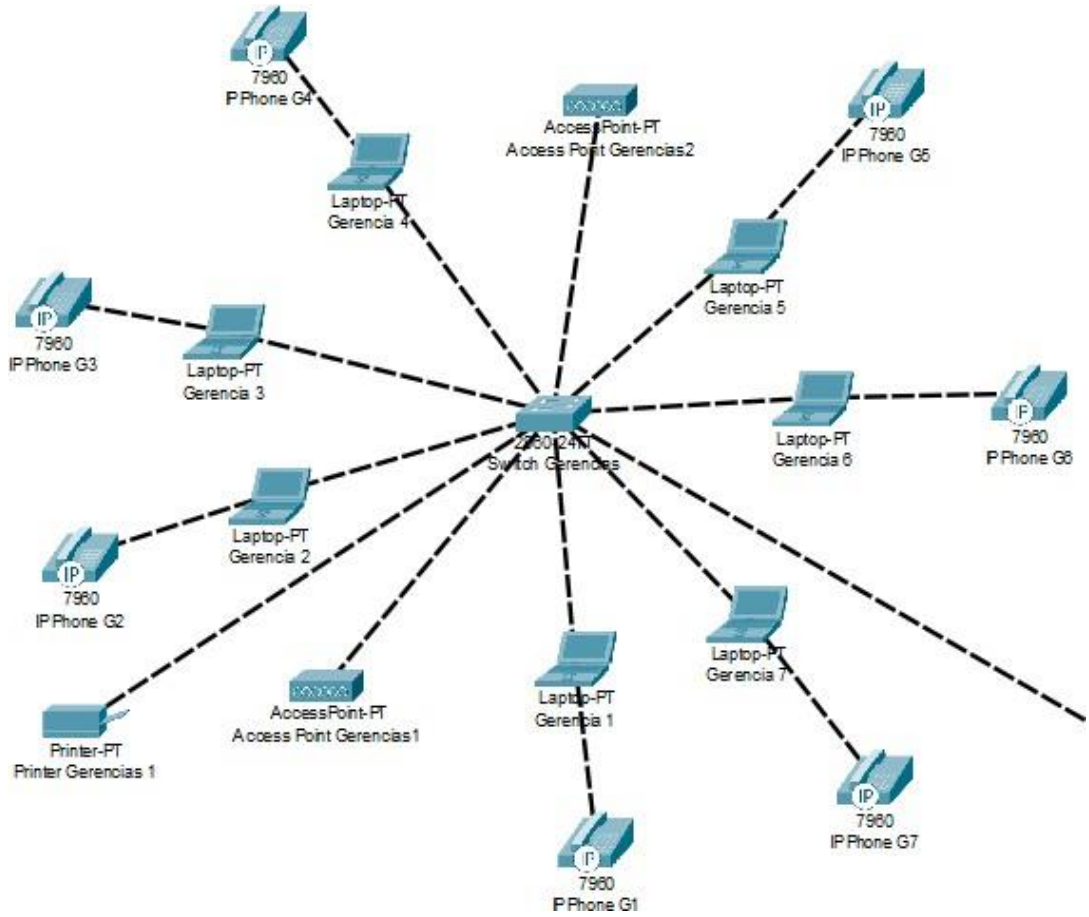
El área de coordinación está compuesta por siete equipos portátiles, dos Access Points, siete teléfonos IP y una impresora configurada en red, su función es la coordinar cada proyecto u organización protegida, llevar control de los incidentes, diseñar los procedimientos, procesos y ajustar las políticas de seguridad a los objetivos específicos de cada organización.

Ilustración 11 Esquema pictográfico centro de Coordinadores.



Fuente: Elaboración del autor.

Ilustración 12 Esquema de red creado desde Cisco Packet tracer.



Fuente: Elaboración del autor.

El centro de soporte IT se encuentra bajo la Vlan 13, a continuación, se especifica el direccionamiento para cada dispositivo.

Tabla 16 Direccionamiento IP de los dispositivos.

Ubicación	Nombre	Tipo	Red
Centro de Coordinadores	laptop Gerencia 1	Laptop	192.168.13.6
Centro de Coordinadores	laptop Gerencia 2	Laptop	192.168.13.7
Centro de Coordinadores	laptop Gerencia 3	Laptop	192.168.13.8
Centro de Coordinadores	laptop Gerencia 4	Laptop	192.168.13.9

Centro de Coordinadores	laptop Gerencia 5	Laptop	192.168.13.10
Centro de Coordinadores	laptop Gerencia 6	Laptop	192.168.13.11
Centro de Coordinadores	laptop Gerencia 7	Laptop	192.168.13.12
Centro de Coordinadores	Teléfono 1	teléfono IP	192.168.13.13
Centro de Coordinadores	Teléfono 2	teléfono IP	192.168.13.14
Centro de Coordinadores	Teléfono 3	teléfono IP	192.168.13.15
Centro de Coordinadores	Teléfono 4	teléfono IP	192.168.13.16
Centro de Coordinadores	Teléfono 5	teléfono IP	192.168.13.17
Centro de Coordinadores	Teléfono 6	teléfono IP	192.168.13.18
Centro de Coordinadores	Teléfono 7	teléfono IP	192.168.13.19
Centro de Coordinadores	AccesPoint1	Enrutador inalámbrico	192.168.13.20
Centro de Coordinadores	AccesPoint1	Enrutador inalámbrico	192.168.13.20

Fuente: Elaboración del autor.

A continuación, se presentan las características técnicas de los equipos (hardware).

Tabla 17 Características de los equipos.

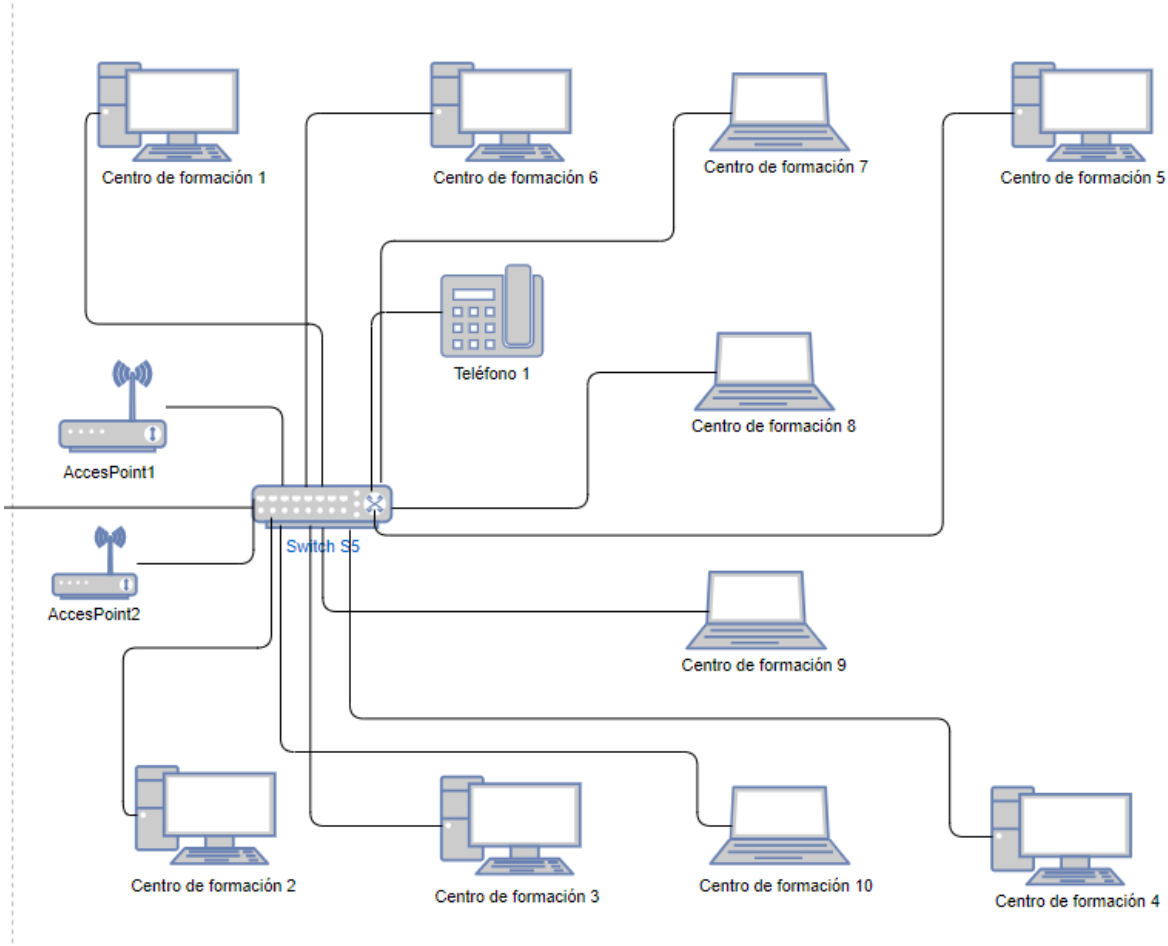
Clase	Equipo	Características	procesador	RAM	HDD
Portátiles	Portátil HP 14-cf3034la	Equipo portátil de alto rendimiento.	Intel Core i3-1005G1	4 GB de SDRAM DDR4-2666	512 GB SSD

Fuente: Elaboración del autor.

8.10. Esquema centro de Formación.

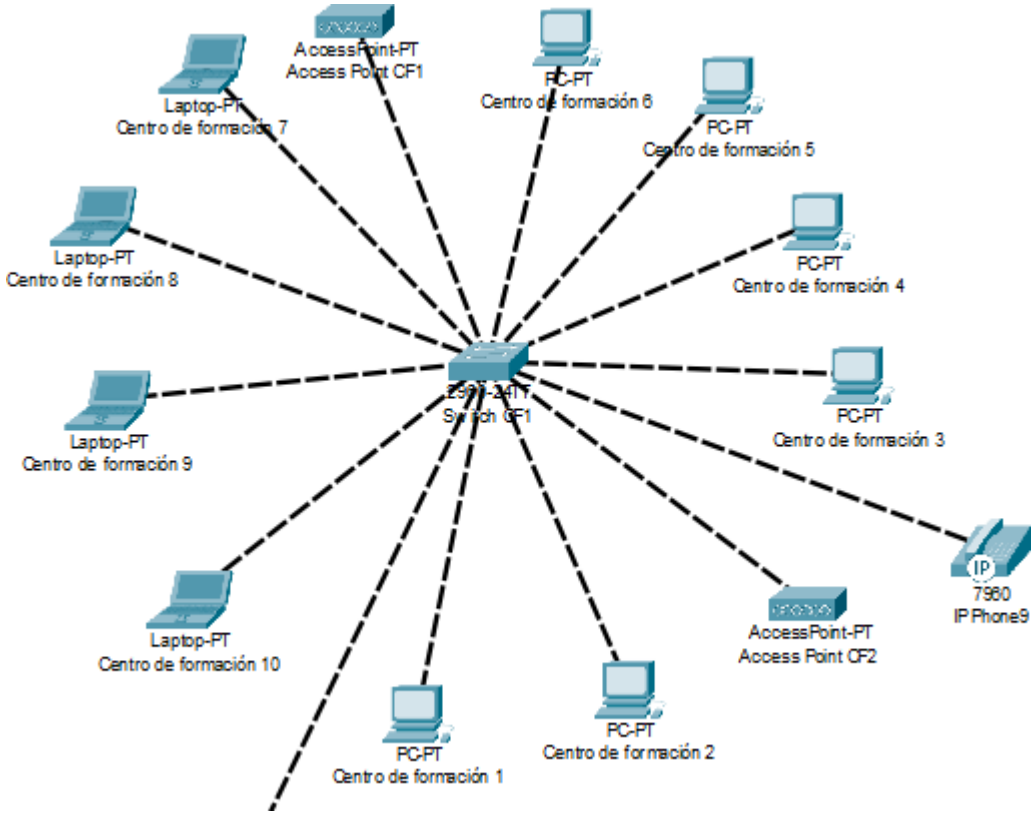
El centro de formación está compuesto por 6 equipos de cómputo, cuatro portátiles, un teléfono IP y dos Access points, su función es brindar capacitación en manejo de herramientas de protección y monitoreo ante incidentes de seguridad, en este espacio se capacita a los técnicos e ingenieros que ingresan Cibersecurity de Colombia LTDA.

Ilustración 13 Esquema pictográfico centro de Formación.



Fuente: Elaboración del autor.

Ilustración 14 Esquema de red creado desde Cisco Packet tracer.



Fuente: Elaboración del autor.

El centro de Formación se encuentra bajo la Vlan 14, a continuación, se especifica el direccionamiento para cada dispositivo.

Tabla 18 Direccionamiento IP de los dispositivos.

Ubicación	Nombre	Tipo	Red
Centro de Formación	Centro de formación 1	Desktop	192.168.14.2
Centro de Formación	Centro de formación 2	Desktop	192.168.14.3
Centro de Formación	Centro de formación 3	Desktop	192.168.14.4
Centro de Formación	Centro de formación 4	Desktop	192.168.14.5
Centro de Formación	Centro de formación 5	Desktop	192.168.14.6

Centro de Formación	Centro de formación 6	Desktop	192.168.14.7
Centro de Formación	Centro de formación 7	Laptop	192.168.14.8
Centro de Formación	Centro de formación 8	Laptop	192.168.14.9
Centro de Formación	Centro de formación 9	Laptop	192.168.14.10
Centro de Formación	Centro de formación 10	Laptop	192.168.14.11
Centro de Formación	Telefono1	teléfono IP	192.168.14.15
Centro de Formación	AccesPoint1	Enrutador inalámbrico	192.168.14.17

Fuente: Elaboración del autor.

A continuación, se presentan las características técnicas de los equipos (hardware).

Tabla 19 Características de los equipos.

Clase	Equipo	Características	procesador	RAM	HDD
Equipos de cómputo de escritorio	HP All-in-One PC 21-b0017la	Equipo de cómputo de alto rendimiento todo en uno marca HP	procesador Intel Core i3 de 10.ª generación o procesador Intel Core i3-1005G1 a 1,2 GHz, hasta 3,4 GHz	4 GB de SDRAM DDR4-3200 (1 x 4 GB)	Unidad interna Disco duro-SATA de 1 TB y 7200 rpm
Portátiles	Portátil HP 14-cf3034la	Equipo portátil de alto rendimiento.	Intel Core i3-1005G1	4 GB de SDRAM DDR4-2666	512 GB SSD

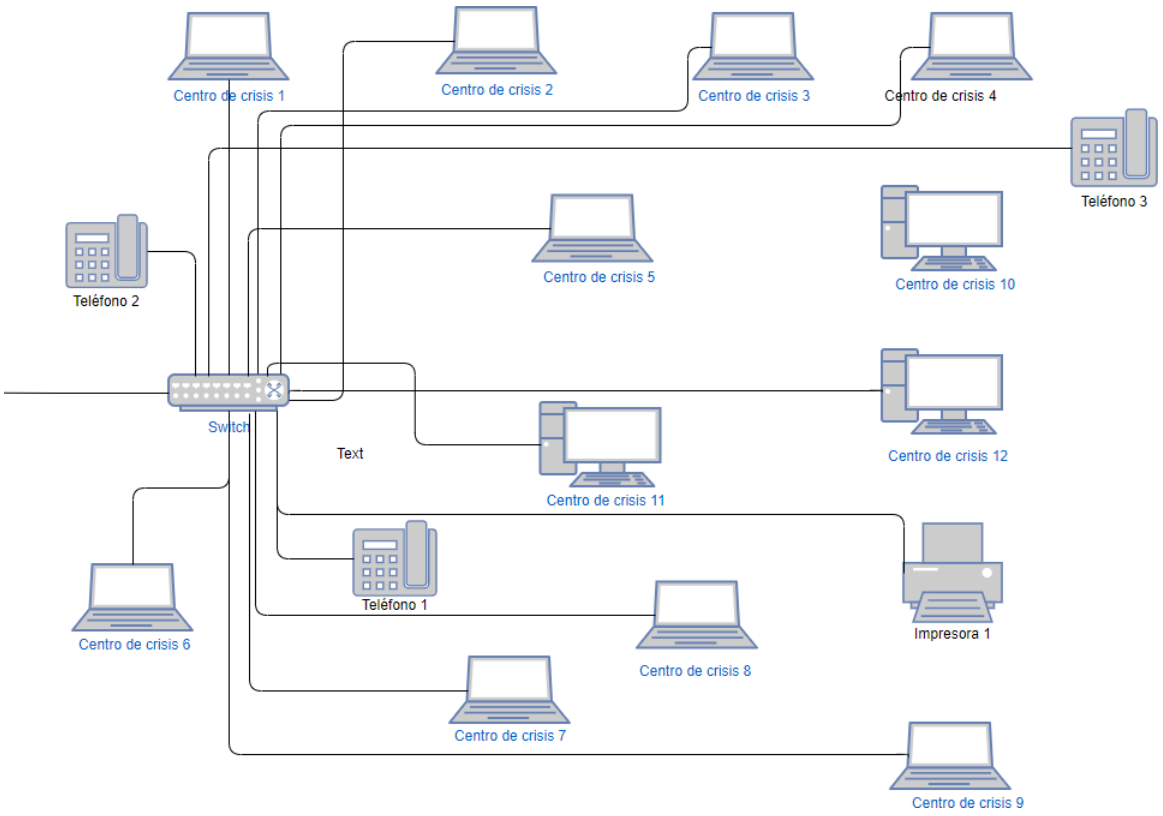
Fuente: Elaboración del autor.

8.11. Esquema centro de Crisis.

El centro de crisis permite tomar acciones inmediatas ante incidentes de seguridad de nivel alto, como lo son los ataques de denegación de servicios DoS, se tiene acceso directo a todas las herramientas de control y monitoreo con que cuenta el CSIRT.

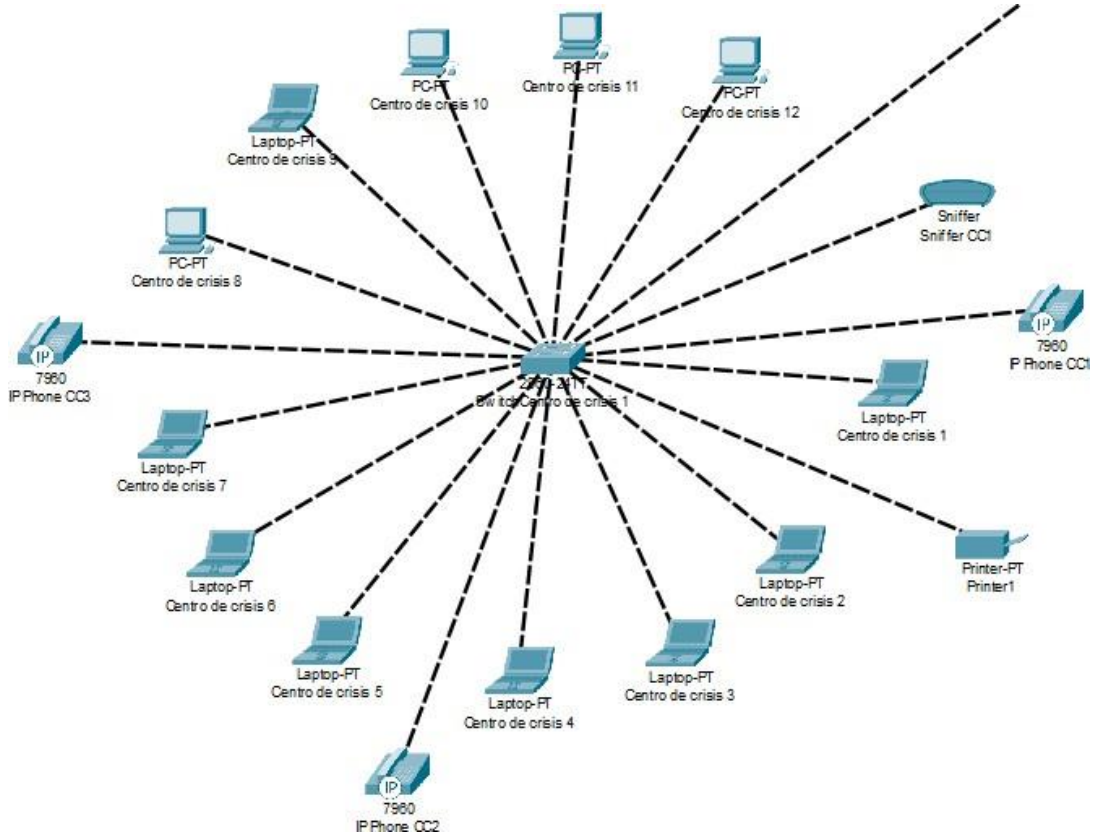
Está compuesto por 9 equipos portátiles, 3 equipos de escritorio, 1 impresora y 3 teléfonos IP.

Ilustración 15 Esquema pictográfico centro de Crisis.



Fuente: Elaboración del autor.

Ilustración 16 Esquema de red creado desde Cisco Packet tracer.



Fuente: Elaboración del autor.

El centro de Crisis se encuentra bajo la Vlan 15, a continuación, se especifica el direccionamiento para cada dispositivo.

Tabla 20 Direccionamiento IP de los dispositivos.

Ubicación	Nombre	Tipo	Red
Centro de Crisis	Centro de crisis 1	Laptop	192.168.15.4
Centro de Crisis	Centro de crisis 2	Laptop	192.168.15.5
Centro de Crisis	Centro de crisis 3	Laptop	192.168.15.6
Centro de Crisis	Centro de crisis 4	Laptop	192.168.15.7
Centro de Crisis	Centro de crisis 5	Laptop	192.168.15.8
Centro de Crisis	Centro de crisis 6	Laptop	192.168.15.9
Centro de Crisis	Centro de crisis 7	Laptop	192.168.15.10
Centro de Crisis	Centro de crisis 8	Laptop	192.168.15.11
Centro de Crisis	Centro de crisis 9	Laptop	192.168.15.12
Centro de Crisis	Centro de crisis 10	Desktop	192.168.15.13

Centro de Crisis	Centro de crisis 11	Desktop	192.168.15.14
Centro de Crisis	Centro de crisis 12	Desktop	192.168.15.15
Centro de Crisis	Teléfono 1	teléfono IP	192.168.14.18
Centro de Crisis	teléfono 2	teléfono IP	192.168.14.19
Centro de Crisis	teléfono 3	teléfono IP	192.168.14.20

Fuente: Elaboración del autor.

A continuación, se presentan las características técnicas de los equipos (hardware).

Tabla 21 Características de los equipos.

Clase	Equipo	Características	procesador	RAM	HDD
Equipos de cómputo de escritorio	HP All-in-One PC 21-b0017la	Equipo de cómputo de alto rendimiento todo en uno marca HP	procesador Intel Core i3 de 10.ª generación o procesador Intel Core i3-1005G1 a 1,2 GHz, hasta 3,4 GHz	4 GB de SDRAM DDR4-3200 (1 x 4 GB)	Unidad interna Disco duro-SATA de 1 TB y 7200 rpm
Portátiles	Portátil HP 14-cf3034la	Equipo portátil de alto rendimiento.	Intel Core i3-1005G1	4 GB de SDRAM DDR4-2666	512 GB SSD

Fuente: Elaboración del autor.

8.12. Listado de Software.

Existen en el mercado una gran variedad de software que puede ser aplicado para las funciones del CSIRT, software especializado, de código abierto o bajo licencia comercial, para la operación del CSIRT de la empresa Cibersecurity de Colombia Ltda se optado por el uso de software Open Source que cumpla con los requerimientos para la prestación del servicio.

A continuación, se relaciona un listado de posible software Open Source a utilizar:

Tabla 22 Listado de Software Open Source para trabajar en el CSIRT.

Software	características
Nessus	Software diseñado para la recuperación de contraseñas, pero también permite cubrir vulnerabilidades de seguridad de caché.[140]
Wireshark	Analizador de protocolos de red, permite realizar análisis en tiempo real del tráfico de la red.[141]
Kali Linux	Sistema operativo Linux diseñado para realizar pruebas de seguridad en modo forense.[142]
Sysinternals	Conjunto de herramientas de administración para Windows.[143]
Karma	Integrador de datos, permite integrar información de varias fuentes para el posterior modelado, automatiza los análisis de los datos.[144]
Wellenreiter	Herramienta de auditoría y control de redes inalámbricas, permite extraer información de la red para análisis, soporta protocolos DHCP y ARP.[145]
FlawFinder	Software que permite analizar código fuente C y C + + en búsqueda de vulnerabilidades clasificadas por nivel de riesgo.[146]
OSSIM	Software de recopilación, normalización y análisis de eventos, permite realizar evaluación de vulnerabilidades, detección de instrucciones, monitoreo del comportamiento[147]

[140]tenable. «LA FAMILIA NESSUS.» 2020. [en línea] https://es-la.tenable.com/products/nessus
[141]Wireshark.org. «Wireshark.» 2020. [en linea] https://www.wireshark.org/.
[142]Kali. «Kali - The Most Advanced Penetration Testing Distribution.» 2020. [en linea] https://www.kali.org/.
[143]Microsoft. «Windows Sysinternals.» 2021. [en linea] https://docs.microsoft.com/en-us/sysinternals/.
[144]Karma. «Karma.» 2020. [en linea] https://karma-runner.github.io/latest/index.html.
[145]Wellenreiter. «Welcome to the project page of wellenreiter.» -. [en linea] http://wellenreiter.sourceforge.net/.
[146]Flawfinder «Flawfinder.» 2020. [en linea] https://dwheeler.com/flawfinder/.
[147]AT&T . «AlienVault OSSIM.» -. en linea] https://cybersecurity.att.com/products/ossim

Syslog-NG	Sistema de gestión de registros de eventos, permite análisis miles de registros de forma rápida, además contiene un espacio seguro de almacenamiento.[148]
Rootkit Detective	Herramienta que permite la eliminación de rootkits complejos.[149]
AppArmor	Sistema de control de acceso obligatorio basado en módulos, su función es validar la autorización de un proceso antes de ejecutarse, se aplica con base a reglas sobre cada aplicativo así se controlan recursos y procesos no autorizados.[150]
Areca Backup	Sistema de copias de seguridad personal, permite mantener la información en ubicaciones seguras para luego ser enviada.[151]
Sentry	Sistema de auditoría de error en código fuente, analiza el código y muestra los errores de sintaxis y de aplicación.[152]
DansGuardian	Software de control de contenido, su función es controlar el acceso a los sitios web, contiene filtros para virus.[153]
Zabbix	Software para monitorear el rendimiento y la capacidad de operación de servidores, aplicaciones, equipos de cómputo y sistemas de bases de datos, permite crear alertas ante eventos.[154]
Graylog	Es una herramienta que permite la administración y gestión de registros de datos, está diseñado con una base de datos MongoDB.[155]

[148]syslog. «syslog-ng.» 2020. [en linea] https://www.syslog-ng.com/trials/.
[149]McAfee. «RootkitRemover.» 2020. [en linea] https://www.mcafee.com/enterprise/es-es/downloads/free-tools/rootkitremover.html.
[150]Debian. «El manual del Administrador de Debian.» -. [en linea] https://debian-handbook.info/browse/es-ES/stable/sect.apparmor.html.
[151]Areca Backup. «Areca Backup.» -. [en linea] http://www.areca-backup.org/.
[152]SENTRY. «Sentry for Open Source.» -. [en linea] https://sentry.io/for/open-source/.
[153]EcuRed. «DansGuardian.» -. [en linea] https://www.ecured.cu/DansGuardian.
[154]Zabbix. «Network Monitoring.» -. [en linea] https://www.zabbix.com/network_monitoring.
—. «Zabbix.» 2020. [en linea] https://www.zabbix.com/.
[155]Jerónimo, Javier. «Graylog – Arquitectura tolerante a fallos y escalable.» 2015. [en linea] https://javierjeronimo.es/2015/03/23/graylog-arquitectura-tolerante-a-fallos-y-escalable/.

Urbackup	Software Open Source que permite realizar copias de seguridad completas, diferenciales e imágenes completas del sistema.[156]
Firejail	Herramienta open Source, está escrita sobre lenguaje de programación C, cuenta con interfaz gráfica o puede trabajarse desde la terminal para crear sandboxing dentro del sistema Linux.[157]

Fuente: Elaboración del autor luego de consulta realizada en internet.

Del listado anterior se seleccionó las siguientes herramientas para el desarrollo de los laboratorios: Zabbix, Graylog, Urbackup y Firejail

[156]Protege.la. «UrBackup.» -. [en linea] https://protege.la/urbackup/#:~:text=UrBackup%20es%20una%20herramienta%20Open,versiones%20(cliente%20y%20servidor).

[157]La mirada del replicante. «Aislando aplicaciones del resto del sistema con Firejail.» 2017. [en linea] https://lamiradadelreplicante.com/2017/04/10/aislando-aplicaciones-del-resto-del-sistema-con-firejail/#:~:text=Firejail%20es%20una%20herramienta%20escrita,un%20entorno%20con%20privilegios%20limitados

9. DISEÑO DE LOS AMBIENTES CONTROLADOS Y LA PROPUESTA DE ARQUITECTURA FUNCIONAL DEL CSIRT.

Como parte final del proceso de diseño del CSIRT, se realizó la evaluación del software Open Source seleccionando anteriormente, para esto se crearon máquinas virtuales sobre VMware Workstation 16 bajo ambientes controlados.

se realizó la virtualización de los siguientes servidores:

Servidor de Monitoreo – Software Zabbix

Correlacionador de Eventos – Software Graylog

Servidor de Copias de Seguridad – Software Urbackup

Servidor Sandbox – Software Firejal

9.1. Servidor de monitoreo – software Zabbix.

Zabbix es un sistema de monitoreo de redes diseñado bajo licencia Open Source y creado por Alexei Vladished, el aplicativo es capaz de realizar monitoreo en tiempo real de los eventos ocurridos en los servicios de red, servidores, hardware y aplicaciones en los equipos que cuentan con su agente instalado.[158]

Características:

Capacidad de monitoreo elevado y alto rendimiento.[159]

Permite realizar monitoreo centralizado mediante su ambiente web.[160]

Sus agentes son compatibles con sistemas operativos como Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows 2000, Windows Server

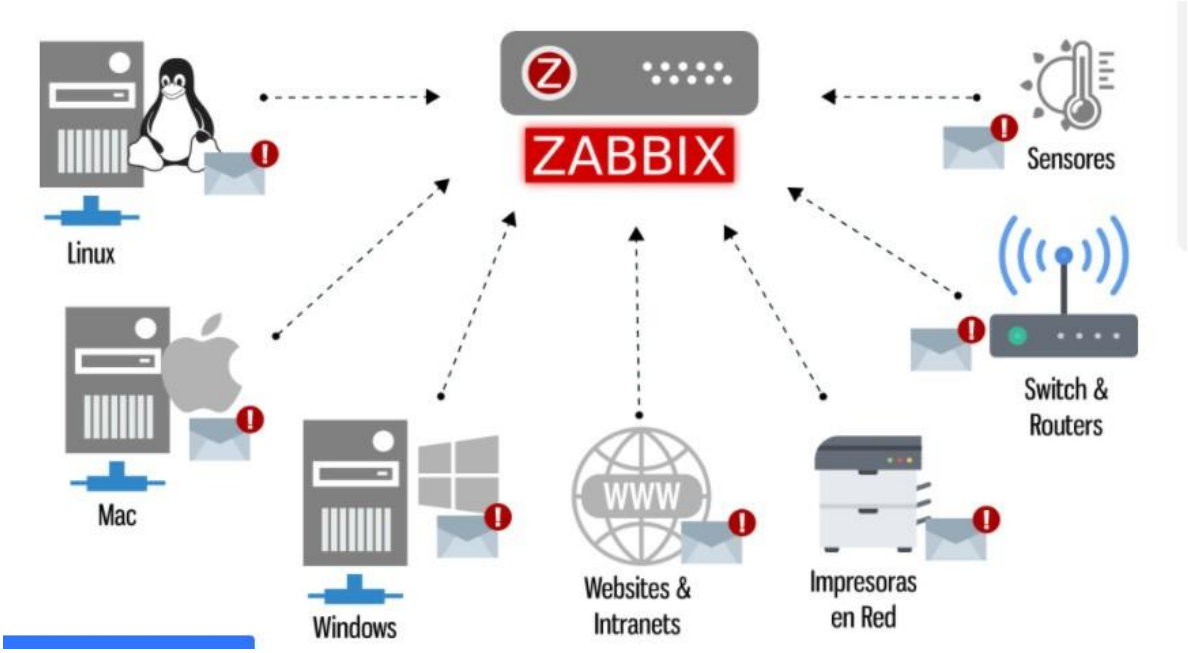
[158]Hernandez, Juan Estuardo. «Conoce como funciona Zabbix y como usarlo.» 2013. [en linea] http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo.
[159]Ibid P 1
[160]Ibid P 1

2003, Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows 8 y recientemente Windows 2012.[161]

Permite realizar al mismo tiempo inventario de equipos y mapas de red, es multiplataforma, soporta base datos MySQL, Oracle, SQlite y Postgres.[162]

Su funcionamiento consiste en la instalación del servicio sobre una plataforma Linux, en este caso CentOS, se debe configurar el direccionamiento IP para que pueda recopilar información mediante los agentes, se almacena la información en su base de datos y se consulta por medio de la interfaz web.

Ilustración 17 Como funciona Zabbix.



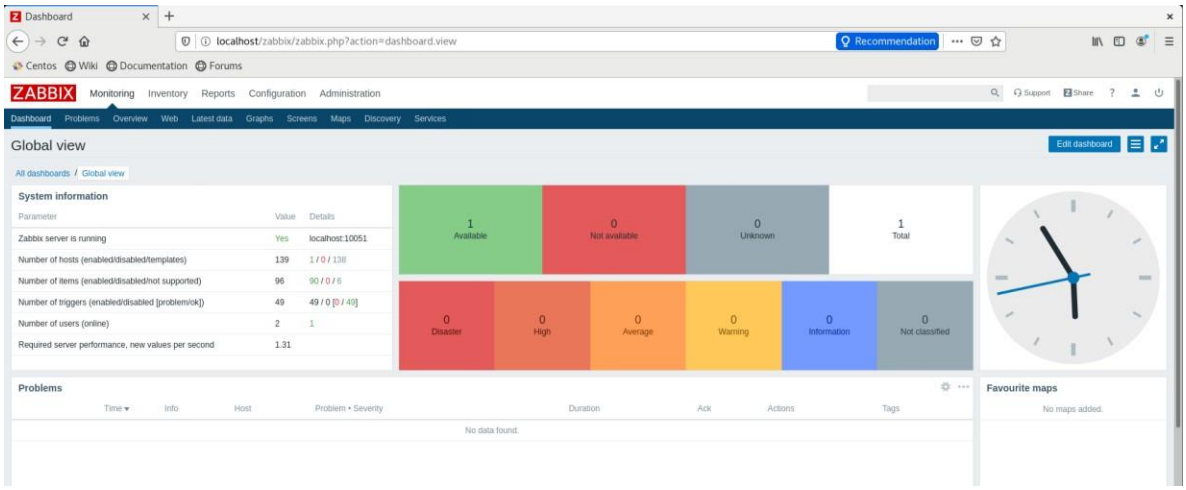
Fuente: Hernandez, Juan Estuardo. «Conoce como funciona Zabbix y cómo usarlo.» 2013. [en línea] http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo.

Se selección esta herramienta debido a que es totalmente Open Source y se encuentra documentación sobre su uso y configuración gracias a su página principal y a comunidades que colaboran entre sí para mejorar el producto.

[161]Hernandez, Juan Estuardo. «Conoce como funciona Zabbix y como usarlo.» 2013. [en linea] http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo.
[162]Zabbix. «Zabbix.» 2020. [en linea] https://www.zabbix.com/.

Para la implementación del servidor de monitoreo, se ha realizado la instalación de una máquina virtual Linux CentOS sobre VMware Workstation 16, CentOS es una edición Linux de grado Enterprise, es utilizado tanto en escritorios como para uso de servidores por ser muy robusto y estable, está diseñado sobre código RHEL.[163]

Ilustración 18 Detalle del Dashboard de Zabbix, interfaz gráfica.



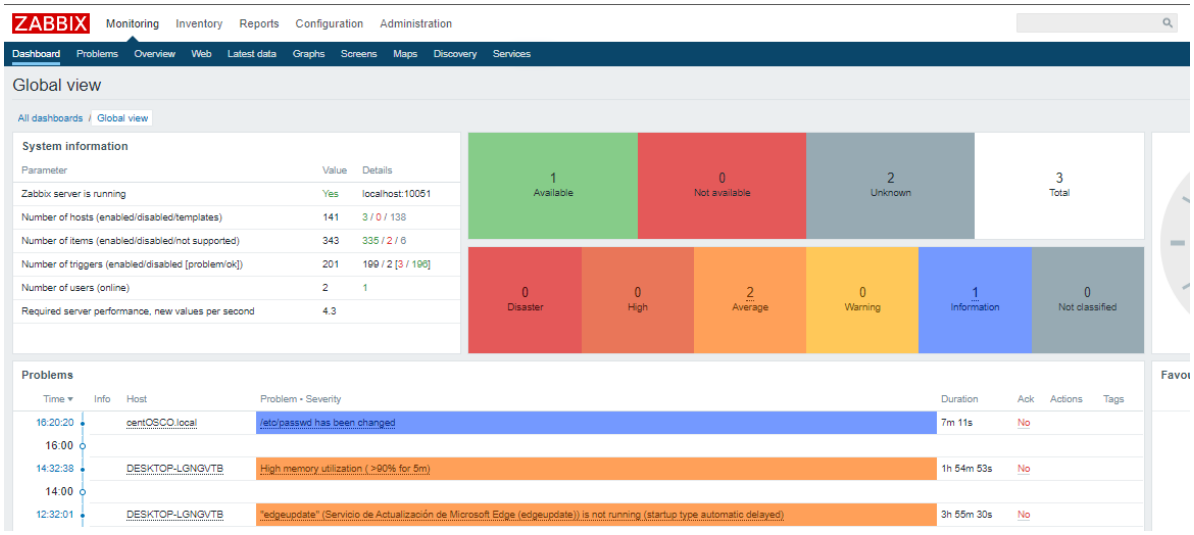
Fuente: Elaboración del autor.

En la imagen se detalla el entorno grafico del servidor Zabbix, detallando el estado del equipo o equipos que están bajo monitoreo.

Para esta práctica se realiza la instalación del agente Zabbix sobre dos sistemas distintos, Windows 10 pro (DESKTOP-LGNGVTB) y CentOS 8 (centOSCO.local), una vez instalado el agente, el servidor Zabbix comienza a recibir la información de los equipos.

[163]Digital Guide IONOS. «¿Qué es CentOS? Versiones CentOS y requisitos del sistema.» 2020. [en linea] https://www.ionos.es/digitalguide/servidores/know-how/que-es-centos-versiones-y-requisitos-del-sistema/.

Ilustración 19 Panel Zabbix con reporte equipo DESKTOP-LGNGVTB

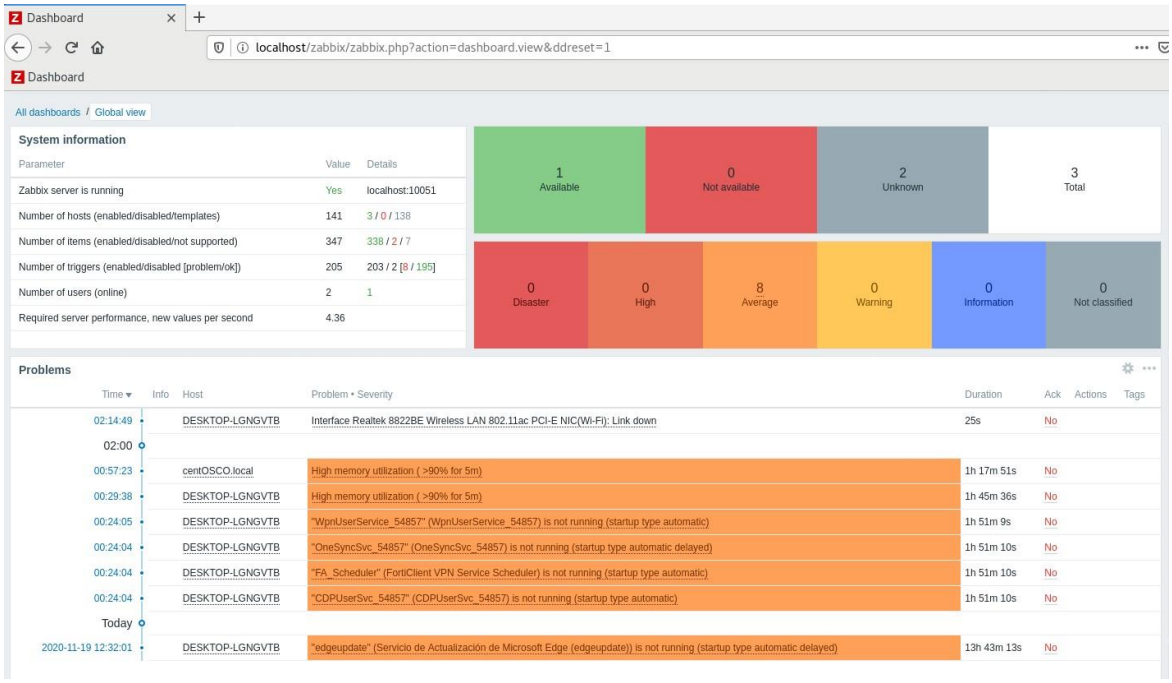


Fuente: Elaboración del autor.

En la imagen se observa que Zabbix ha detectado cambio en el archivo /etc/passwd en el equipo centOSCO.local, puede ser asociado a un cambio en la configuración, labores administrativas con el usuario “su” (root) o posibles ataques a la seguridad del sistema.

El proceso de identificación de alertas de Zabbix permite tomar medidas sobre el posible incidente de seguridad registrado, identificando un posible acceso no autorizado al sistema del servidor monitoreado.

Ilustración 20 Alerta por consumo de memoria swap alta.



Fuente: Elaboración del autor.

En la imagen se observa que Zabbix ha detectado un alto consumo de la memoria de intercambio swap, posiblemente por demasiados procesos ejecutándose, pero es una alerta que se debe revisar ya que puede ser algún proceso malicioso.

9.2. Correlacionador de Eventos – Software Graylog.

Para el servidor Correlacionador de Eventos se ha empleado la herramienta Open Source Graylog, es una herramienta que permite la administración y gestión de registros de datos, está diseñado con una base de datos MongoDB, Elasticsearch y Scala, su función es trabajar como un sistema centralizado de control de logs, es un sistema tolerante a fallos capaz de soportar varias arquitecturas.[164]

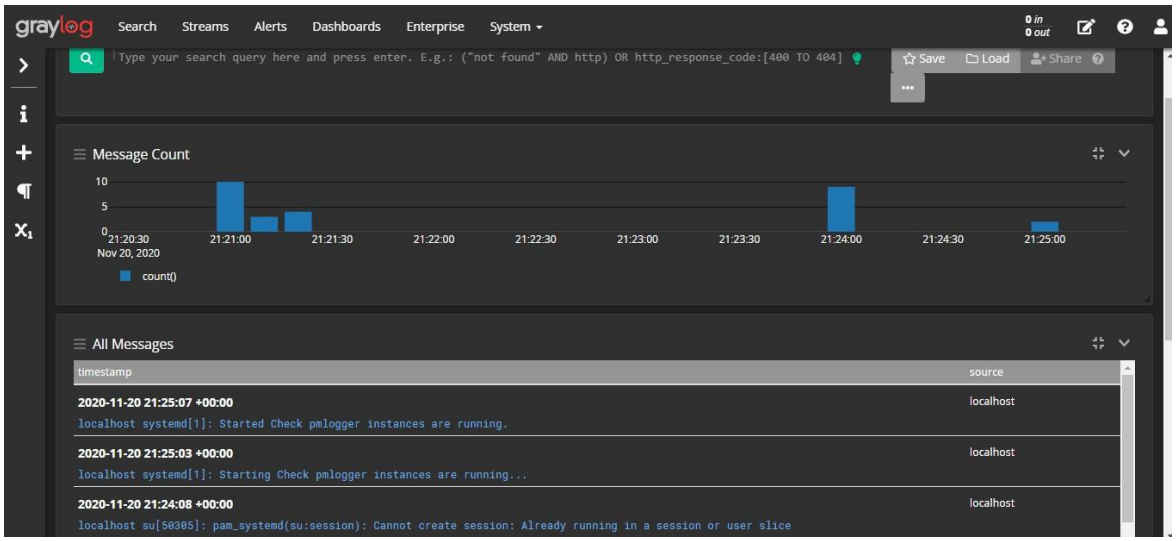
Cuenta con un servidor principal encargado de recibir y almacenar la información recibida por los agentes instalados en los equipos, al igual que Zabbix su interfaz es web, lo que permite si se tiene el acceso, consultarlo desde cualquier equipo que este en la misma red que el servidor.[165]

[164]Jerónimo, Javier. «Graylog – Arquitectura tolerante a fallos y escalable.» 2015. [en linea] https://javierjeronimo.es/2015/03/23/graylog-arquitectura-tolerante-a-fallos-y-escalable/.
[165]DesdeLinux. «Graylog, una herramienta para la administración y análisis de registros.» -. [en linea] https://blog.desdelinux.net/graylog-una-herramienta-para-la-administracion-y-analisis-de-registros/.

Su funcionamiento está basado en la lectura de los logs de eventos, los analiza y los presenta en forma compresible para el usuario además permite realizar búsquedas avanzadas mediante consultas estructuradas.[166]

Se selección esta herramienta Open Source por altamente escalable y robusto, lo que permite el monitoreo de grandes cantidades de servidores y equipos de forma óptima.

Ilustración 21 Detalle del Dashboard de Graylog, interfaz gráfica.

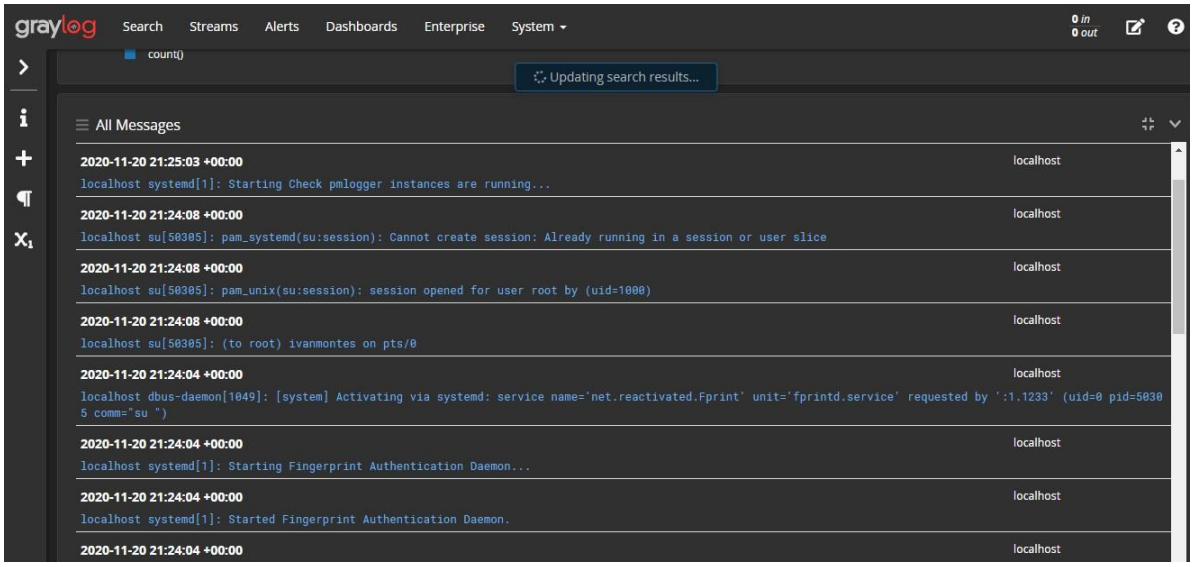


Fuente: Elaboración del autor.

En la imagen se puede visualizar el registro de logs obtenidos desde el servidor de monitoreo en un tiempo determinado, Graylog toma todos los logs desde el equipo luego de ser instalado el agente de conexión, interpreta los logs en bruto por medio de syslog y los muestra en forma comprensible y ordenada para el usuario

[166]DesdeLinux. «Graylog, una herramienta para la administración y análisis de registros.» -. [en linea] https://blog.desdelinux.net/graylog-una-herramienta-para-la-administracion-y-analisis-de-registros/.

Ilustración 22 Registro detallado de logs del servidor de monitoreo.

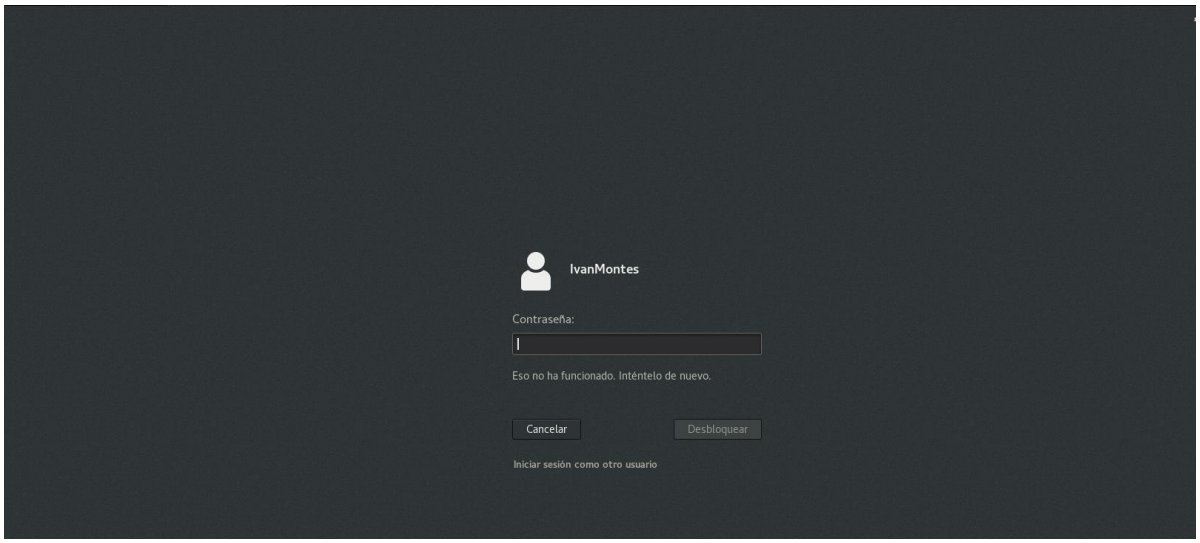


Fuente: Elaboración del autor.

A continuación, se relacionan los logs que han sido leídos por Graylog, se aprecian logs relacionados con la red e inicio de sesión.

El primer log indica la verificación realizada por el sistema sobre el inicio de instancias.

Ilustración 23 Verificación del registro de los logs.



Fuente: Elaboración del autor.

En la imagen se realiza una prueba ingresando las credenciales del usuario IvanMontes de forma incorrecta para verificar que se reporta el evento en Graylog.

Ilustración 24 Verificando logs de clave incorrecta.

Fuente: Elaboración del autor.

En la imagen se aprecia el registro sobre el intento de ingreso con clave incorrecta que se realizó sobre el servidor de monitoreo, se detalla nombre de usuario, hostname del equipo además de la hora del evento.

Esta información permite identificar posibles intentos no autorizados de acceso a al sistema monitoreado, Graylog permite de esta forma mantener control sobre los sistemas y una eventual atención ante posibles incidentes de seguridad.

9.3. Servidor de Copias de Seguridad – Software Urbackup.

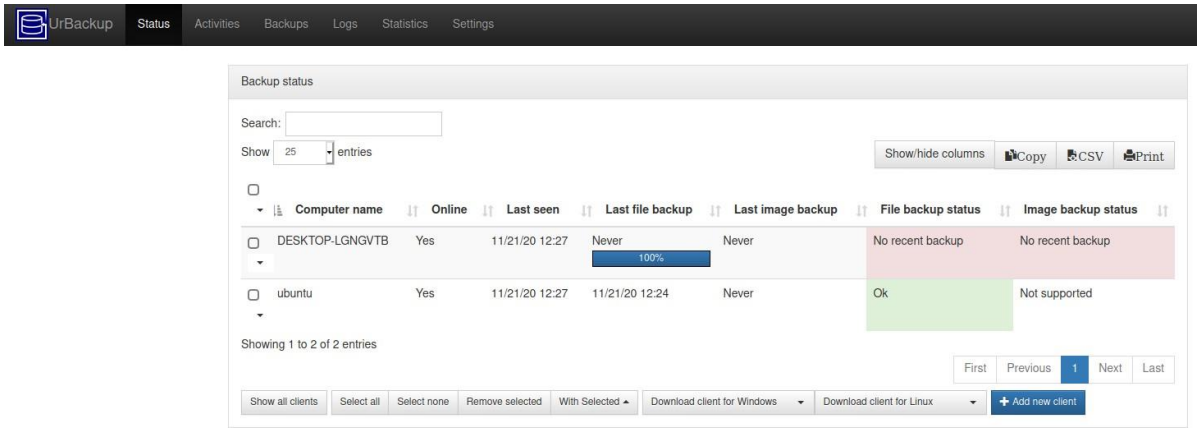
Para el servidor de copias de respaldo se emplea la herramienta open Source UrBackup él tiene un módulo del lado del servidor para gestionar las copias de seguridad y un agente para la conexión de los equipos al servidor, permite realizar backup completos, diferenciales e imágenes completas del sistema.[167]

Una ventaja es que es multiplataforma tanto para el servidor como para el agente, además los procesos de backup se realizan mientras los sistemas están activos, no es necesario detener las acciones que se realizan en ellos, cada cierto tiempo realiza un escaneo de las carpetas que se seleccionaron para copia en busca de cambios de los archivos y así crear backup incrementales.[168]

[167]Protege.la. «UrBackup.» -. [en linea] https://protege.la/urbackup/#:~:text=UrBackup%20es%20una%20herramienta%20Open,versiones%20(cliente%20y%20servidor).
[168]Ibid P 1

El proceso de restauración de la información se puede realizar directamente desde la interfaz web o desde el explorador de archivos ingresando al servidor y al respaldo.

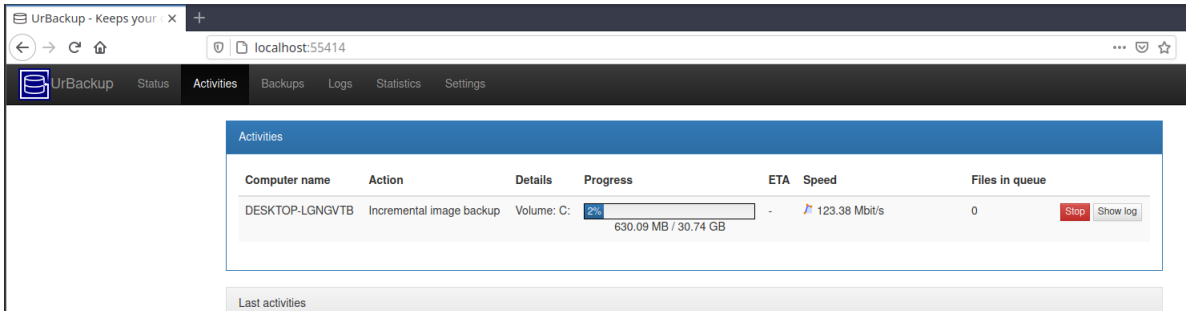
Ilustración 25 Detalle del Dashboard de Urbackup, interfaz gráfica.



Fuente: Elaboración del autor.

En la imagen se muestra el detalle de dos tareas de copia de información para dos equipos, la primera tarea sobre un equipo con sistema Windows cuenta con una copia de seguridad inicial en proceso mientras que la segunda tarea realiza a un equipo con sistema Ubuntu se encuentra finalizada

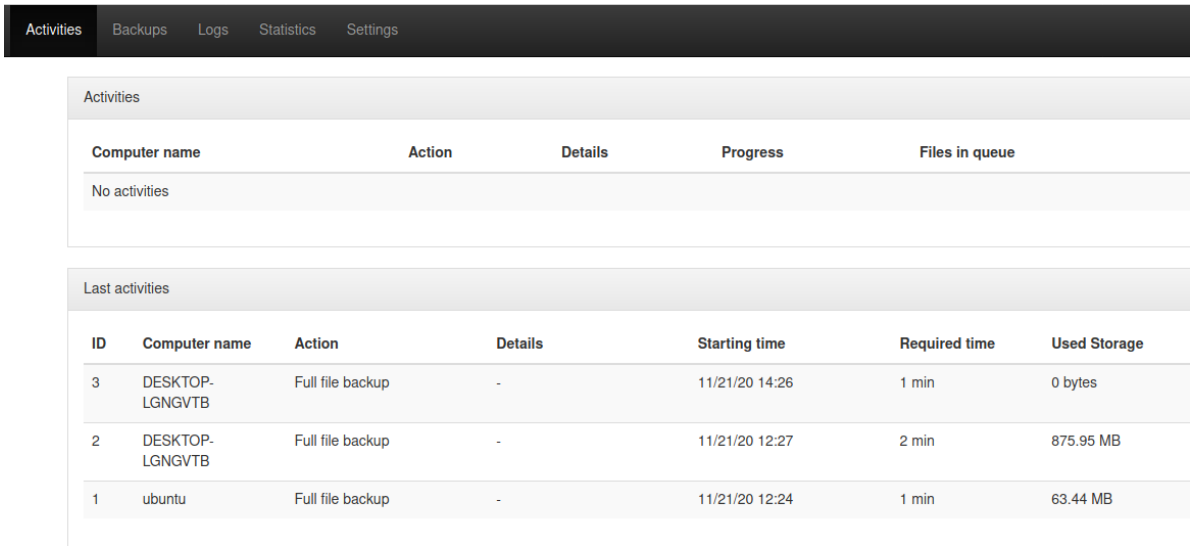
Ilustración 26 Proceso backup incremental sobre equipo Windows 10.



Fuente: Elaboración del autor.

El proceso se inicia de forma automática tan pronto el servidor registra el equipo, se crea una copia de seguridad inicial completo del equipo, según la parametrización establecidas de carpetas a respaldar, luego de esto, al identificarse cambios en los archivos, se inicia la tarea de backup incremental para guardar los últimos cambios realizados.

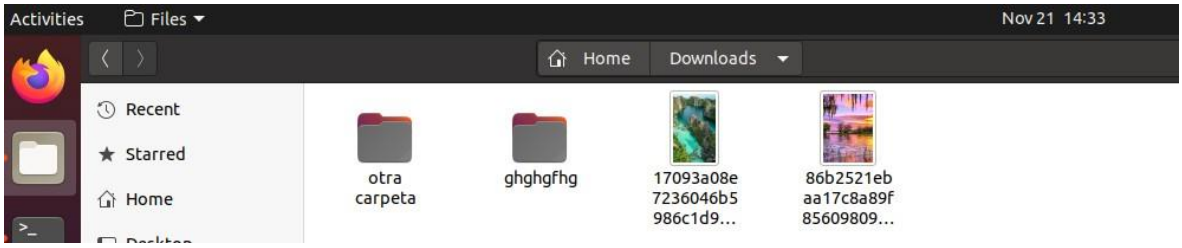
Ilustración 27 Detalle de las actividades en proceso.



Fuente: Elaboración del autor.

Se detalla el proceso completo de copia de seguridad al equipo Windows 10 pro (DESKTOP-LGNGVTB) y al equipo Ubuntu conectados en la red, se indica el estado de la copia de información, el tiempo transcurrido y la cantidad de información almacenada.

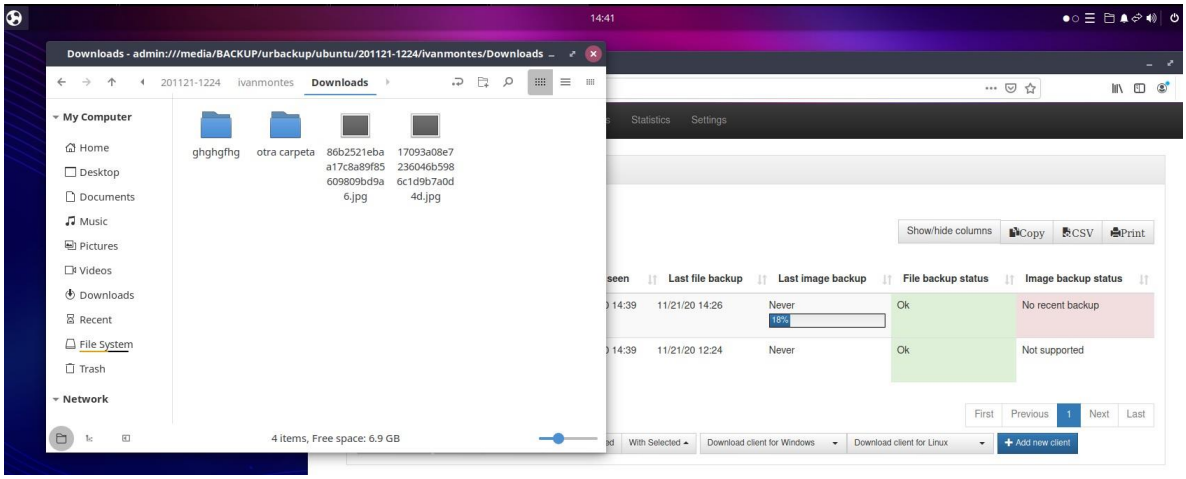
Ilustración 28 Detalle carpeta “Downloads” del equipo Ubuntu.



Fuente: Elaboración del autor.

Elementos guardados en la carpeta descargas del equipo Ubuntu del cual se realizó copia de seguridad.

Ilustración 29 Verificación copia de seguridad.



Fuente: Elaboración del autor.

Verificación de copia de seguridad en el servidor de copias de seguridad, detalle de la carpeta “Downloads” del usuario ivanmontes sobre el equipo Ubuntu, se identifica que la copia de seguridad se realizó correctamente.

9.4. Servidor Sandbox – Software Firejal.

Para la implementación del servidor Sandbox se he seleccionado la herramienta open Source Firejail, está escrita sobre lenguaje de programación C, cuenta con interfaz gráfica o puede trabajarse desde la terminal para crear sandboxing dentro del sistema Linux.

Firejail es una herramienta SUID diseñada para reducir los incidentes de seguridad al evitar la ejecución de aplicaciones o enlaces que se consideran sospechosos en entornos de producción, Firejail crea un espacio independiente de ejecución permitiendo que un proceso tenga acceso a los recursos del kernel en una vista privada.[169]

Una ventaja de Firejail es que permite la ejecución de cualquier proceso, desde servidores, aplicación graficas o de terminal hasta sesiones de usuarios.[170]

[169]Ubunlog. «Firejail, ejecuta de forma segura aplicaciones no confiables en Ubuntu.» -. [en linea] https://ubunlog.com/firejail-ejecuta-aplicaciones-ubuntu/.
[170]Ibid P 1

Entre sus principales características se encuentran[171]:

Contenedor del sistema de archivos.

Filtros de seguridad.

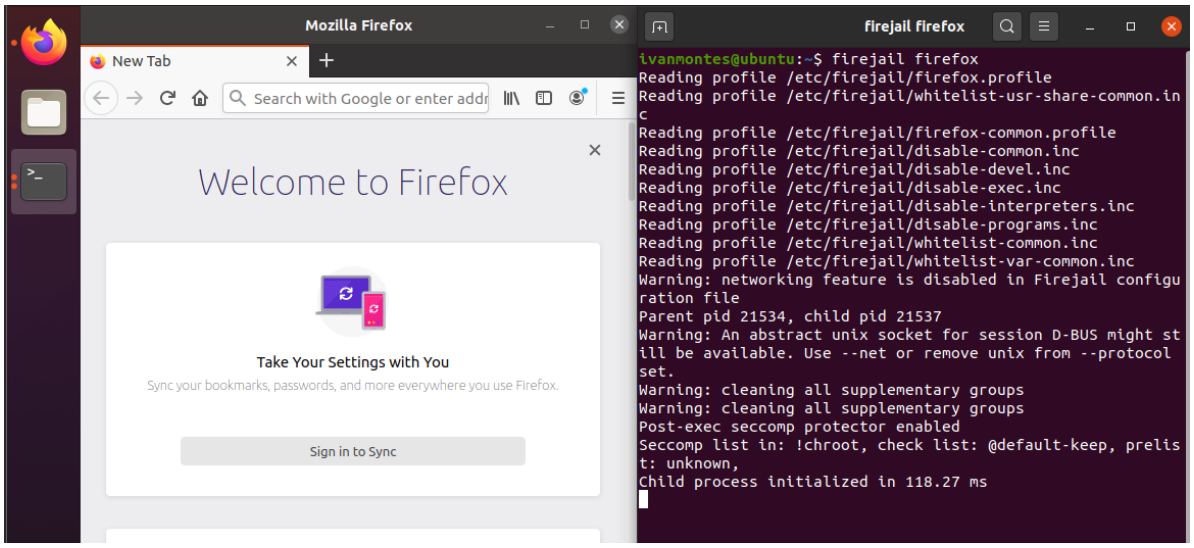
Compatibilidad con redes.

Perfiles de seguridad.

Asignación de recursos.

Para su ejecución se debe colocar la sintaxis Firejail [aplicación a ejecutar] de esta forma el aplicativo se ejecuta bajo los permisos del usuario sobre el cual se ejecuta bajo condiciones limitadas, es decir si en total de acceso que normalmente tiene la aplicación.[172]

Ilustración 30 Ejecución de Firefox sobre sandbox Firejail**.**



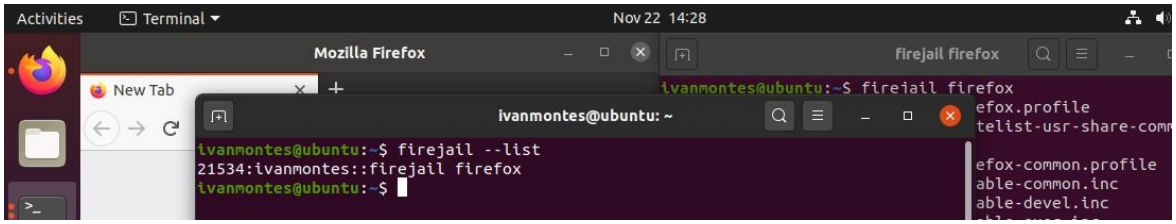
Fuente: Elaboración del autor.

[171]Ubunlog. «Firejail, ejecuta de forma segura aplicaciones no confiables en Ubuntu.» -. [en linea] https://ubunlog.com/firejail-ejecuta-aplicaciones-ubuntu/.

[172]La mirada del replicante. «Aislando aplicaciones del resto del sistema con Firejail.» 2017. [en linea] https://lamiradadelreplicante.com/2017/04/10/aislando-aplicaciones-del-resto-del-sistema-con-firejail/#:~:text=Firejail%20es%20una%20herramienta%20escrita,un%20entorno%20con%20privilegios%20limitados.

En la imagen se aprecia la ejecución del aplicativo Firefox sobre Firejail con funciones limitadas y bajo un ambiente controlado, en este modo es posible evaluar las condiciones de seguridad de la aplicación sin exponer directamente al equipo.

Ilustración 31 verificación de aplicaciones.



Fuente: Elaboración del autor.

Mediante la ejecución del comando firejail –list se puede comprobar el aplicativo o aplicativos que se están ejecutando bajo ambientes controlados Sandbox.

La aplicación de esta herramienta dentro del CSIRT es fundamental al permitir el análisis de posibles amenazas en los navegadores web, ya sea por plugin instalados o por acceso a paginas no seguras, además permite comprar enlaces sospechosos y aplicaciones no seguras sin afectar los equipos que están en producción.

10. ANALISIS DE LOS RESULTADOS OBTENIDOS.

Luego de realizar la investigación preliminar, se presenta a continuación los resultados obtenidos, estos resultados darán una visión global del problema de ciberseguridad existente hoy en día y como un nuevo CSIRT ayudara a enfrentar los incidentes de seguridad que se presenten.

10.1. Establecer los lineamientos de operación de un CISRT.

Durante la investigación se encontró información relevante sobre los lineamientos de operación de un CSIRT, para el diseño del CSIRT del Cibersecurity de Colombia Ltda. Se aplicaron los conceptos y esquemas de funcionamiento recomendados por Enisa[173], OEA[174], Centro Criptográfico Nacional de España[175] entre otros logrando el diseño de un sistema ante incidentes informáticos robusto, adaptado a las necesidades de proteccion del país.

La propuesta de diseño de un CSIRT para a empresa Cibersecurity de Colombia Ltda, es una aproximación a los aspectos administrativos, técnicos y lógicos además de una clara explicación a los procesos, procedimientos y políticas de seguridad con que debe iniciar cualquier CSIRT en la actualidad.

10.2. Establecer las métricas de evaluación de los posibles incidentes.

Bajo este objetivo se identificó el conjunto de mejores métricas a aplicar dentro de un CSIRT, esta información fue tomada en su mayoría de la Guía nacional de notificación y gestión de ciberincidentes INCIBE[176] y del Centro Criptográfico Nacional de España [177] por su amplia experiencia en la operación y creación de CSIRT, las métricas permiten llevan el control en la atención de incidentes de

[173]Enisa csirt. «Cómo crear un CSIRT paso a paso.» 2006. [en linea]. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-n9P4muDvAhXwEVkFHfN3A_4QFjAAegQIAxAD&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcsirt-setting-up-guide-in-spanish%2Fat_download%2FfullReport&usg=AOvVaw2F8Wp_02LEvZ-NMA.

[174]OEA. «Buenas Prácticas para establecer un CSIRT nacional.» 2016. [en linea] https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

[175]Centro Criptografico Nacional. «Guía de Creación de un CERT/CSIRT.» 2011. [en linea] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.

[176]INCIBE. «Guía nacional de notificación y gestión de ciberincidentes.» 2020. [en linea] https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes

[177]

ciberseguridad, además permiten evaluar el cumplimento de los ANS (acuerdo de nivel de servicio) y la calidad del servicio prestado.

Las métricas indicadas en este trabajo son las mínimas para la puesta en funcionamiento de un CSIRT, las métricas deben adaptarse al alcance propio del CSIRT y las entidades a las que se les prestara servicio.

10.3. Proponer una estructura operativa y una infraestructura funcional.

Aunque existen una gran variedad de modelos organizacionales, luego de la investigación se llegó a la conclusión que el CSIRT debe operar bajo el concepto de un Modelo integrado en una organización preexistente de esta forma debe estar bajo una estructura organizacional definida y un modelo operacional independiente, bajo sus propias normas, equipo de trabajo y controles para mantenerse operativamente hablando independiente del resto de la oficina de tecnologías de la información y no tener injerencia directa en la infraestructura de la empresa.

10.4. Diseñar ambientes controlados con una propuesta de arquitectura funcional.

Luego del análisis de las diferentes herramientas de monitoreo y control presentes en el mercado y cumpliendo con el requisito de usar únicamente software Open Source, se estableció el uso de un conjunto de herramientas que cumplen a cabalidad con el objetivo de efectuar el control de monitoreo (Zabbix[178], Graylog[179], Urbackup[180], Firejal[181]) , una vez completado este paso y luego de la creación de los ambientes contralados se comprobó la efectividad y funcionalidad del software seleccionado, se pudieron realizar prácticas de análisis de logs de eventos, monitoreo de red, pruebas en sandbox y pruebas de backup de equipos dentro de la infraestructura lo que demuestra la aplicabilidad de estos sistemas dentro del funcionamiento del CSIRT, es de aclarar que existen números aplicativos Open Source para realizar estas tareas pero no todas realizan las mismas funciones de

[178]Hernandez, Juan Estuardo. «Conoce como funciona Zabbix y como usarlo.» 2013. [en linea] http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo.
[179]Jerónimo, Javier. «Graylog – Arquitectura tolerante a fallos y escalable.» 2015. [en linea] https://javierjeronimo.es/2015/03/23/graylog-arquitectura-tolerante-a-fallos-y-escalable/.
[180]Protege.la. «UrBackup.» -. [en linea] https://protege.la/urbackup/#:~:text=UrBackup%20es%20una%20herramienta%20Open,versiones%20(cliente%20y%20servidor).
[181]Ubunlog. «Firejail, ejecuta de forma segura aplicaciones no confiables en Ubuntu.» -. [en linea] https://ubunlog.com/firejail-ejecuta-aplicaciones-ubuntu/.

monitoreo ni cuentan con módulos adicionales Open Source y/o documentación necesaria para su implementación y mantenimiento.

11. CONCLUSIONES.

El desarrollo del presente trabajo permitió identificar las características fundamentales de un CSIRT para la atención de incidentes de seguridad informática, permito establecer sus principales ejes de actuación al igual que su marco operacional, estableciendo los lineamientos para una posible implementación a futuro, la defensa de las infraestructuras ya sean públicas o privadas se han convertido en una necesidad vital en estos tiempos debido al aumento de los ataques reportados, el diseño técnico planteado busca obtener un sistema de respuesta ante incidentes cibernéticos eficiente reuniendo un conjunto de recomendaciones técnicas y procedimentales que sean comprobado a nivel mundial por organizaciones de renombre y que aplicadas correctamente conforman junto al personal humano un escudo de proteccion digital.

Se pudo analizar el funcionamiento interno de un CSIRT, algunas herramientas de control reactivo y/o proactivo y como la aplicación de controles de seguridad informática impacta positivamente a las organizaciones, cada día los ataques cibernéticos son más complejos y elaborados, lo que dificulta la proteccion de los activos de información por parte de las organizaciones, un CSIRT permite controlar estos activos de forma eficiente manteniendo controles, políticas y planes de acción específicas para cada organización que está bajo su protección.

Permitió establecer el conjunto de políticas básicas con que debe contar un CSIRT para entrar en operación además del modelo de asimilación de controles para lograr una correcta supervisión y atención de los incidentes identificados. Permitió determinar los procesos con sus correspondientes métricas de análisis de resultados basados en los acuerdos de nivel de servicios que se establezcan para cada organización.

Se estableció una estructura jerárquica y de infraestructura que permite la operación de un CSIRT de forma casi inmediata, estableciendo los componentes de red necesarios para su correcto funcionamiento además de un conjunto de herramientas de software y hardware capaz de ofrecer una solución a las necesidades de monitoreo y control.

Se realizo la montaje y puesta en marcha de los servidores de control necesarios para el análisis de vulnerabilidades dentro de la infraestructura del CSIRT, estas aplicaciones son de tipo open Source y facilitan su instalación, además mediante

sus características permiten realizar un análisis detallado del tráfico de red, de los eventos de sistema registrados en los servidores y activos de información más importantes, de forma que se puede llevar un control detallado sobre la seguridad informática, estas herramientas son de son fácil instalación y uso, lo que permite la puesta en funcionamiento en tiempos cortos de implementación.

12. RECOMENDACIONES.

El diseño de un CSIRT está fundamentado por su capacidad de respuesta ante los incidentes de seguridad informática y por los servicios que decide prestar, por más grande y robusto que sea un CSIRT, la cantidad de servicios ofrecidos para la seguridad informática son demasiados y no se pueden prestar todos al tiempo, es importante definir desde el principio el alcance que tendrá el CISRT para poder establecer claramente las políticas, los procesos y los procedimientos a implementar más adelante.

La selección de las herramientas de monitoreo debe estar sustentadas en la obtención del mejor sistema, en este caso se utilizaron herramientas Open Source, totalmente funcionales y con grandes características, las cuales permiten realizar un detallado análisis de los equipos conectados a la red y de los eventos ocurridos.

13. BIBLIOGRAFIA.

Andrade, Roberto. Fuertes, Walter. Diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: escuela politécnica del ejército. -. [en línea]. [Fecha de consulta: 10 de marzo de 2021]. disponible en: https://repositorio.espe.edu.ec/bitstream/21000/6972/1/AC-GRT-ESPE-47091.pdf.

Areca Backup, Areca Backup. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: http://www.areca-backup.org/

Amenazas del cibercrimen en Colombia 2016 -2017. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Asobancaria. Alianza del pacifico: fomentando la seguridad digital a través de la cooperación. 2019. [en línea]. [Fecha de consulta: 10 de marzo de 2021]. disponible en: https://www.csirtasobancaria.com/sala-de-prensa/alianza-del-pacifico-fomentando-la-seguridad-digital-a-atraves-de-la-cooperacion.

AT&T Cybersecurity, AlienVault OSSIM the world's most widely used open source SIEM. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://cybersecurity.att.com/products/ossim

BA-CSIRT. ¿Qué es ba-csirt? 2020. [en línea]. [Fecha de consulta: 10 de marzo de 2021]. disponible en: https://www.ba-csirt.gob.ar/index.php?u=quienes-somos.

BID - OEA. Riesgos, avances y el camino a seguir en américa latina y el caribe. 2020. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Buenas Prácticas para establecer un CSIRT nacional. [en línea]. [Fecha de consulta: 11 de enero de 2020]. disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Caivirtual.policia.gov.co. Amenazas del cibercrimen en Colombia 2016 -2017. 2017. [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.

Ccit.org.co. Tendencia de cibercrimen en Colombia 2019 -2020. 2020. [en línea]. . [Fecha de consulta: 11 de marzo de 2020]. disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf.

Centro criptográfico Nacional. Guía nacional de notificación y gestión de ciberincidentes. 2020. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes.

Centro criptográfico Nacional. Guía de Creación de un CERT/CSIRT. 2011. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf.

Centro Nacional de Respuesta a Incidentes de Seguridad Informática. gub.uy. 2020. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-el-certuy.

Computing. Los 10 ciberataques más grandes de la década. 2020. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-mas-grandes-de-decada.1.html.

Contraloría de Bogotá. Procedimiento gestión de seguridad Informatica. 2018 [en línea]. [Fecha de consulta: 12 de septiembre de 2020].

disponibleen:http://www.contraloriabogota.gov.co/sites/default/files/Contenido/Normatividad/Resoluciones/2018/RR_047_2018%20Adopta%20y%20Actualiza%20Procedimientos%20que%20Conforman%20el%20PGTI%20en%20la%20Contralor%C3%ADa%20de%20Bogot%C3%A1%20D.C/PGTI-06%20Proced%20G.

Cuervo Álvarez, Sara. Implementación ISO 27001. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/10/scuervoTFM0617presentaci%C3%B3n.pdf.

Conpes Lineamientos de política para ciberseguridad y ciberdefensa [en línea]. [consultado el 10 de enero de 2020]. disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

CERTuy: Hacia un CSIRT Nacional [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom013.pdf

Creación de un equipo de respuesta a incidentes de seguridad informática: un proceso para empezarlo [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https: https://csirtpe.files.wordpress.com/2013/06/crearuncsirt-final.pdf

CSIRT, ¿De qué se trata?, modelos posibles, servicios y herramientas [en línea]. [consultado el 11 de enero de 2020]. disponible en: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

Debian, Introducción a AppArmor. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://debian-handbook.info/browse/es-ES/stable/sect.apparmor.html

Definición e Implementación de un Centro de Atención de Incidentes (CERT) para un Ámbito Universitario [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: http://sedici.unlp.edu.ar/handle/10915/21246

Departamento Nacional de Planeación. 2017. [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en:

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf.

DesdeLinux. Graylog, una herramienta para la administración y análisis de registros. [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https://blog.desdelinux.net/graylog-una-herramienta-para-la-administracion-y-analisis-de-registros/.

Digital Guide IONOS. ¿Qué es CentOS? Versiones CentOS y requisitos del sistema. 2020. [en línea]. https://www.ionos.es/digitalguide/servidores/know-how/que-es-centos-versiones-y-requisitos-del-sistema/.

¿Qué es CentOS? Versiones CentOS y requisitos del sistema. [en línea]. [Fecha de consulta: 15 de noviembre de 2020]. disponible en: https://www.ionos.es/digitalguide/servidores/know-how/que-es-centos-versiones-y-requisitos-del-sistema/

EcuRed, DansGuardian. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.ecured.cu/DansGuardian

Esquema Nacional de Seguridad. Guía de seguridad (ccn-stic-810) guía de creación de un cert / csir [en línea]. [Fecha de consulta: 08 de enero de 2020]. disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Guia_Creacion_CERT-CSIRT.pdf

El tiempo.com. Colombia sufrió 42 billones de intentos de ciberataques en 3 meses. 2019. [en línea]. [Fecha de consulta: 08 de enero de 2020]. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666.

Enisa. Cómo crear un CSIRT paso a paso. 2006. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-n9P4muDvAhXwEVkFHfN3A_4QFjAAegQIAxAD&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fcsirt-setting-up-guide-in-spanish%2Fat_download%2FfullReport&usg=AOvVaw2F8Wp_02LEvZ-NMA.

Europa.eu. Agencia de la Unión Europea para la Ciberseguridad (ENISA). 2019. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://europa.eu/european-union/about-eu/agencies/enisa_es.

Estado Libre Asociado de Puerto Rico. Políticas y Procedimientos de Seguridad Informática. 2015. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.de.pr.gov/wp-content/uploads/2014/09/Politicas_y_procedimientos_de_seguridad_PUBLICADO.pdf.

FIRST. FIRST History. 2020. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.first.org/about/history.
FIRST. FIRST Teams. 2020. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.first.org/members/teams/.

Flawfinder, Flawfinder, [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://dwheeler.com/flawfinder/

Fortalecimiento de la gestión TI en el estado [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelode-Seguridad/

Giraldo Gallo, John Fabio. Infraestructuras críticas cibernéticas en Colombia [en línea]. [Fecha de consulta: 08 de enero de 2020]. disponible en: http://www.ccit.org.co/wp-content/uploads/sesion-5-panel-infraestructuras-criticasciber-en-colombia.pdf

Gobierno Digital. Entra en operación el CSIRT de Gobierno. [en línea]. [Fecha de consulta: 11 de enero de 2020]. disponible en: https://estrategia.gobiernoenlinea.gov.co/623/w3-article-77743.html

Gobierno digital. Entra en operación el CSIRT de gobierno. 2018. [en línea]. [Fecha de consulta: 08 de enero de 2020]. disponible en: https://gobiernodigital.mintic.gov.co/portal/Noticias/77743:Entra-en-operacion-el-CSIRT-de-Gobierno.

Guía de seguridad. Guia de creación de un CERT/CSIRT. [en línea]. [Fecha de consulta: 12 de enero de 2020]. disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810Guia_Creacion_CERT-CSIRT.pdf.

Hernandez, Juan Estuardo. Conoce como funciona Zabbix y cómo usarlo. 2013. [en línea]. [Fecha de consulta: 10 de noviembre de 2020]. disponible en: http://911-ubuntu.weebly.com/zabbix_como_funciona/conoce-la-estructura-de-zabbix-y-como-usarlo.

Herrera Monterroso, Harold Eduardo. Gestiopolis. Metodología para evaluación, diagnóstico y diseño de procesos. 2007. [en línea]. [Fecha de consulta: 10 de noviembre de 2020]. disponible en: https://www.gestiopolis.com/metodologia-para-evaluacion-diagnostico-y-diseno-de-procesos/.

Icontec, norma técnica NTC-ISO/IEC colombiana 27001. [en línea]. [Fecha de consulta: 12 de marzo de 2020]. disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Instituto nacional de ciberseguridad de España. Glosario de términos de ciberseguridad. [en línea]. [Fecha de consulta: 12 de enero de 2020]. disponible en: (https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridadguia-aproximacion-el-empresario).

Instituto Nacional de Ciberseguridad. Que es INCIBE. 2019. [en línea]. [Fecha de consulta: 12 de enero de 2020]. disponible en: https://www.incibe.es/que-es-incibe.

ISOTools Excellence. ISO 27001: ¿Qué significa la Seguridad de la Información? [en línea]. [Fecha de consulta: 12 de enero de 2020]. disponible en:(http://www.pmgssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion).

Infocyte. Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks. 2021. [en línea]. [Fecha de consulta: 10 de noviembre de 2020]. disponible en: https://www.infocyte.com/es/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/.

ISO 27002:2013. 14 dominios, 35 objetivos de control y 114 controles. [en línea]. [Fecha de consulta: 10 de noviembre de 2020]. disponible en: https://www.efectus.cl/wp-content/uploads/2018/12/Controles_ISO27002-2013.pdf

IT Masters MAG. Ciberataques que marcaron esta década. 2019. [en línea]. [Fecha de consulta: 10 de noviembre de 2020]. disponible en: https://itmastersmag.com/noticias-analisis/ciberataques-que-marcaron-esta-decada/.

Javier Jerónimo. Graylog – Arquitectura tolerante a fallos y escalable. [en línea]. [Fecha de consulta: 11 de noviembre de 2020]. disponible en: https://javierjeronimo.es/2015/03/23/graylog-arquitectura-tolerante-a-fallos-y-escalable/

Kali. Our Most Advanced Penetration Testing Distribution, Ever. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.kali.org/
Karma. Karma. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://karma-runner.github.io/latest/index.html

La amenaza cibernética contra infraestructuras críticas: Un enfoque práctico para abordar este riesgo desde la perspectiva del Operador Nacional de Energía de Colombia. [en línea]. [Fecha de consulta: 12 de enero de 2020]. disponible en: http://www.cigrecolombia.org/Documents/Memorias/Jornada-riesgos-2018/2Riesgo%20y%20ciberseguridad%20en%20SCADA%20-CIGRE-Col-2018.pdf

La mirada del replicante, Aislando aplicaciones del resto del sistema con Firejail. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://lamiradadelreplicante.com/2017/04/10/aislando-aplicaciones-del-resto-del-sistema-con-firejail/#:~:text=Firejail%20es%20una%20herramienta%20escrita,un%20entorno%20con%20privilegios%20limitados.

Lacnic. Lacnic anuncia la constitución de su CSIRT. 2020. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://www.lacnic.net/4463/1/lacnic/lacnic-anuncia-la-constitucion-de-su-csirt.

Lanfranco, Lic. Einar. CSIRTs, ¿De qué se trata?, modelos posibles, 2016. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf.

LatinPyme. Seguridad informática en Colombia por buen camino. 2020. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://www.latinpymes.com/?p=4507.

Manual de diagnóstico y prevención de vulnerabilidades de datos para pymes [en línea]. [Fecha de consulta: 12 de enero de 2020]. disponible en: https://repository.unad.edu.co/bitstream/handle/10596/15026/80225921.pdf?sequence=1&isAllowed=y

McAfee, RootkitRemover. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.mcafee.com/enterprise/es-es/downloads/free-tools/rootkitremover.html

Microsoft. Windows Sysinternals. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://docs.microsoft.com/en-us/sysinternals/

Ministerio de Telecomunicaciones de Colombia. Controles de Seguridad y privacidad de la información. 2016. [en línea]. [Fecha de consulta: 12 de marzo de 2020]. disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Ministerio de Telecomunicaciones de Colombia. Ley 1273 de 2009. 2009. [en línea]. [Fecha de consulta: 12 de marzo de 2020]. disponible en: https://normograma.mintic.gov.co/mintic/docs/ley_1273_2009.htm.

Ministerio de Telecomunicaciones de Colombia. Seguridad y privacidad de la información. 2016. [en línea]. [Fecha de consulta: 12 de marzo de 2020]. disponible en:https://www.mintic.gov.co/gestionti/615/articles482_G8_Controles_Seguridad.pdf.

Ministerio de defensa. Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. 2017. [en línea]. [Fecha de consulta: 12 de marzo de 2020]. disponible en: file:///C:/Users/Ivan/AppData/Local/Temp/MicrosoftEdgeDownloads/8e193f78-95bf-4dce-8122-c6a23dd82fff/PLAN_PUBLICO.pdf.

Modelo de Coordinación y Atención de Emergencias en el ámbito de la Sociedad de la Información [en línea]. [Fecha de consulta: 13 de enero de 2020]. disponible en: https://www.nacon3seg/publico/seriesCCN-STIC/

Organización y Operación de un CSIRT. [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https://www.sites.oas.org/cyber/Documents/2016%20%20Buenas%20Practicas%20CSIRT.pdf

OEA. Buenas Prácticas para establecer un CSIRT nacional. 2016. [en linea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

Protege.la. UrBackup. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://protege.la/urbackup/#:~:text=UrBackup%20es%20una%20herramienta%20Open,versiones%20(cliente%20y%20servidor).

Ramirez Luna, Heltton Emmanuel. Desarrollo de un marco de trabajo para la protección de un equipo de respuesta ante incidencias de seguridad informática (CSIRT) [en línea]. [Fecha de consulta: 08 de enero de 2020]. disponible en: https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/442/1/ZACTE47.pdf

Secretaria del Senado. Ley 1273 de 2009. 2021. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

Secretaria del Senado. Ley 1928 de 2018. 2018. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html.

Secretaria del Senado. Ley estatutaria 1266 de 2008. 2008. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.

Sentry, Sentry for Open Source. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://sentry.io/for/open-source/
Syslog-NG, The foundation of log management. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.syslog-ng.com/

Superfinanciera. Superfinanciera fortalece la protección de la información. 2018. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00.

syslog. syslog-ng. 2020. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://www.syslog-ng.com/trials/.

Tenable. La familia Nessus. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://es-la.tenable.com/products/nessus

Ubunlog. Firejail, ejecuta de forma segura aplicaciones no confiables en Ubuntu. -. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://ubunlog.com/firejail-ejecuta-aplicaciones-ubuntu/.

Universidad Internacional de Valencia. ¿Qué es la seguridad informática y cómo puede ayudarme? 2020. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme.

Universidad Técnica Particular de Loja. Manual de Políticas Institucionales. 2011. [en línea]. [Fecha de consulta: 20 de noviembre de 2020]. disponible en: https://csirt.utpl.edu.ec/sites/default/files/files/ManualPoliticas.pdf.
Tendencia de cibercrimen en Colombia 2019 -2020. [en línea]. [Fecha de consulta: 12 de septiembre de 2020]. disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Trusting Infrastructure. The Emergence of Computer Security Incident Response, 1989–2005 [en línea]. [Fecha de consulta: 08 de enero de 2020]. disponible en: https://preprint.press.jhu.edu/tec/content/trusting-infrastructure-emergencecomputer-security-incident-response-1989%E2%80%932005

Vanguardia. Los delitos cibernéticos se dispararon en Colombia durante la pandemia. [en línea]. [Fecha de consulta: 26 de noviembre de 2020]. disponible en: https://www.vanguardia.com/area-metropolitana/bucaramanga/los-delitos-ciberneticos-se-dispararon-en-colombia-durante-la-pandemia-KJ2685268

Welivesecurity.com. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? [en línea]. [Fecha de consulta: 10 de enero de 2020]. disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirtrespuesta-incidentes/

Wellenreiter. Welcome to the project page of wellenreiter. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: http://wellenreiter.sourceforge.net/

Wireshark. About Wireshark. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.wireshark.org/

Zabbix, Quasar software. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.quasarbi.com/ZABBIX.html

Zabbix. Network Monitoring. -. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.zabbix.com/network_monitoring.

Zabbix. Zabbix. 2020. [en línea]. [Fecha de consulta: 03 de marzo de 2020]. disponible en: https://www.zabbix.com/.