DISEÑO TÉCNICO DE LA IMPLEMENTACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMATICA CYBER SECURITY DE COLOMBIA LTDA.

JHON ALEXANDER LEAL MENDIVELSO

Proyecto para acceder al título de
Especialista en Seguridad Informática

Director:
Mtr. Ing. EDGAR MAURICIO LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGÍA E INGENIERÍA
BOGOTÁ D.C.
2020

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C, Diciembre de 2020

DEDICATORIA

A mi mamá y a mi hermana, por su entrega desinteresada, dedicación y motivación en el camino para alcanzar mis objetivos académicos.

AGRADECIMIENTOS

Doy gracias a Dios por la vida, por orientarme durante el desarrollo de mi carrera, por el soporte y la fuerza que me levanta cuando me encuentro débil.

Gracias a mi madre y mi hermana por ser las principales promotoras de mis objetivos. A mi hermana por creer en mis sueños; y a mi madre por las lecciones de vida que me ha dado y los principios y valores inculcados desde pequeño.

Agradezco a todos los tutores de la UNAD, con quienes tuve la oportunidad de compartir los entornos de aprendizaje, por haber orientado mi formación, guiada a través de sus conocimientos, durante mi pregrado y especialización. Y de manera muy específica, al Ing. Edgar Mauricio López, director del proyecto de grado, quien, a través de su conocimiento y experiencia, ha orientado de manera adecuada el desarrollo de este proyecto aplicado.

TABLA DE CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

ACL: (Access Control List) Listas de Control de acceso. Especifican que usuarios o procesos del sistema tienen acceso a determinados objetos.

AMENAZA: Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información

ARPANET: The Advanced Research Projects Agency Network. Antecesora de lo que hoy conocemos como internet.

ATAQUE: Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

BACKDOOR: Puerta trasera. Dentro del ámbito de programación, es un término que se utiliza para referenciar código que permite a un usuario externo, acceder al sistema saltándose los controles de seguridad.

CERT: (Computer Emergency Response Team). Equipo de respuesta ante emergencias informáticas.

CRACKER: Un hacker es alguien que descubre las debilidades de un computador o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

CRIPTOGRAFÍA: Se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ilegibles a receptores no autorizados.

CSIRT: (Computer Security Incident Respose Team) Equipo de respuesta a incidentes de seguridad informática.

DEFACEMENT: Consiste en un ataque a un sitio web, con el objetivo de cambiar su apariencia visual, con fines maliciosos.

DES: (Data Encryption Standard). Algoritmo de cifrado simétrico que fue escogido como estándar en 1976. Hoy en día se considera inseguro.

ENDPOINT: Punto final. Hace referencia al último nodo de una red. Para un ciber delincuente, representan puntos donde pueden explotar vulnerabilidades.

EXPLOT: Es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.

GATEWAY: Pasarela o puerta de enlace, es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos de red, sirviendo de enlace aun cuando cuenten con protocolos y arquitecturas diferentes.

GUSANO: Es un malware que tiene la propiedad de duplicarse a sí mismo.

HACKER: Es todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información al alcance de todos constituye un extraordinario bien.

HONEYNET: Son un tipo especial de Honeypot de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes.

HONEYPOT: Es el software o conjunto de computadores cuya intención es atraer a atacantes, simulando ser sistemas vulnerables o débiles a los ataques.

INCIDENTE: Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información

IDS: (Intrusion Detection System) Sistema de Detección de intrusos.

IPS: (Intrusion Prevention System) Sistema de Prevención de Intrusiones.

MALWARE: Código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

PHISHING: Término utilizado para identificar un tipo de ataque utilizado para engañar víctimas, ganándose su confianza y haciéndose pasar por alguien o una empresa reconocida para capturar datos de manera fraudulenta.

RANSOMWARE: En español traduce secuestro de datos. Es un tipo de ataque que consiste en restringir el acceso a determinadas partes o archivos del sistema infectado. Para luego pedir recompensa por la liberación o retiro de esta restricción.

RIESGO: Es la posibilidad latente de que ocurra un evento que afecte de manera negativa la infraestructura o sistema de información de una organización.

RSA: (Rivest, Shamir y Adleman). Sistema criptográfico de clave pública, creado en 1979, su nombre obedece a sus creadores. Utilizado para cifrar documentos y para firmas digitales.

SGSI: Sistema de Gestión de Seguridad Informática.

SHA: (Secure Hash Algorithm, Algoritmo de Hash Seguro). Sistema de funciones hash criptográficas relacionadas de la Agencia Nacional de Seguridad de Estados Unidos.

SNIFFER: Herramienta que se encarga de capturar y analizar paquetes que viajan a través de una red.

SOC: Security Operation Center, Centro de Operaciones de seguridad. Centro de monitoreo que previene y controla la seguridad de las redes de una empresa.

SPEAR PHISHING: Es una estafa de correo electrónico dirigida específicamente a personas u organizaciones, con fines maliciosos.

SSL: (Secure Sockets Layer) Capa de puertos seguros. Protocolo que hace uso de certificados digitales para establecer conexiones seguras entre un cliente y un servidor, cuya comunicación es totalmente cifrada.

TROYANO: Hace referencia a un virus informático muy popular que consiste en engañar a la víctima para tomar el control remoto de la máquina.

TLS: (Transport layer Security) Seguridad de la Capa de transporte. Se trata de una versión mejorada del protocolo SSL, que también cifra la conexión entre dos puntos, que puede ser cliente y servidor, entre dos servidores o entre dos clientes.

UPS: Sistema de alimentación de energía ininterrumpido. Suministra energía eléctrica durante un tiempo para poder apagar servidores y sus respectivos servicios de manera correcta en caso de una falla en el suministro de energía.

VIRTUALIZACIÓN: Creación en versión virtual de recursos tecnológicos, a través de herramientas de software. Instalación de un sistema operativo dentro de otro, al que se le conoce como anfitrión, donde se asigna hardware y recursos físicos, a las máquinas virtuales instaladas.

VIRUS: Es un software malicioso cuyo objetivo es alterar el normal funcionamiento de un sistema informático, sin autorización ni conocimiento del usuario.

VLAN: Virtual LAN (Local Area Network), Concepto que se emplea en informática para crear redes lógicas independientes dentro de una misma red física.

VPN: (Virtual Private Network) Red Privada Virtual. Es una herramienta de red que permite extender de manera segura, la red LAN, sobre una red pública, otra red privada o una no controlada como internet.

VULNERABILIDAD: Debilidad o falla en el sistema, que pone en riesgo la seguridad de la información que puede permitir a un atacante, comprometer la integridad, confidencialidad y disponibilidad de la misma.

INTRODUCCIÓN

El continuo aumento de usuarios de Internet, que a finales del año 2019, llegó al 53.6% de la población mundial, un poco más de 4.100 millones de personas, según informe publicado por la unión Internacional de Telecomunicaciones (ITU)[1], de las Naciones Unidas. Sumado al incremento de redes interconectadas alrededor del mundo, la aparición de nuevas plataformas de tecnología y la utilización de distintas interfaces, han generado un inmenso ecosistema digital, que busca catapultar el progreso comercial, mejorando y sintetizando los procesos de producción de las organizaciones y dejando un saldo económico a favor. Pero también, han favorecido la aparición de amenazas, con técnicas cada vez más modernas y peligrosas.

La importancia de la implementación de un CSIRT se fundamenta en proporcionar servicios de atención inmediata ante incidentes de seguridad informática que se presenten, dotando de modernas herramientas tecnológicas a los miembros del CSIRT, para lograr resultados óptimos en la intervención de los mencionados incidentes y reduciendo de manera considerable el impacto sobre los activos de información.

Un CSIRT, aparte de dar solución oportuna a los incidentes y tomar acciones para reducir la cantidad de los mismos. También proporciona herramientas de gestión de calidad en cuanto a seguridad de la información, y adaptación a la normativa vigente, orientada a la protección de la información.

Este proyecto está enfocado principalmente en el Diseño técnico de la implementación de un Centro de Respuesta a Incidentes de Seguridad Informática, en la empresa, Cyber Security de Colombia Ltda. Listando los servicios que puede ofrecer un CSIRT.

[1] INTERNATIONAL TELECOMUNICATION UNION. [Sitio web]. Individuals using the internet, 2005 – 2019. Naciones Unidas. [Consulta: 24 de Octubre 2020]. Disponible en: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

1. PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES

La historia de los equipos de respuesta a incidentes de seguridad, nació hace 30 años aproximadamente, cuando la cantidad de dispositivos conectados a internet era muy reducida. De acuerdo a reseña histórica de Ecured[2], en el año 1988, aparece el primer gusano de internet, más conocido como gusano Morris, llamado así, gracias a su creador Robert Tappan Morris. El cual logró colapsar al menos al 10% de las máquinas conectadas a internet de la época.

Luego de este antecedente, y con los continuos incidentes de seguridad que se han presentado a través de la historia, la DARPA[3] (Defense Advanced Research Projects Agency), empezó a pensar en un equipo que se encargara de gestionar dichos incidentes, de modo más organizado y estructurado, conformando un esquema de seguridad de las organizaciones, que en principio se llamó CERT, Computer Emergency Response Team.

Dichos equipos fueron evolucionando con el pasar de los años, y mucho más con el aumento acelerado de interconexiones entre dispositivos a nivel mundial, lo cual trajo consigo, un incremento en los riesgos, ataques y vulnerabilidades de las redes de datos, desbordando de manera considerable, la cantidad de incidentes de seguridad que se presentaban a diario. Por tal razón, crece la importancia de dichos equipos de respuesta a incidentes, que hoy día se les conoce como CSIRT, tanto en organizaciones privadas como públicas.

1.2 DEFINICIÓN DEL PROBLEMA

A diario, organizaciones a nivel mundial, son víctimas de ataques a sus sistemas de información, aprovechando vulnerabilidades de su infraestructura tecnológica, utilizando técnicas como: Phishing, ransomware, entre otros. A finales de 2019, la compañía británica Comparitech, at través del investigador Paul Bischoff[4], realizó un análisis de dispositivos infectados, ataques a sistemas financieros y legislación en cuanto delitos cibernéticos, en 60 países, para evidenciar el nivel de seguridad

[2] ECURED. Gusanos Informáticos. [Consulta: 24 de Octubre 2020]. Disponible en: https://www.ecured.cu/Gusano_(inform%C3%A1tica)

[3] DARPA. Defense Advanced Research Proyects Agency. Disponible en: https://www.darpa.mil/our-research

[4] BISCHOFF, Paul. (2020). ¿Qué países tienen la peor (y mejor) ciberseguridad? Comparitech. Disponible en: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

frente al cibercrimen. Donde se estableció que Colombia cuenta con problemas significativos en cuanto a ciberseguridad. Si bien no se encuentra entre los países con peor índice de seguridad digital, si presenta falencias en su legislación informática y protección contra ataques cibernéticos.

El análisis tomó en cuenta siete criterios, donde se evidencia que en Colombia el 12,52% de los dispositivos móviles están infectados con algún tipo de malware diseñado para entrar o destruir el sistema sin autorización del usuario. Es un porcentaje medio, si se tiene en cuenta que el más bajo se encuentra en Japón con apenas el 1,34%, y el más alto se presenta en Nigeria con el 28%. En ordenadores, las infecciones son mayores y, en Colombia, afectan al 16,4% de los sistemas. Al país no le fue muy bien en la calificación de su legislación, que mide qué tan actualizada está para brindar garantías de ciberseguridad. El puntaje fue de 4 sobre 10, aunque ningún país pasó de 7, ni China ni Francia, los mejor posicionados en ese ítem.

Por otro lado, en publicación de Global Security Index de ITU[5], se determinó que el país se encuentra en un rango medio de seguridad, de acuerdo a su nivel de compromiso y participación en programas e iniciativas de seguridad cibernética. Además, se Ubica a Colombia en el puesto 7 del ranking a nivel del continente americano, y en el puesto 73 a nivel mundial.

La principal preocupación, se enmarca en lo difícil que es incorporar personal con habilidades en ciberseguridad que se necesitan para contrarrestar los posibles riesgos, y el presupuesto asignado para implementar una solución integral que pueda hacer frente a los incidentes que se presentan a diario.

Esto sumado a que cada día aparecen nuevas formas y modos de ataque, con diversas técnicas que hacen mucho más difícil la protección de los sistemas de información. Muchas veces los administradores TI, ni siquiera pueden establecer la forma como se vulneraron los controles de seguridad de su red. Lo cual nos lleva a concluir que ninguna solución de seguridad es completamente eficaz.

¿Cómo puede la implementación de un CSIRT privado en Cyber Security de Colombia Ltda., reducir el riesgo y contrarrestar los ataques cibernéticos?

[5] INTERNATIONAL TELECOMUNICATION UNION. (2019). The Global Cybersecurity Index. Geneva, Swtzerland. Disponible en:
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

2. JUSTIFICACIÓN

La continua evolución de la tecnología en nuestros tiempos, forja grandes desafíos respecto de seguridad de la información a las diferentes organizaciones a nivel mundial, donde la protección de datos y de equipos, está en manos de la mencionada seguridad de la información. De igual manera, el crecimiento de las redes, la aparición de múltiples plataformas tecnológicas, y la necesidad de comunicación entre los diferentes dispositivos de red, ha traído consigo nuevas amenazas y técnicas de ciberataques.

Con el fin de proteger los activos de información, hace varios años, aparecen los llamados CSIRT, los cuales tienen como objetivo fundamental, atender de manera inmediata los incidentes de que se puedan presentar, con el fin de reducir el daño o afectación en los diferentes procesos.

Para dar solución a la situación, se presentan varias opciones que no logran satisfacer las necesidades de la organización y que van desde el apoyo de los CSIRT gubernamentales, que fueron creados para asuntos de seguridad nacional específicamente, pasando por adquisición de soluciones de seguridad perimetral, antivirus, entre otras. O contratando un servicio de CSIRT comercial a un proveedor reconocido. Por último, se encuentra la opción que puede cumplir con los requisitos de seguridad que necesita la organización. Se trata de la implementación de un CSIRT privado que se encargue específicamente de atender y dar respuesta a incidentes de seguridad que se puedan presentar dentro de su sistema. Para lo cual debe incorporar personal capacitado, con expertos en seguridad de la información, quienes deben conocer la estructura tecnológica y funcionamiento de toda la red, bases de datos, aplicativos y demás servicios de la empresa. Lo cual, acarrea un alto costo, en cuanto a infraestructura, equipos y personal capacitado.

Como lo menciona Eduardo Carozo[6], en revista de la UNAM, Dicho equipo de profesionales se debe encargar de generar alertas y advertencias, enviando comunicados a los responsables del equipo o servicio afectado, realizar el adecuado tratamiento de incidentes, estudio y análisis de los mismos para determinar las causas o la vulnerabilidad que permitió que se materializara; realizar auditorías de seguridad de manera periódica para medir el nivel de vulnerabilidad y amenazas que presenta el sistema, y realizar análisis forense cuando ocurra algún caso de delito informático, con el fin de establecer responsabilidades.

[6] CAROZO B., Eduardo. Centro de respuesta a incidentes informáticos... ¿Para qué? En Revista Seguridad cultura de prevención para TI. Vol 16. (Ago 2018). Disponible en: https://revista.seguridad.unam.mx/numero-16/centro-de-respuesta-incidentes-informáticos-para-qué

3. OBJETIVOS

3.1 Objetivo General

Elaborar la documentación técnica de un Centro de Respuesta a Incidentes de Seguridad Informática, caso de estudio Cyber Security de Colombia Ltda.

3.2 Objetivos específicos:

- Recopilar información relacionada con herramientas de hardware y software que permitan desarrollar las actividades del CSIRT, teniendo presente que sus servicios son reactivos y proactivos.
- Elaborar la estructura organizacional del CSIRT, determinando detalladamente los roles y responsabilidades de cada actor.
- Diseñar el mapa de la estructura tecnológica del CSIRT teniendo presente que las dependencias mínimas con las que debe contar son: Centro de Datos, I+D+i, Centro de Operaciones, Soporte TI, Coordinaciones, Área Logística, Salón de Formación, Salón de crisis.
- Listar y definir los servicios que puede prestar el CSIRT a la empresa Ciber Security de Colombia Ltda.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Existen diferentes equipos de respuesta a incidentes de seguridad, distribuidos de la siguiente forma:

4.1.1 A nivel Mundial.

4.1.1.1 FIRST. Foro Global de Respuesta a Incidentes y Equipos de Seguridad. Es una organización líder a nivel mundial, creada en el año 1990, que congrega una gran cantidad de CSIRT, de diferentes organizaciones gubernamentales, comerciales, militares y educativas. Su principal función es promover la cooperación y trabajo conjunto con el fin de prevenir incidentes, fomentar una rápida reacción ante incidentes e impulsar el intercambio de información entre los más de 500 miembros distribuidos en los 5 continentes. Dentro del marco de las siguientes actividades:

- Fomentar y promover el desarrollo de productos, políticas y servicios de seguridad de calidad.
- Desarrollar y promulgar las mejores prácticas de seguridad informática.
- Promover la creación y expansión de equipos de respuesta a incidentes y miembros de organizaciones de todo el mundo.
- Los miembros de FIRST desarrollan y comparten información técnica, herramientas, metodologías, procesos y mejores prácticas.
- Los miembros de FIRST utilizan sus conocimientos, habilidades y experiencia combinados para promover un entorno electrónico global más seguro y seguro.

FIRST[7], está vinculado activamente con organizaciones del orden mundial como Géant, Lacnic, Unión Internacional de Comunicaciones UIC, Foro Mundial de Conocimientos Cibernéticos GFCE, Organización del CERT de Cooperación Islámica OIC-CERT, Centro de Información de la Red Asia Pacifico APNIC, La Organización de los Estados Americanos OEA, Organización para el avance de los Estándares de Información Estructurada OASIS y Mitre Engenuidad, que contribuyen a mejorar la respuesta de los equipos miembros, ante incidentes

[7] FIRST IMPROVE SECURITY TOGETHER. [sitio web]. Foro Global de Respuesta a Incidentes y Equipos de Seguridad. [Consulta 27 de mayo 2020]. Disponible en: https://www.first.org/

4.1.2 A nivel Continental.

4.1.2.1 ENISA. Agencia Europea de Seguridad de las redes y de la información[8]. Creada en 2004 por la unión europea, lleva más de 10 años apoyando a los estados de la UE, y a las comunidades CSIRT. Dentro de sus funciones, cuenta con información de configuración ejecución y desarrollo de capacidades de los equipos de respuesta a incidentes de seguridad Informática

Cuenta con un documento tipo directiva, donde relaciona todas las disposiciones que deben adoptar los países miembros en cuanto a la importancia de los que se le asigna a los sistemas de información, cuya confidencialidad y seguridad son esenciales para el desarrollo de las actividades económicas y en general el continuo trasegar del mercado.

En el artículo 12 de la mencionada directiva, se establece la red de CSIRT nacionales, para fomentar la confianza de los países miembros, e iniciar un trabajo conjunto entre ellos, donde se incluye la participación del CERT-UE, y de ENISA con la secretaria general. Se establece también las funciones que tendrá la red de CSIRT, dentro de las cuales, se relacionan:

- Intercambio de información acerca de servicios y operaciones y capacidades de cooperación de cada CSIRT.
- intercambio de información no confidencial sobre incidentes individuales.
- Debatir e identificar una respuesta coordinada a un incidente identificado en alguno de los estados miembros.
- Prestar apoyo a los estados miembros para afrontar incidentes transfronterizos.
- Discutir e identificar diferentes formas de cooperación en relación a: categorías de riesgos e incidentes, alertas tempranas, ayuda mutua, etc.
- Debatir lecciones aprendidas de casos abordados con relación a eventos de seguridad de la red CSIRT.
- Emitir directrices orientadas a mejorar el trabajo conjunto de la red CSIRT.

Según el parlamento europeo[9], Cada año y medio la red CSIRT elabora un documento que evalúa la experiencia adquirida, y la cooperación operativa entre los países miembros. Es importante mencionar que la red CSIRT, establece sus propias normas y procedimientos

[8] ENISA. Agencia de la Unión Europea para la seguridad Cibernética. (2019). CSIRT en Europa. Disponible en: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

[9] DIRECTIVA (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, sobre medidas para un alto nivel común de seguridad de redes y sistemas de información en toda la Unión. Disponible en: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

4.1.2.2 APCERT. Asia Pacific Computer Emergency Response Team[10]. Encargado de mantener una red confiable de expertos en seguridad informática en la región de Asia Pacifico, con el fin de mejorar la competencia de la región en lo que respecta a incidentes de seguridad informática, mediante la aplicación de las siguientes tareas:

- Mejorar la cooperación regional e internacional de Asia y el Pacífico en materia de seguridad de la información.
- Desarrollar conjuntamente medidas para hacer frente a incidentes de seguridad de redes a gran escala o regionales.
- Facilitar el intercambio de información y el intercambio de tecnología, incluida la seguridad de la información, virus informáticos y código malicioso entre sus miembros.
- Promover la investigación y el desarrollo en colaboración sobre temas de interés para sus miembros.
- Ayudar a otros CERT y CSIRTS en la región a realizar una respuesta de emergencia informática eficiente y efectiva.
- Proporcionar aportes y/o recomendaciones para ayudar a abordar los problemas legales relacionados con la seguridad de la información y la respuesta a emergencias a través de las fronteras regionales

4.1.3 A nivel Colombia

4.1.3.1 CSIRT Ponal Colombia. Equipo de respuesta a incidentes de seguridad informática, de la Policía Nacional de Colombia.

> Grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones. Sus objetivos específicos son:
>
> Proveer asistencia técnica, asesoría y apoyo a la comunidad y a las organizaciones en general, en la protección de amenazas y/o incidentes informáticos. Consolidar los procesos y procedimientos de atención de incidentes de seguridad de la información mediante el uso de estándares y buenas prácticas. Activar los mecanismos de colaboración para la coordinación y gestión de incidentes entre entidades.
>
> Establecer alianzas estratégicas con organismos nacionales e internacionales, entidades públicas y privadas, para afianzar los mecanismos de ayuda mutua en materia de seguridad

[10] APCERT. Asia Pacific Computer Emergency Response Team. [sitio web]. Supporting the Internet Security in Asia Pacific. [consulta 27 de mayo de 2020]. Disponible en: https://www.apcert.org/about/mission/index.html

de la información. Fomentar la concienciación en el manejo de la información y la implementación de las políticas de seguridad de la información.

Generar estrategias de divulgación para suministrar un sistema de alertas tempranas, anuncios y comunicados que permitan prevenir los riesgos asociados a la seguridad de la información. Promover en las organizaciones públicas y privadas la creación e integración de esquemas de atención de incidentes de seguridad CSIRT[11].

4.1.3.2 CSIRT Financiero Asobancaria. Este CSIRT nace gracias a la asociación Bancaria y de Entidades financieras de Colombia, Asobancaria, en consecuencia, con lo dispuesto por el gobierno nacional en el CONPES 3854 de 2016, donde se insta a crear colaboración entre el sector privado y el sector público para combatir las amenazas que presenta el sector financiero de una manera integral.

Se encarga de dar apoyo a las entidades financieras en el mejoramiento de sus capacidades de prevención de incidentes de seguridad, toma la vocería ante las autoridades nacionales en materia de ciberseguridad, fomentan el intercambio de información de seguridad informática entre entidades del sector financiero.

Dentro de su plataforma, cuentan con anuncios de seguridad que permiten informarse sobre nuevas alertas que se presentan a diario, como análisis de malware, indicadores de compromiso, variantes de malware, detección phishing, entre otros, que le permiten a las entidades financieras estar al tanto de las novedades y nuevos riesgos en materia de ciberseguridad, para implementar técnicas o procedimientos con el fin de prevenir o contrarrestar la materialización de dichos riesgos[12].

4.2 MARCO CONCEPTUAL

4.2.1 Definición: CSIRT: Equipo de Respuesta a Incidentes de seguridad Informática. Entidad o grupo dentro de una organización, que tiene la responsabilidad de coordinar y apoyar la respuesta a un evento o incidente de seguridad Informática. Los cuales pueden ser implementados por naciones, organizaciones gubernamentales, industria comercial o instituciones educativas, con el fin de controlar el daño causado por los incidentes, suministrar una guía para las actividades de respuesta y recuperación, y prevenir que ocurran incidentes futuros.

[11] CSIRT PONAL. Policía Nacional. Oficina de Telemática. Disponible en: https://cc-csirt.policia.gov.co/quienes-somos

[12] CSIRT Asobancaria. Un enfoque colaborativo y proactivo en la gestión de ciberseguridad del sector financiero colombiano. Disponible en: https://csirtasobancaria.com/

Los objetivos del CSIRT se enmarcan en reducir la afectación o impacto en los sistemas de información de una empresa, de la mano con el resguardo de los eventos registrados en los hechos y su respectiva documentación. De esta manera, se puede conocer todos los aspectos del incidente, lo cual ayudará a encontrar las causas y establecer posibles responsabilidades.

Una vez identificado el contexto, se debe coordinar con los administradores de TI, para realizar tareas de recuperación inmediata, de tal manera que la empresa siga desarrollando sus procesos de manera oportuna y lo más pronto en la medida de las posibilidades, para reducir el impacto a niveles que pueda soportar la empresa.

En la figura 1, se puede observar la clasificación de los CSIRT, según los modelos organizacionales, la cual, ayuda a la comunicación entre ellos, para poder responder a los incidentes de seguridad informática, Cada uno de los modelos brinda diferentes servicios, en diferente calidad y a diferente nivel, teniendo en cuenta la experiencia y madurez del equipo, dependiendo de los objetivos de la organización

Figura 1. Clasificación de los CSIRT en base a los modelos organizacionales

Fuente: RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação. [En línea]. Porto: Estado actual de equipos de respuesta a incidentes de seguridad informática. [Fecha de consulta 18 de noviembre de 2019]. Disponible en: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952015000100002

Por otro lado, Miguel Ángel Mendoza[13], menciona que es necesario evitar que dichos eventos u otros de iguales características, se presenten de nuevo, atacando directamente la causa u origen del incidente. Con la documentación de toda esta información, se alimenta una plataforma de conocimiento, como casos tácticos de dichos eventos, buscando eliminar la posibilidad de que vuelvan a ocurrir, y en caso de que ocurra, ya se tiene un registro histórico, donde se puede consultar las soluciones dadas en su momento.

También contiene tareas y procedimientos para compartir dichos casos de incidentes, con otros CSIRT, creando un equipo que trabaja de manera conjunta compartiendo conocimiento, experiencias y soluciones

4.2.2 Tipos de CSIRT. Actualmente existen diferentes tipos de CSIRT de acuerdo a sus clientes y sus objetivos según su ubicación en diferentes ámbitos y sectores de la sociedad a nivel mundial.

4.2.2.1 CSIRT para PYMES. Debido a su tamaño no se justifica que se dedique un CSIRT para una pequeña empresa, por lo que este tipo de CSIRT atiende grupos de pequeñas empresas con características muy similares en cuanto a su área de producción o enfoque comercial.

4.2.2.2 CSIRT Académico. Este tipo de CSIRT presta sus servicios a instituciones académicas como universidades o centros de investigación, y sus campus virtuales.

4.2.2.3 CSIRT Militar. Su función se desarrolla en instituciones de carácter militar que tienen infraestructuras tecnológicas con fines de defensa.

4.2.2.4 CSIRT Comercial. Funciona como proveedor de servicio de CSIRT, sus clientes son entidades comerciales y en general de carácter privado.

4.2.2.5 CSIRT Interno. Este CSIRT es de carácter privado y únicamente presta sus servicios a la organización a la que pertenece. No cuentan con sitios web públicos.

[13] MENDOZA, Miguel Angel. (2015). Welivesecurity by ESET. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

4.2.2.6 CSIRT Gubernamental. Este tipo de CSIRT tiene por objeto proteger la infraestructura TI, de un estado nación y proporciona sus servicios a toda la población. Generalmente se enfocan en las instituciones públicas y entidades del estado. Se adaptan a cada gobierno para satisfacer las necesidades de comunidades específicas de la región.

Tabla 1. CSIRTs Nacionales en Latinoamérica

País miembro de la OEA con CSIRT Nacional	Nombre del CSIRT por país
México	CERT-MX
Guatemala	CSIRT-GT
El salvador	SalCERT
Trinidad y Tobago	TT-CSIRT
Costa Rica	CSIRT-CR
Panamá	CSIRT-Panamá
Venezuela	VenCERT
Guyana	CSIRT.GY
Colombia	ColCERT
Ecuador	Ecucert
Perú	PeCERT
Brasil	CERT.Br
Bolivia	CSIRT-BO
Paraguay	CERT-PY
Uruguay	CERTuy
Argentina	ICIC-CERT
Chile	CSIRT-CL

Fuente: MURQUINCHO PUMA, Diego Eduardo. Área de la energía las industrias y los recursos no renovables. Seguridad Informática, Universidad de Loja Ecuador. [Consultado 29 de mayo 2020]. Disponible en: https://www.studocu.com/ec/document/universidad-nacional-de-loja/seguridad-de-la-informacion/resumenes/csirts-latinoamerica/3781244/view

4.2.3 Seguridad Informática. Es el área de la tecnología que se encarga de prevenir y detectar el uso inadecuado o no autorizado de un sistema informático, y datos en general. Su objetivo se enfoca en la protección de los activos de información y recursos informáticos, de los constantes ataques y riesgos que se pueden presentar, ya sea con intenciones maliciosas, con intenciones de conseguir dinero, o simplemente por errores humanos no intencionales.

Podemos decir que a seguridad informática es una rama de la seguridad de la información, puesto que esta última abarca un sinnúmero de controles de seguridad que tienen que ver también con documentos, evidencias, procesos y procedimientos físicos que involucren información o datos, y también la digitalización de dichos procesos y datos, que corresponde a la seguridad informática. La cual además de la digitalización de la información, también administra herramientas de seguridad de hardware y software, para satisfacer las necesidades de los usuarios ante los riesgos que se presentan a diario.

La seguridad informática se basa en la protección de las propiedades de la información que se describen a continuación:

4.2.3.1 Confidencialidad. La información solo puede estar disponible o ser mostrada para personas o procesos autorizados.

4.2.3.2 Integridad. Es la propiedad que tiene como objeto mantener la información libre de modificaciones no autorizadas.

4.2.3.3 Disponibilidad. La información debe estar disponible cuando sea requerida por usuarios o procesos.

4.2.4 Incidente de Seguridad Informática. Corresponde a cualquier evento que se registre de acceso o intento de acceso de manera ilegal a información privada de una organización con fines delictivos que buscan afectar el normal funcionamiento de los sistemas de información. Estos eventos deben quedar debidamente documentados y registrado en el Sistema de Gestión de seguridad de la Información de la empresa, con el fin de tomar acciones para evitar que se vuelva a presentar o para saber cómo contrarrestar el riesgo que generan dichos incidentes.

Existen tres tipos de incidentes según su origen:

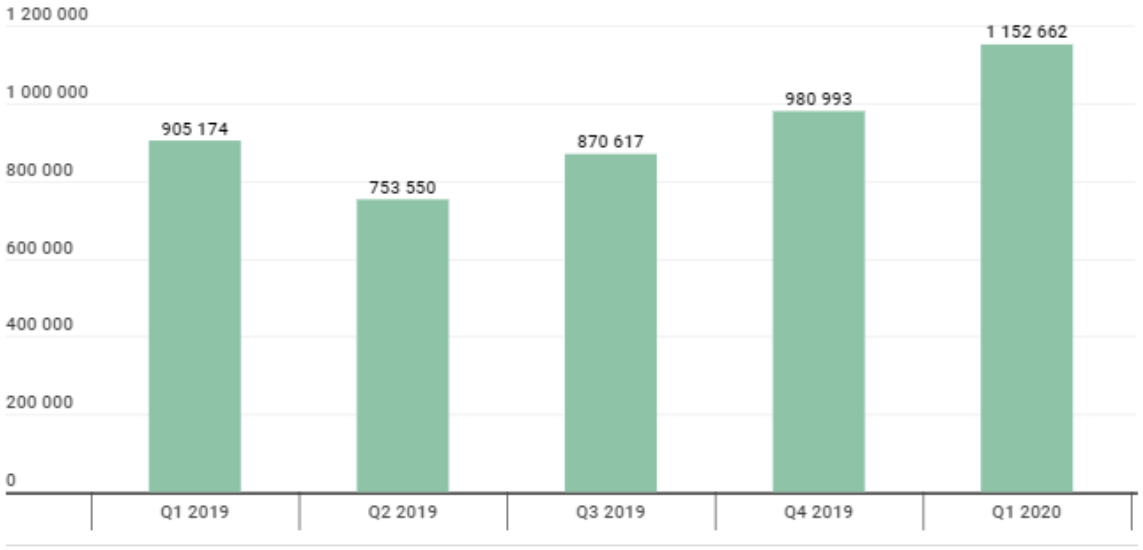
4.2.4.1 Ataques externos. Se trata de hackeos, sabotajes realizados desde fuera de la red de la empresa, con técnicas como Phishing o ransomware. Donde los delincuentes aprovechan las vulnerabilidades de seguridad para lanzar sus ataques.

4.2.4.2 Ataques Internos. Estos eventos se pueden presentar con empleados de la misma organización como directivos, proveedores, prestadores de servicios, contratistas y otros. Que ya sea por desconocimiento o indisciplina no se ajustan a los protocolos y políticas de seguridad de la información de la empresa, o en el caso más grave cuando se presenta el conocido ataque de hombre en medio.

4.2.4.3 Desastres Naturales. Cualquier organización se encuentra expuesta a riesgo de ser afectada por la ocurrencia de fenómenos naturales que se pueden presentar de manera impredecible como: incendios, terremotos, inundaciones, entre otros, que pueden afectar la continuidad del negocio de diferentes maneras directas e indirectas, para lo cual se debe contemplar planes de contingencia y recuperación ante este tipo de incidentes.

4.2.5 Amenaza. Se define como amenaza a toda acción, evento o situación que pueda poner en riesgo la seguridad de la información.

Figura 2. Estadísticas de las amenazas móviles



Fuente: KASPERSKY. (2020). Secure List. Desarrollo de las amenazas informáticas en el primer trimestre de 2020 Estadísticas. [Consulta 29 de mayo de 2020] Disponible en: https://securelist.lat/it-threat-evolution-q1-2020-statistics/90344/

Las amenazas nacen de la presencia de vulnerabilidades. Es decir, solamente pueden existir amenazas si existe al menos una vulnerabilidad que pueda ser aprovechada o explotada. Un sinnúmero de situaciones ha generado el crecimiento de amenazas intencionales como nuevas técnicas de ingeniería social, y ausencia de planes de concientización y formación a los usuarios respecto a seguridad informática. Las amenazas pueden clasificarse en dos tipos:

4.2.5.1 Intencionales. Son los eventos que pueden ocurrir como consecuencia de un intento deliberado de producir un daño. Que se puede dar, explotando las vulnerabilidades que presenta el sistema para realizar inyección de código malicioso, o realizar ataques de denegación de servicio.

También se presenta mediante la técnica de ingeniería social, engañando a cualquier usuario del sistema convenciéndolo de entregar datos confidenciales, haciéndole creer que se está comunicando con alguna entidad bancaria o del gobierno, etc. (Más conocida como técnica de Phishing)

4.2.5.2 No intencionales. Según LACNIC[14], Se producen tras la ocurrencia de eventos no planeados ni esperados, o por la omisión involuntaria de una acción, que, aunque no buscan explotar alguna vulnerabilidad, si representan un riesgo que puede causar daños a los activos de información. Estos eventos no intencionales se clasifican de la siguiente manera:

- Desastres Naturales: Terremotos, tornados, inundaciones, erupciones volcánicas, etc.
- Eventos terroristas o actos de guerra: Bombas, secuestros, ataques químicos, etc.
- Accidentes: Explosiones, incendios, averías en tubería, choques vehiculares, etc.
- Emergencias sanitarias: Pandemia, peste, plaga.
- Otros eventos: Errores en dispositivos, errores humanos, vandalismo, pérdida de comunicación

4.2.6 Vulnerabilidad. Corresponde a la falta de controles administrativos, técnicos o físicos, o debilidad en los mismos, que puede permitir la materialización de amenazas de manera más fácil y con mayor afectación al sistema.

Las vulnerabilidades se pueden agrupar de acuerdo a su función de la siguiente manera:

- Diseño: Debilidades en el diseño de protocolos utilizados y políticas de seguridad deficientes y obsoletas.

[14] LACNIC. (2012). Gestión de Incidentes de Seguridad Informática. Registro de Direcciones de Internet para América Latina y el Caribe. Proyecto AMPARO. [Consulta 29 de mayo 2020]. Disponible en: https://warp.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

- Implementación: Fallas por errores de programación, existencia de puertas traseras, fallas de los fabricantes.
- Uso: Configuración inadecuada, ausencia de capacitación y concientización a los usuarios del sistema, utilización de herramientas que facilitan los ataques.
- Vulnerabilidad de día cero: Se presenta cuando no existe una solución conocida para remediar una vulnerabilidad, pero hay conocimiento de cómo explotarla.

4.2.7 Criptografía. Es una técnica antigua, que se usa desde sus inicios para proteger información privada, y prevenir que personas no autorizadas accedan a ella. De acuerdo con José Pastor Franco[15] y sus colaboradores en su libro, Criptografía Digital: Fundamentos y aplicaciones, su aparición data de los inicios de la escritura, donde el hombre empezó a utilizar diferentes técnicas para ocultar el verdadero significado de los mensajes, y que solo pudiera ser descifrado por el receptor del mismo. En tal sentido, solo quienes conocían el método de cifrado, podían leer claramente el contenido del mensaje oculto.

Con el paso del tiempo y el avance en la tecnología, la criptografía fue evolucionando, y mejorando las técnicas para codificar la información y así adaptarse a un mundo interconectado, que demanda seguridad en sus comunicaciones. Tal como lo relata Roberto García[16], en su libro, Criptografía clásica y moderna, que cuenta con un recorrido por la historia, donde relaciona los aportes de los más destacados contribuyentes de esta técnica. Desde la civilización egipcia, los espartanos, pasando por Julio Cesar y Cesar Augusto, entre otros, como Claude Elwood Shannon, a quien, gracias a su publicación, Teoría de las comunicaciones Secretas, la criptografía deja ser considerada un arte y pasa a considerarse como una ciencia.

Roberto García[17], también destaca, como a lo largo de la historia, la criptografía ha jugado un papel muy importante en los acontecimientos más relevantes e importantes de la humanidad, donde se ha utilizado para salvaguardar información

[15] FRANCO, José Pastor; SARASA LÓPEZ, Miguel Ángel y SALAZAR RIAÑO, José Luis. Criptografía Digital: Fundamentos y aplicaciones. Editorial Zaragoza. (2001). Disponible en: https://www.casadellibro.com/libro-criptografia-digital-fundamentos-y-aplicaciones-2-ed/9788477335580/798279

[16] GARCÍA, R. D. M. (2009). Criptografía clásica y moderna. España: Septem Ediciones. P. 14 Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/102985

[17] Ibid., p. 40

confidencial, o bien sea para descifrar datos encriptados, como es el caso de la famosa máquina enigma, utilizada en la segunda guerra mundial.

4.3 MARCO LEGAL

4.3.1 CONPES 3854 de 2016. "Política Nacional de Seguridad Digital Documento de la Presidencia de la república, da una nueva perspectiva a la seguridad de la información al incorporar la gestión del riesgo como uno de los pilares fundamentales. Este Conpes está orientado a gestionar el aumento del riesgo que puede amenazar la seguridad de la Nación, y establecer normas y leyes que hagan frente a los desafíos en cuanto a seguridad de la información en el país"[18].

4.3.2 Ley 1273 del 05 de enero de 2009. "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[19].

A través de esta ley, el gobierno de Colombia, modifica el código penal en el artículo 53, quedando como agravante el uso de medios informáticos para la comisión de delitos, y adiciona un título llamado, de la protección de la información y de los datos, derogando todas las disposiciones que le sean contrarias, en especial el art 195 del mismo código penal

4.3.3 Ley 1928 del 24 de julio de 2018. "Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest"[20].

Con esta ley, el estado colombiano aprueba y aplica el convenio de Budapest, firmado por los estados miembros del concejo de Europa, que fija una política penal, orientada a proteger a la sociedad de la ciberdelincuencia, a través de la

[18] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). Conpes 3854. Política Nacional de Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

[19] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (2009). Ley 1273 de 2009. Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos". Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

[20] PRESIDENCIA DE LA REPUBLICA DE COLOMBIA. (2018). Ley 1928 del 24 de julio de 2018. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

implementación de una legislación adecuada, que brinda los poderes legales suficientes para luchar contra los delitos cibernéticos, promoviendo la cooperación internacional, con participación de los estados miembros y del sector privado.

4.3.4 CONPES 3701 del 14 de julio de 2011. "Lineamientos de política para ciberseguridad y ciberdefensa. Con este documento el gobierno de Colombia, asigna presupuesto al ministerio de defensa nacional, para crear una estrategia que define los lineamientos orientados a contrarrestar el aumento de amenazas informáticas que afectan al país"[21].

Este documento surge de la problemática que presentaba el estado en el año 2010, donde su capacidad para afrontar las amenazas cibernéticas, tenía muchas debilidades, y no existía una estrategia nacional al respecto. Para su aplicación, se definen lineamientos que incluyen recomendaciones que deben aplicar las entidades involucradas directa o indirectamente.

4.3.5 Resolución 093 del 11 de febrero de 2019. "Por la cual se delegan unas funciones, se conforman unos comités y se dictan otras disposiciones" [22].

Capítulo Segundo: Comité de seguridad de la información. Art. 72. Se crea el comité de seguridad de la Información del departamento Administrativo de la Republica de Colombia. Art. 73. Se determina el objeto del Comité. Art. 74. conformación del Comité de seguridad de la información. Art. 75. Relaciona las funciones del comité de seguridad de la información.

Capítulo Tercero: Equipo de respuesta a incidentes de seguridad de la Información. Art. 77. Se establece como órgano consultivo del Comité de Seguridad de la información, el CSIRT, sus miembros son: la jefatura para la protección presidencial del Departamento Administrativo de la Presidencia de la Republica

[21] COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (2011). CONPES 3701 de 2011. Lineamientos de política para la Ciberseguridad y Ciberdefensa. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[22] COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. (2019). Resolución 93 de 2019. "Por la cual se delegan unas funciones, se conforman unos comités y se dictan otras disposiciones" Disponible en: http://legal.legis.com.co/document/Index?obra=legcol&document=legcol_6069d1a9118047e6a0c0e0050ac80965

4.3.6 L-TI-26 octubre de 2019. ”Lineamientos para gestión de incidentes y vulnerabilidades de seguridad de la información. Su objetivo es asegurar que los incidentes y vulnerabilidades de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente mediante el despliegue de acciones o actividades correctivas que permitan minimizar sus efectos”[23].

4.3.7 Decreto 1377 de 2013. “Por el cual se reglamenta parcialmente la ley 1581 de 1012. Mediante este decreto, el gobierno nacional reglamenta y ordena algunas disposiciones respecto a la ley 1581 de 2012, para la protección de datos personales, que, concede el derecho a todas las personas, de conocer, actualizar o modificar toda la información que se haya recogido sobre ellas en bases de datos o archivos”[24].

El decreto 1377 determinó que el tratamiento de datos personales debe estar legalizado por medio de un contrato suscrito entre el dueño de la información y responsable de tal actividad. También determinó que el segundo debe responder por los perjuicios ocasionados a los titulares de los datos personales por el tratamiento inadecuado de los mismos.

4.4 MARCO HISTÓRICO

En el año 1988 se presentó el primer gran ataque a las tecnologías de la información, a causa de un gusano informático, conocido con el nombre de Morris. Como lo relata West-Brown Moira y otros[25], Este ataque fue obra de Robert Tappan Morris, un estudiante de la Universidad de Harvard de 23 años. El gusano terminó afectando un 10% de los sistemas conectados al entonces ARPANET (Advanced Research Projects Agency Network), antecesor de lo que hoy conocemos como Internet.

Gran parte de los equipos afectados corresponde a servidores de correo y de la troncal principal de ARPANET, lo cual motivó a muchos sitios a retirar sus sistemas de la red para evitar ser infectados, dejando inoperantes muchos canales de comunicación y causando un alto costo en dinero por la falta de conexión. Por esta

[23] DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. (2019). Lineamiento para gestión de incidentes y Vulnerabilidades de seguridad de la información. Disponible en: https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/L-TI-26-Gestion-Incidentes-Vulnerabilidades.pdf

[24] JURISCOL. (2013). Sistema Único de Información Normativa. Decreto 1377 de 2013. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081

[25] GEORGIA Killcrece, Klaus-Peter Kossakowski, Robin Ruee, and Mark Zajicek. State of the practice of computer security incident response teams (csirts). Technical report, DTIC Document, 2003. Disponible en: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

razón surge la necesidad de establecer un trabajo coordinado entre los administradores de TI, para gestionar la seguridad de la información de manera eficiente. Luego de identificar la necesidad, la DARPA (Defense Advanced Research Projects Agency), anuncia financiamiento para el desarrollo de un centro de incidentes de seguridad, enfocado en atender el problema de un modo más organizado y estructurado. Es entonces cuando nace CERT, Coordination Center (CERT-CC), en diciembre de 1988, en Pensilvania EE.UU.

Con el paso de los años, fueron a pareciendo más equipos de respuesta a incidentes, cada uno según su propósito, ubicación geográfica, presupuesto y grupo de clientes atendidos. La interacción entre estos equipos se dificultó debido a las diferencias de idioma, zona horaria, y legislación internacional. Desde entonces los CSIRT han venido evolucionando de acuerdo a las necesidades de las organizaciones públicas y privadas a nivel mundial, dando la relevancia suficiente para poder atender oportunamente los incidentes de seguridad informática que también evolucionan a diario.

4.5 MARCO ESPACIAL

El proyecto aplicado se desarrolla en el ámbito de las diferentes organizaciones públicas o privadas, que tienen la necesidad de atender los incidentes de seguridad informática que se pueden presentar a diario en sus sistemas de información e infraestructura tecnológica, con el fin de dar respuesta inmediata y contrarrestar el daño o posible afectación a los objetivos del negocio o misión institucional, de manera oportuna.

El proyecto se enmarca dentro de las posibilidades y entorno que permiten las leyes y el marco tecnológico en Colombia, Donde, como ya se describió antes, existen diversas opciones de implementación de un CSIRT. Que, para este caso, se trata del tipo comercial, donde se proporciona servicio de CSIRT a cambio de una remuneración, a través de Acuerdos de Nivel de Servicio SLA.

4.6 MARCO METODOLOGICO

Para la elaboración de este proyecto se utilizará una metodología documental descriptiva, seleccionando y compilando información a través de la asimilación y crítica de títulos y documentos, y demás material de consulta con respecto a la implementación de Equipos de respuesta a Incidentes de seguridad Informática.

La metodología es cuantitativa, puesto que uno de sus objetivos es la cuantificación, medición y análisis estadístico de datos recolectados, respecto la cantidad de

incidentes, amenazas, riesgos, vulnerabilidades y ataques contra las infraestructuras tecnológicas de las organizaciones a nivel mundial. Por otro lado, la metodología también es cualitativa, cuando se indaga por las características de las diferentes funciones y equipos que conforman el CSIRT, para poder establecer condiciones de eficiencia y eficacia de las tareas de gestión ante incidentes de seguridad, al momento de garantizar la integridad, disponibilidad, y confiabilidad de la información.

La técnica de recolección de información que se va a utilizar es documental, realizando análisis y estudio de casos de implementación de CSIRT en organizaciones públicas y privadas a nivel mundial, recolectando datos de incidencias y utilización de nuevas técnicas que permitan afinar las políticas de planteamiento, configuración y administración de un equipo de Respuesta a Incidentes de Seguridad Informática.

4.7 MARCO TECNOLÓGICO

4.7.1 Sistemas de Detección de Intrusos IDS. Mecanismos que hacen parte del conjunto de seguridad de una organización. Cristian Borghello, indica en la revista SEGU INFO, que consiste en herramientas (software) o equipos (hardware), que se encargan de detectar actividades anómalas, a través de un conjunto de métodos y técnicas que pueden revelar la actividad sospechosa de un recurso del sistema o comportamiento anómalo en los paquetes del tráfico de red[26].

Los IDS se clasifican según su función de la siguiente manera:

4.7.1.1 Host-Based IDS: Operan en un host para detectar actividad maliciosa en el mismo.

4.7.1.2 Network- Based IDS: Operan sobre los flujos de información intercambiados en una red.

4.7.1.3 Knowledge- Based IDS: Sistemas basados en Conocimiento.

[26] Borghello, Cristian. 2020. Detección de Intrusos en tiempo Real. Noticias sobre seguridad de la información. SEGU INFO. [Consultado 20 de mayo 2020]. Disponible en: https://www.segu-info.com.ar/proteccion/deteccion

4.7.1.4 Behavior-Based IDS: sistemas basados en Comportamiento. Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperado de un usuario en el sistema

4.7.2 APT´s Advanced Persistent Threat. Amenaza Avanzada Persistente, traducido al español. Se trata de un tipo sofisticado de ciberataque, que demanda más creatividad y esfuerzo de los delincuentes, puesto que prefieren objetivos de gran escala como organizaciones.

Se basan en el robo de información y espionaje de sistemas, con una característica especial, que ejecutan el ataque de manera constante, donde los responsables son muy dedicados, y tienen un objetivo específico. A diferencia de otras técnicas que buscan infectar la mayor cantidad posible de equipos, por ejemplo, utilizando redes de botnets, donde, entre más víctimas alcanzadas, mayor posibilidad de obtener dinero o recursos informáticos.

Los objetivos de las APT, se eligen y estudian detalladamente con tiempo de anticipación, generalmente enfocado a grandes empresas y organizaciones gubernamentales, buscando afectar un determinado equipo o servicio, el cual contiene información de alto valor. Como menciona Lorena Fernández[27], se pensaría que estos ataques están dirigidos a ejecutivos de alto nivel o personal a cargo de información financiera, pero por obvias razones, dicho personal cuenta con controles de seguridad y personal trabajando para proteger la información que ellos manejan. Por lo tanto, los APT eligen objetivos más sencillos como empleados de bajo nivel, los cuales no ejecutan tareas importantes dentro de la organización y tampoco almacenan en sus equipos información sensible, pero si se encuentran dentro de la misma red del objetivo principal, utilizándolo como un puente para llegar

Los grupos de APT, están motivados por mucho más que solo perjudicar a usuarios o personas, estos dedican tanto tiempo, infraestructura y esfuerzo, porque están orientados en conseguir altísimas cantidades de dinero o poder, cuando se trata de espionaje político, o robo de información confidencial de los gobiernos. También se han registrado ataques que buscan el robo de información de propiedad intelectual de las diferentes áreas del conocimiento, como patentes o secretos comerciales, para luego venderla de alguna manera. Se ha determinado que la mayoría de ataques APT, empiezan por la explotación de vulnerabilidades ya conocidas y que la víctima no ha podido tratar. De esta manera la víctima no podrá distinguir fácilmente si se trata de un APT o un ataque tradicional.

[27] FERNANDEZ, Lorena. (2020). Redes Zone. Qué son los Advanced Persistent Threats y cómo protegernos de los APT. [consulta 30 de mayo 2020] Disponible en: https://www.redeszone.net/tutoriales/seguridad/advanced-persistent-threats-apt-protegernos/

Para poder identificar que se trata de un ataque APT, se han documentado las siguientes características:

- Aumento de registros de inicio de sesión por la noche
- Presencia de backdoors de tipo troyano
- Flujo de datos mayor que el normal
- Transporte de datos sospechosos
- Campañas de Phishing especificas (speer phishing)

Figura 3. Advanced Threat Lifecycle

Fuente: KASPERSKY. (2020). [Sitio web]. 5 Warning Signs of Advanced Persistent Threat and How to Prevent Advanced Persistent Threats. The Advanced Threat Lifecycle. [Consulta: 30 de mayo 2020]. Disponible en: https://www.kaspersky.com/resource-center/threats/advanced-persistent-threat

Según Imperva[28], un ataque APT exitoso puede tener 3 fases, como se detalla a continuación:

[28] IMPERVA. (2020). [sitio web]Amenaza Persistente Avanzada (APT). [Consulta: 30 de mayo 2020]. Disponible en: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

4.7.2.1 Infiltración: Se produce atacando los activos web y los recursos de red a través de inyección de código u otros métodos. O atacando usuarios humanos mediante el uso de ingeniería social, como spear Phishing, donde realizan un análisis y estudio de los gustos y actividad diaria en internet, para lograr llamar más fácil la atención de la víctima y hacer que caiga en el anzuelo. A la vez pueden enviar ataques de DDoS, para distraer al personal de seguridad de la red y debilitar el perímetro.

Una vez se logra la infiltración, los atacantes pueden instalar un Shell de puerta trasera, que puede otorgar gestión remota

4.7.2.2 Expansión: Al establecer el acceso remoto a un equipo dentro de la red, el grupo APT, comienza acciones para comprometer más miembros de la organización, recopilando información crítica como datos de empleados y registros financieros. En esta etapa, dependiendo del objetivo, ya se podría vender la información extraída o modificarla para sabotear algún proceso de la empresa.

4.7.2.3 Extracción: Generalmente el ataque APT, almacena la información recolectada en un lugar seguro dentro de la red. Para extraerla los delincuentes utilizan técnicas de ruido blanco, como ataques de denegación de servicio distribuido para distraer a los administradores de red y debilitar los controles de seguridad, mientras extraen la información que necesitan

4.7.3 EDR Endpoint Detection And Response. Ante la aparición de nuevas y mejoradas técnicas de ataque a las estructuras tecnológicas, el índice de amenazas actual se ha aumentado considerablemente, donde las tecnologías preventivas no logran proteger eficazmente a las organizaciones. Surge la necesidad de soluciones especializadas enfocadas en los puntos finales para prevenir ataques dirigidos y técnicas complejas como las APT.

Para comprender mejor en que consiste la herramienta EDR, podemos definir endpoint como un dispositivo informático de punto final, que se comunica de manera bidireccional a la red a la que pertenece, y que son la principal puerta de acceso de los delincuentes para atacar una organización. Las herramientas EDR, se usan para atender incidentes en los puntos finales de la red.

Las Herramientas EDR, monitorean los endpoint, recopilando información de los eventos, que luego se registran en una base de datos encargada de realizar análisis, detección, informes y alertas, logrando establecer amenazas a través del análisis de dichos eventos. Sus principales características son: capacidad de anticipación

ante ataques dirigidos mediante el análisis de patrones de comportamiento, disminución del tiempo de exposición a ataques debido a su capacidad reactiva, y una visión global de amenazas contra los endpoints.

4.7.4 Gestor de Contraseñas. Es una aplicación que permite almacenar nombres de usuario y contraseñas de acceso a las diferentes cuentas, servicios, aplicaciones entre otros. Esta información es almacenada en una base de datos cifrada con una contraseña única o clave maestra, para que nadie más que el dueño pueda acceder a dichas contraseñas. De esta manera el usuario solo debe recordar una clave maestra para gestionar las diferentes claves de acceso.

También proporcionan el servicio de generar contraseñas aleatorias para evitar que siempre se use la misma contraseña para una determinada cuenta, y para evitar que el usuario pierda tiempo buscando una contraseña adecuada y que cumpla con los requisitos mínimos exigidos, permitiendo indicar el grado de fortaleza de la palabra o la cadena.

Para elegir un adecuado gestor de contraseñas se deben tener en cuenta las siguientes características:

4.7.4.1 Múltiple factor de autenticación. Control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser.

4.7.4.2 Alertas de seguridad. Característica del gestor de contraseñas que informa o avisa al usuario cuando alguno de los servicios que utiliza ha recibido algún tipo de ataque que pueda comprometer sus cuentas.

4.7.4.3 Versión Portable. El gestor de contraseñas debe contar con una versión portable que se pueda instalar donde quiera que vaya el usuario y tener gestión de sus contraseñas almacenadas.

4.7.4.4 Integración con el navegador. Permite que el gestor de contraseñas coordine y gestione contraseñas de servicios web.

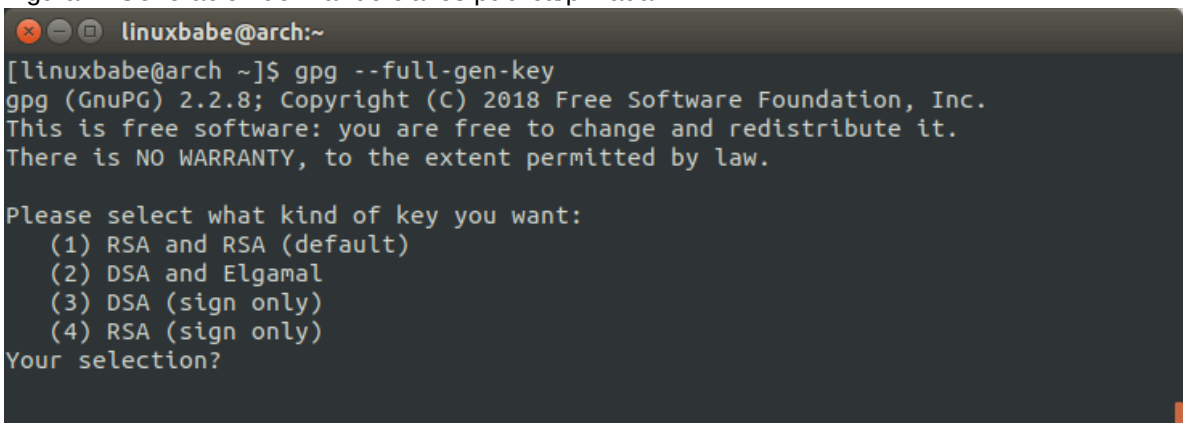
4.7.4.5 Tipo de cifrado. El gestor de contraseñas debe contar con un sistema de cifrado robusto y seguro para proteger la base de datos.

5 DESARROLLO DE LOS OBJETIVOS

5.1 HERRAMIENTAS DE HARDWARE Y SOFTWARE

5.1.1 GNU PG [29]. Implementación completa y gratuita del estándar OpenPGP según lo definido por RFC4880[30], (también conocido como PGP). GnuPG le concede la oportunidad de cifrar y suscribir sus datos y comunicaciones; tiene una plataforma de administración de contraseñas versátil, junto con aplicaciones para diferentes tipos de claves públicas. GnuPG, que también se conoce como GPG, es una herramienta de consola, que utiliza comandos que se adapta fácil a otros aplicativos o herramientas

Figura 4. Generación del Par de claves publica/privada



Fuente: GUOAN, Xiao. (2018). Una guía práctica para GPG - Parte 1 Genere su par de claves. Linuxbabe. [Consulta: 14 de junio 2020]. Disponible en: https://www.linuxbabe.com/security/a-practical-guide-to-gpg-part-1-generate-your-keypair

Una de las principales razones por la que se elige GNU PG, como ya es de público conocimiento que todo el software de GNU es libre, y además se encuentra registrado con licencia GPL (General Public License), la cual garantiza a cualquier organización que lo use, la posibilidad de usar, trabajar, copiar y alterar el software. También, protege el software a través de copyleft, lo cual impide que se apropien de él y le quiten las mencionadas libertades.

Esta herramienta es altamente eficaz en el cifrado de comunicaciones, que puede ser utilizada en cifrado de firma digital, mensajes de correo electrónico y archivos. Cuenta con diversos algoritmos de cifrado simétrico y asimétricos, como RSA, IDEA,

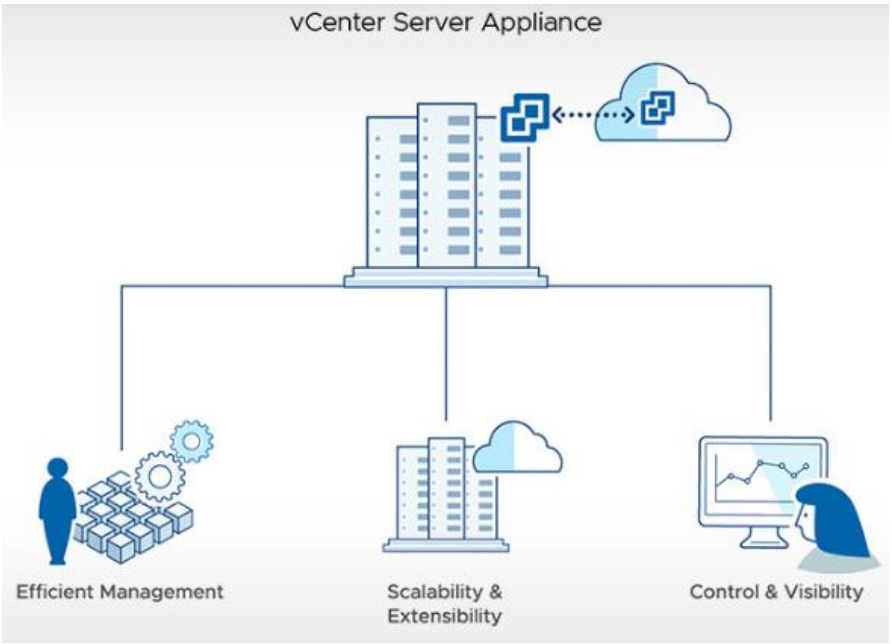
[29] GNUPG. El GNU Privacy Guard. implementación completa y gratuita del estándar OpenPGP. Disponible en: https://www.gnupg.org/
[30] OPENPGP INC. (2007). RFC 4880. Disponible en: https://tools.ietf.org/html/rfc4880

SHA1, ELG, DSA, 3DES, CAST5, AES, entre otros. El cifrado predeterminado de GPG es CAST5, sin embargo, este puede ser cambiado por el usuario, seleccionando alguno de la lista de posibilidades antes nombradas. Posee una interfaz de consola o línea de comandos, pero también tiene la posibilidad de integrar interfaz gráfica a través del uso de algunos pluggins.

5.1.2 VMWare vSphere. "Plataforma de virtualización que permite crear infraestructuras en la nube. Incluye modelo de cloud hibrida y es compatible con más de 2500 aplicaciones. Cuenta con arquitectura hipervisor de vmware, que proporciona un entorno de virtualización optimo, probado para entornos de producción de alto rendimiento"[31].

Incluye también vCenter Server, que corresponde a una herramienta de administración, a través de una plataforma centralizada, que automatiza una infraestructura virtual y extendido a la nube VMware cloud.

Figura 5. Diagrama vCenter



Fuente: VMWARE. [Sitio web]. [Consulta: 21 de mayo de 2020]. VCenter Server. Disponible en: https://www.vmware.com/co/products/vcenter-server.html

Además de la extensibilidad, vCenter ofrece control y visibilidad centralizados para administrar toda la infraestructura desde el mismo lugar, administración con

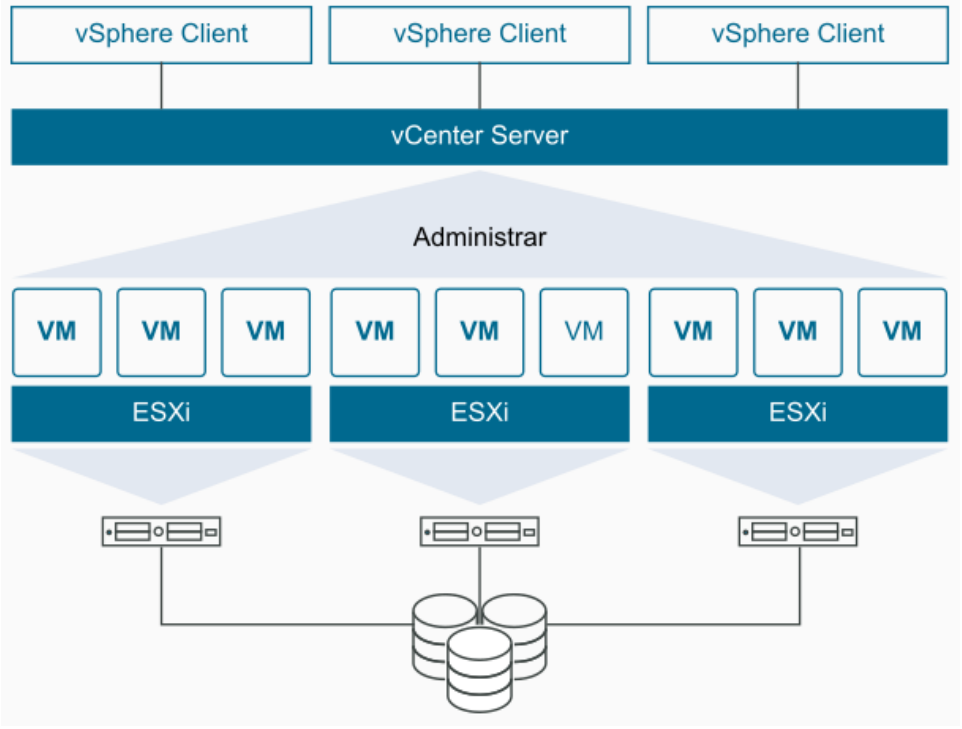
[31] VMWARE. (2011). Vmware vSphere Ediciones de Enterprise y Enterprise Plus. Hoja de datos. Disponible en: https://www.vmware.com/files/es/pdf/VMware-vSphere-Entreprise-Edition-Datasheet.pdf

herramientas potentes como vRealize log insight y optimización anticipativa para obtener la mayor eficiencia de los recursos.

La licencia con Operation Management Enterprise Plus, permite la administración y automatización de las operaciones inteligentes con técnicas de análisis predictivas y cuenta con un paquete de 25 OSI por instancia de vCenter Server Standard. La actualización de vRealize Operation proporciona optimización del rendimiento automatizado, paneles personalizables, análisis de costos específicos y una gran extensibilidad.

vSphere se encarga de transformar los centros de datos en infraestructuras de computación agregadas que incluyen recursos de redes, CPU y almacenamiento. También cumple con administrar dichas infraestructuras en un entorno operativo unificado proporcionando las herramientas para administrar los centros de datos que participan en el entorno.

Figura 6. Diagrama vSphere



Fuente: VMWARE DOCS. Documentación de vMware vSphere. [Consulta: 14 de junio 2020]. Disponible en: https://docs.vmware.com/es/VMware-vSphere/index.html

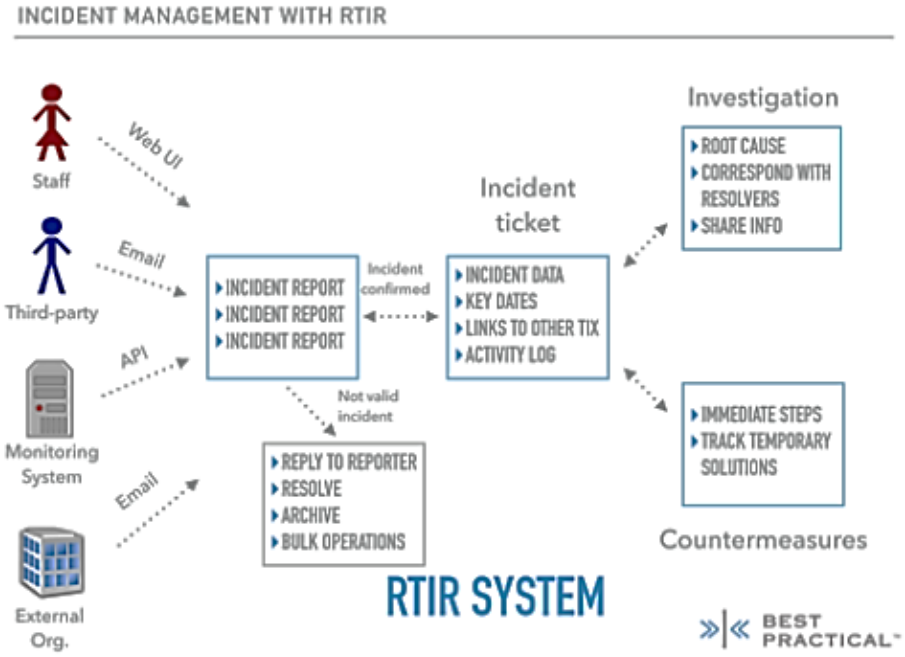
Para implementar toda la plataforma virtual del CSIRT, a través de vmware es necesario contar con 02 servidores con características de hardware robusto que permita garantizar el correcto funcionamiento de todos los servicios virtualizados.

Los siguientes son los requerimientos mínimos, teniendo en cuenta la guía de compatibilidad de hardware con vmware:

- Procesador: AMD EPYC 7001 Series
- 480GB SSD SATA Read Intensive 6Gbps
- Memoria: 32 sockets DIMM DDR4 – Mínimo 512 GB

5.1.3 Request Tracker For Incident Response RTIR. Rastreador de solicitudes para respuesta a incidentes, de Best Practical, se basa en todas las características de RT y proporciona colas de trabajo creadas para equipos de respuesta a incidentes. Es la favorita de muchos equipos CERT y CSIRT en todo el mundo. RTIR, posee características que sirven para correlacionar eventos importantes de incidentes, tanto de personas como de herramientas automatizadas, para encontrar secuencias y vincular múltiples informes de incidentes con un incidente de causa raíz común

Figura 7. Flujo de trabajo de gestión de incidentes RTIR.



Fuente: BEST PRACTICAL. Request Tracker for Incident Response (RTIR). [Consulta: 29 mayo de 2020] Disponible en: https://bestpractical.com/rtir/

Para poder hacer uso de RTIR, es necesaria la instalación de RT, en una máquina virtual con las siguientes características:

- Linux Ubuntu Server 20.04 LTS

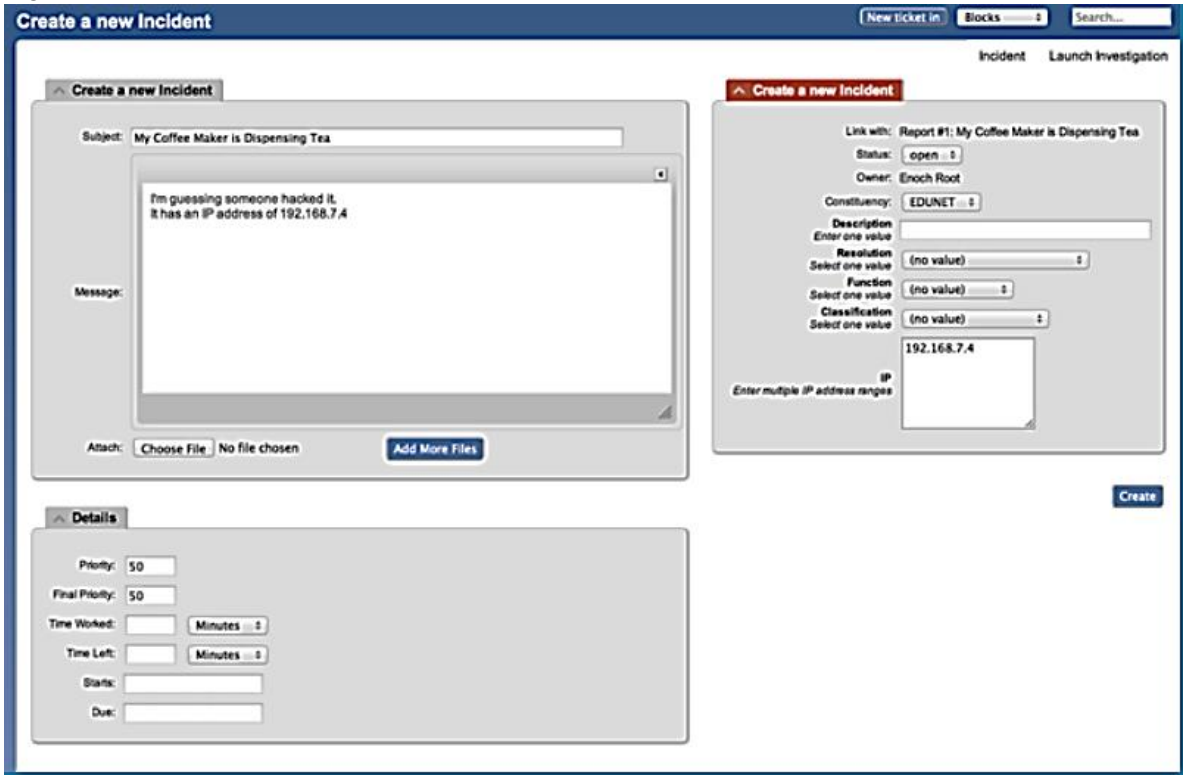
- Apache2
- MariaDB
- Perl

Se trata de una aplicación web, que cuenta con una base de datos en el backend, se puede ejecutar en cualquier navegador, inclusive en algunos equipos móviles.

Cuenta con una interfaz intuitiva y amigable con el usuario para la creación de incidentes:

RTIR permite crear reportes de incidentes personalizados que se acoplen a las necesidades de la organización:

Figura 8. Interfaz de creación de incidentes.



Fuente: FALCONE, Kevin. Request Tracker for Incident Response (RTIR). Best Practical. [Cosulta 14 de junio 2020]. Disponible en: https://www.terena.org/activities/tf-csirt/meeting38/falcone-rtir.pdf

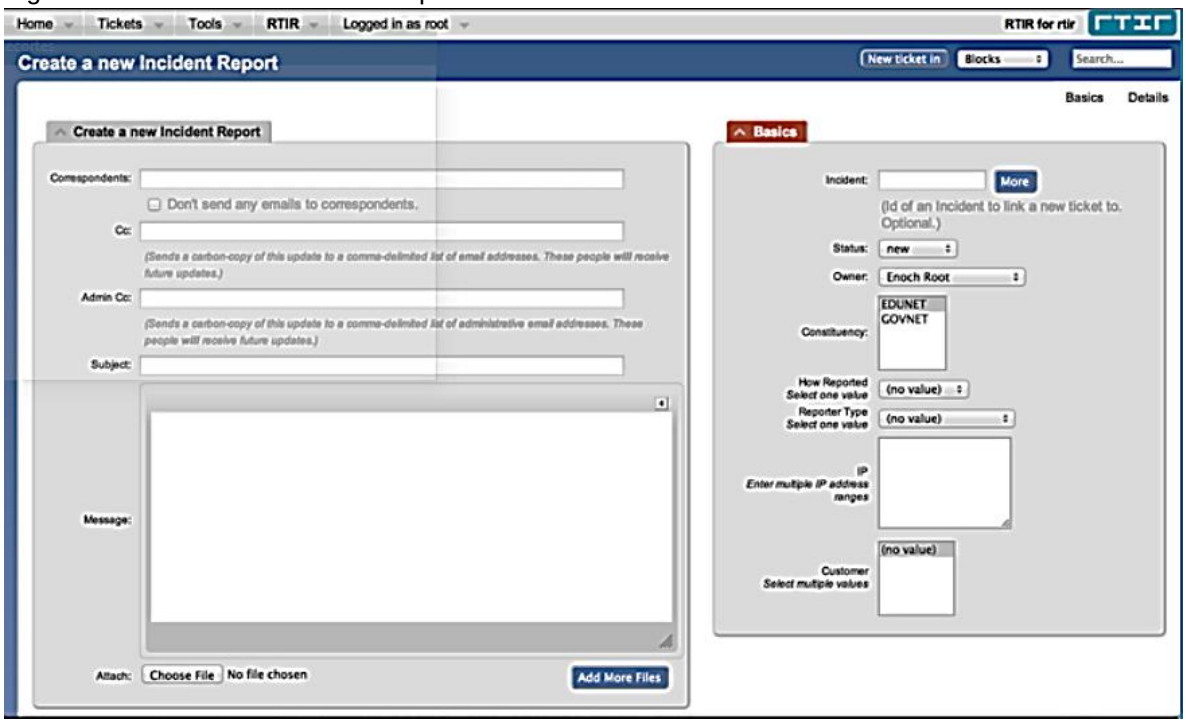
Para efectos de notificaciones, la interfaz de correo electrónico es compatible con diversos servidores de correo. El servidor web puede ser Apache u otro que admita el protocolo de interconexión de programas interactivos Fast CGI, Interfaz común

de entrada, el cual reduce la carga de interconexiones del servidor web, permitiéndole atender más conexiones a la vez.

RTIR, es un software comercial de código abierto que permite desarrollo personalizado o servicio profesional, para este caso se hará de manera personalizada, para reducir costos y que los miembros del CSIRT adecuen la solución para dar mejores resultados de acuerdo las necesidades de la empresa.

RTIR permite crear reportes de incidentes personalizados que se acoplen a las necesidades de la organización:

Figura 9. Interfaz de creación de reportes de incidentes.

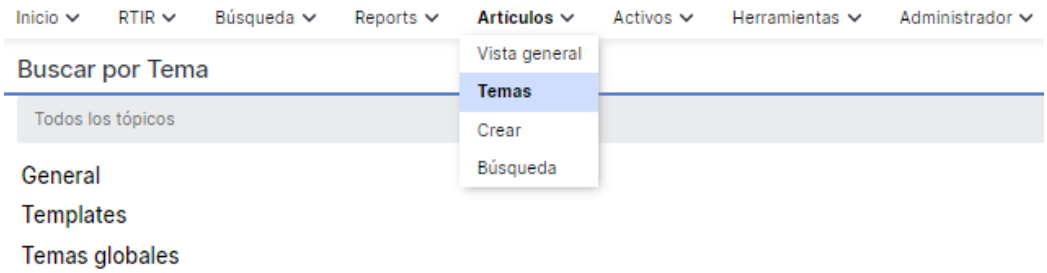


Fuente: FALCONE, Kevin. Request Tracker for Incident Response (RTIR). Best Practical. [Cosulta 14 de junio 2020]. Disponible en: https://www.terena.org/activities/tf-csirt/meeting38/falcone-rtir.pdf

RTIR cuenta con un módulo gestor de conocimiento llamado artículos, el cual, se encarga de sintetizar, organizar y administrar el conocimiento del CSIRT, de acuerdo a la información recopilada de los incidentes registrados.

El mencionado módulo, permite organizar los artículos por temas, que pueden ser parametrizados de acuerdo a las necesidades, como se puede evidenciar en la siguiente imagen:

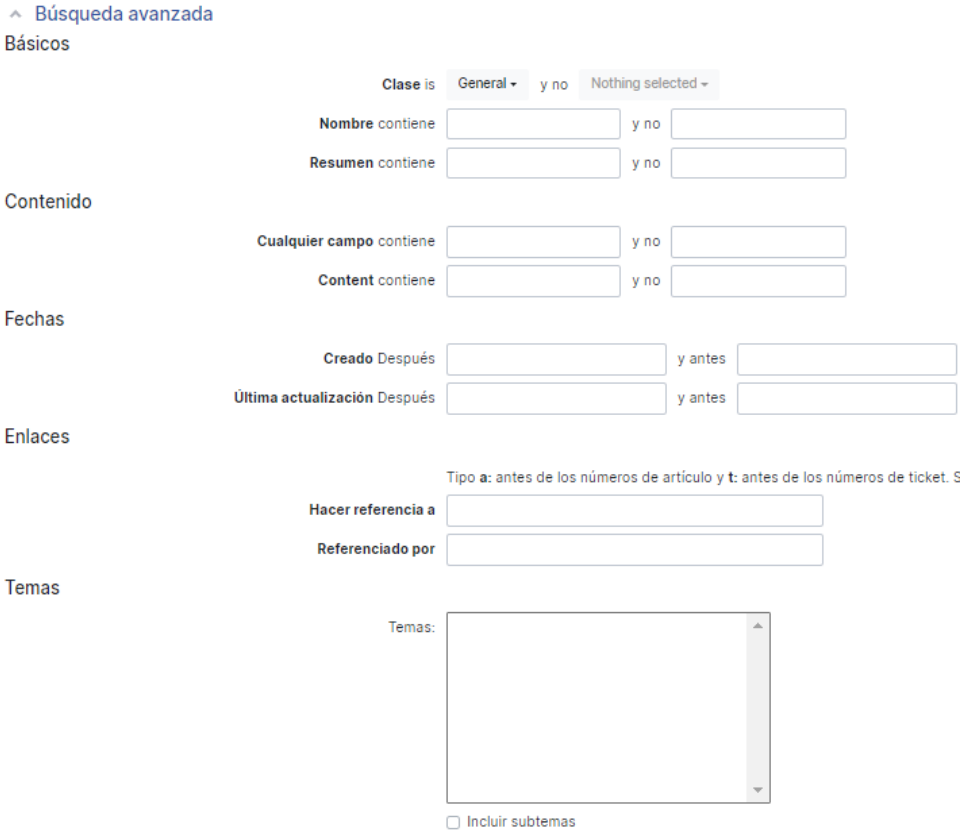
Figura 10. Módulo Artículos RTIR.



Fuente: propia del autor

Una característica destacada, es que cuenta con diversos atributos de filtrado para ejecutar una búsqueda avanzada, de incidentes ya superados. Como también la posibilidad de configurar respuestas predefinidas para responder a las preguntas más frecuentes.

Figura 11. Búsqueda avanzada RTIR.



Fuente: propia del autor

5.1.4 Data Storage. Con la implementación de nuevas técnicas de virtualización, el almacenamiento toma una importante relevancia, en términos de la optimización del uso de recursos y reducción de costos. Al concentrar todo el almacenamiento en un solo lugar, no sólo impacta de manera positiva a los servidores, sino también a las aplicaciones y estaciones de trabajo, que al final se ve reflejado en una mejor experiencia del usuario final.

La clasificación de almacenamiento de datos se divide en cuatro tipos:

- DAS (Direct Attached Storage - Almacenamiento de Conexión Directa). Se trata de un método, donde se conecta las unidades de almacenamiento (discos) directamente al servidor o host.

- NAS (Network Attached Storage - Almacenamiento Conectado en Red). Consiste en un dispositivo de almacenamiento conectado a la red LAN, permitiendo acceso a varios hosts a su almacén de datos por medio de una IP. Administrado por un servidor de archivos.

- SAN (Storage Area Network - Red de área de Almacenamiento). Almacenamiento compartido que ofrece conmutación entre múltiples nodos. Conexiones de fibra óptica y relativamente independiente de la red LAN.

- Almacenamiento de datos en la nube. Proveedores comerciales que ofrecen servicio de almacenamiento virtualizado en la nube, bajo demanda. Puede ser pública, privada o hibrida.

El tipo de almacenamiento para este caso, es SAN, Storage Area Network, el cual, permite una topología de red flexible, y gracias a las conexiones con fibra óptica (FC Fiber Channel), proporciona alta velocidad de transferencia de datos. Además de mejorar el rendimiento, permite disponer de funcionalidades como alta disponibilidad, clonaje volúmenes, respaldo y migración de datos, entre otras.

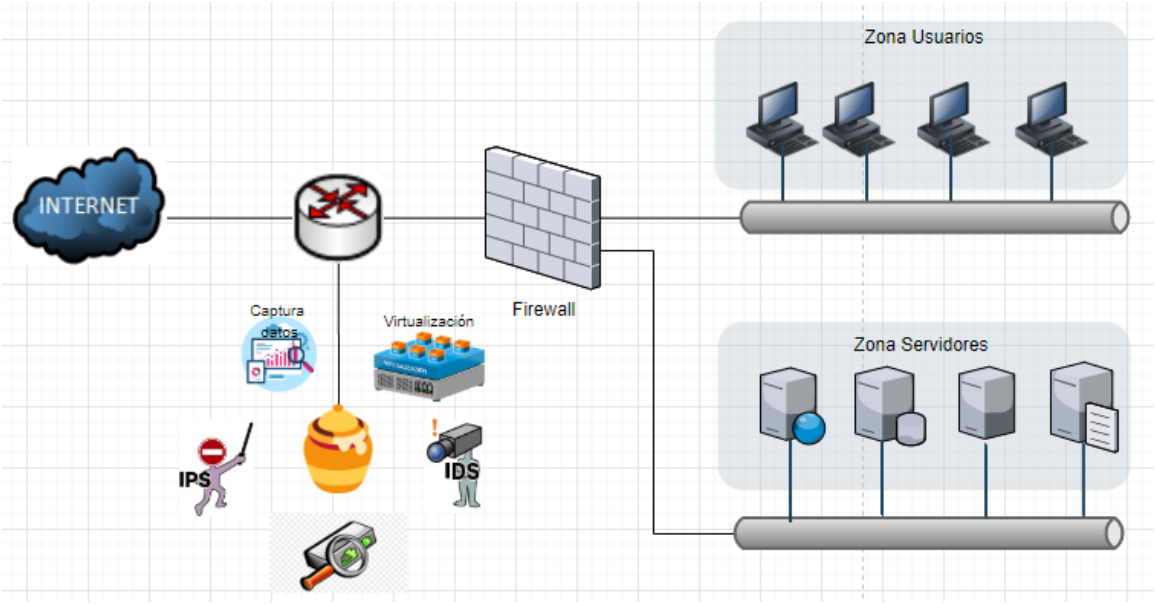
Las características mínimas del equipo adecuado para el almacenamiento del CSIRT son las siguientes:

- S.O: Microsoft Windows Storage Server 2016
- Protocolos de acceso: CIFS, NFS, FTP, SMB3.0, SMB Direct (RDMA)
- Procesador: 6 núcleos, 1.9GHz, 15M cache, 85W
- Arreglo de disco: RAID 10

El acceso al almacenamiento debe estar segmentado como una nube privada, y la seguridad administrada a través de la plataforma Firewall, garantizando la vinculación virtual de los recursos de red con el almacenamiento sin necesidad de una conexión física.

5.1.5 HONEYNET. Para fortalecer la plataforma de seguridad de Ciber Security de Colombia Ltda. en cuanto a IDS/IPS, se propone incluir en su arquitectura de red, una honeynet, con función de producción, puesto que se va a utilizar para proteger la información en un ambiente real, con alto nivel de interacción para poder analizar todo el tráfico que circula en la red, e implementada de manera virtual con el fin de reducir todos los costos que implica el montaje con equipos y software real, que conlleva la compara de licencias y contratación de mantenimientos preventivos y correctivos con la inclusión de repuestos.

Figura 12. Ubicación Honeynet



Fuente: Propia del autor

La implementación, se detalla en the Honeynet Project[32], que consiste en mostrar a los atacantes una red virtual que parezca la real, lo cual permitirá a la empresa, descubrir patrones de ataques, herramientas y métodos de los ciber delincuentes, con el objetivo de analizar el comportamiento de los mismos y ejecutar las políticas y medidas necesarias para contrarrestar dichos ataques en la red real, cerrando las brechas de seguridad que pueda tener la red. Una característica importante de la honeynet, es que no bloquea las acciones de los atacantes, sino que las deja pasar,

[32] THE HONEYNET POJECT. (2019). Sobre nosotros. [Consulta: 29 de mayo 2020]. Disponible en: https://www.honeynet.org/about/

para realizar un monitoreo y registro de las mismas, imitando un entorno del sistema real.

La honeynet ejecutará dos aspectos importantes:

- Control de datos: Actividad de contención, que permite al atacante realizar ciertas maniobras en el honeypot comprometido, sin que el atacante sospeche que se encuentra en un ambiente de prueba y sin que afecte nuestra red real.

- Captura de datos: es la captura y registro de todas las actividades que realiza el atacante, las cuales sirven para aprender de las modalidades, técnicas y métodos utilizados por los ciber delincuentes, sin que se den cuenta que están siendo monitoreados. Dichos registros no pueden ser almacenados en la honeypot

Para la implementación de la honeynet, se relacionan los siguientes requerimientos técnicos:

Requerimientos de Software:

- Herramientas de captura de Honeynet. (Honeywall)[33]. Herramienta de la distribución Linux basada en CentOS, que cuenta con todas las funcionalidades de captura, control y análisis de datos, como: snort, snort in line, Sessionlimit, Sebek, Walleye, Pcap, IPtables, Swatch, Argus + Hflow, Mysql

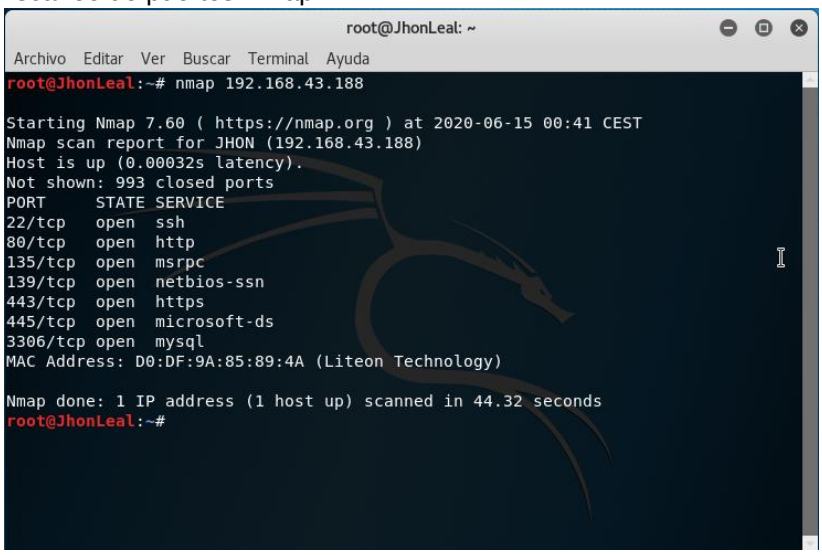
- Kali Linux[34]. Distribución basada en Debian, diseñada para auditoría y seguridad Informática. Fundada por Offesive Security Ltd, con más de 600 herramientas preinstaladas, entre las que se destacan: escáner de puertos y vulnerabilidades, archivos metaexploitables, snifer, herramientas de análisis forense y herramientas de auditoría de tráfico inalámbrico

  Dentro de la gran variedad de herramientas con las que cuenta Kali Linux, se destacan las siguientes:

[33] THE HONEY PROJECT. (2019). Honeywall CDROM. [Consulta: 29 de mayo 2020]. Disponible en: https://www.honeynet.org/projects/old/honeywall-cdrom/
[34] KALI, By Offensive Security. (2020). About Kali Linux. Disponible en: https://www.kali.org/about-us/

Nmap, traduce Network Mapper, se trata de una herramienta muy útil para los administradores de sistemas de información, que permite escanear todo el tráfico de una red, entregando información de puertos abiertos de un determinado host, y el servicio que hay detrás de dicho puerto abierto.

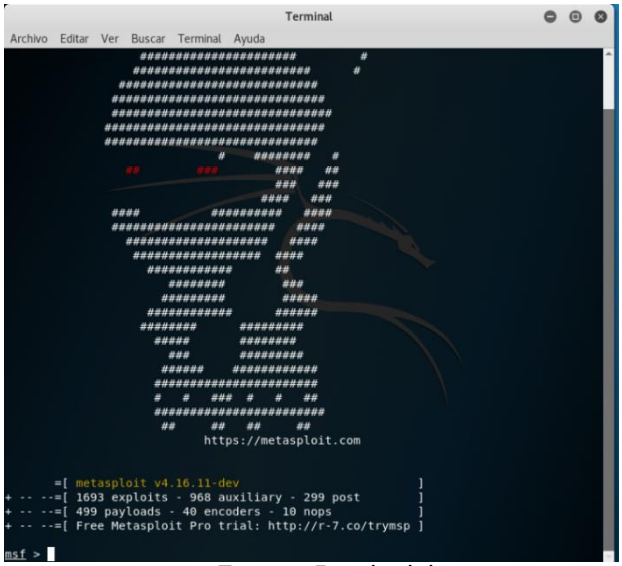
Figura 13. Escaneo de puertos Nmap



Fuente: Propia del autor

Metasploit, es una herramienta de seguridad, que aporta información acerca de vulnerabilidades y sirve para realizar pruebas de penetración y desarrollo de firmas para sistemas de detección de intrusos.

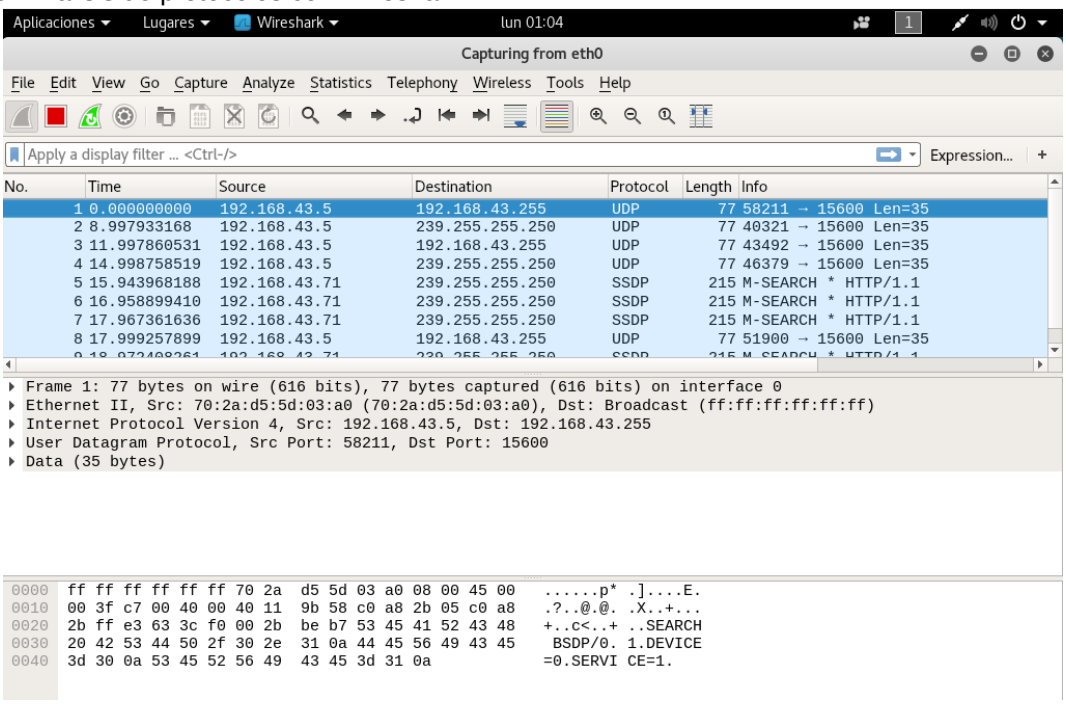
Figura 14. Test de penetración Metasploit.



Fuente: Propia del autor

Wireshark es un analizador de protocolos open-source, cuyo objetivo es el análisis de tráfico, implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos existentes.

Figura 15. Análisis de protocolos con Wireshark



Fuente: Propia del autor

- Sistema Operativo de Red, NOS. DENT[35]. Es un sistema operativo de red estandarizado, de código abierto, basado en Linux. Trata por igual la infraestructura subyacente para la creación de rutas de redes, al tiempo que simplifica las abstracciones existentes como los API, controladores y software abierto. Une a usuarios finales de todas las verticales y permite la transición a redes desagregadas. Permite la colaboración entre desarrolladores a través del hardware de red, con posibilidad de gran variedad de soluciones.

- Microsoft[36] Windows 10 Pro x 64. Es la más vigente versión de sistemas operativos desarrollado por Microsoft, de la familia Windows. Su lanzamiento fue en el año 2015. Con características integradas de seguridad, como

[35] THE LINUX FUNDATION PROJECTS. (2020) DENT Un NOS para todos los demás. Disponible en: https://dent.dev/

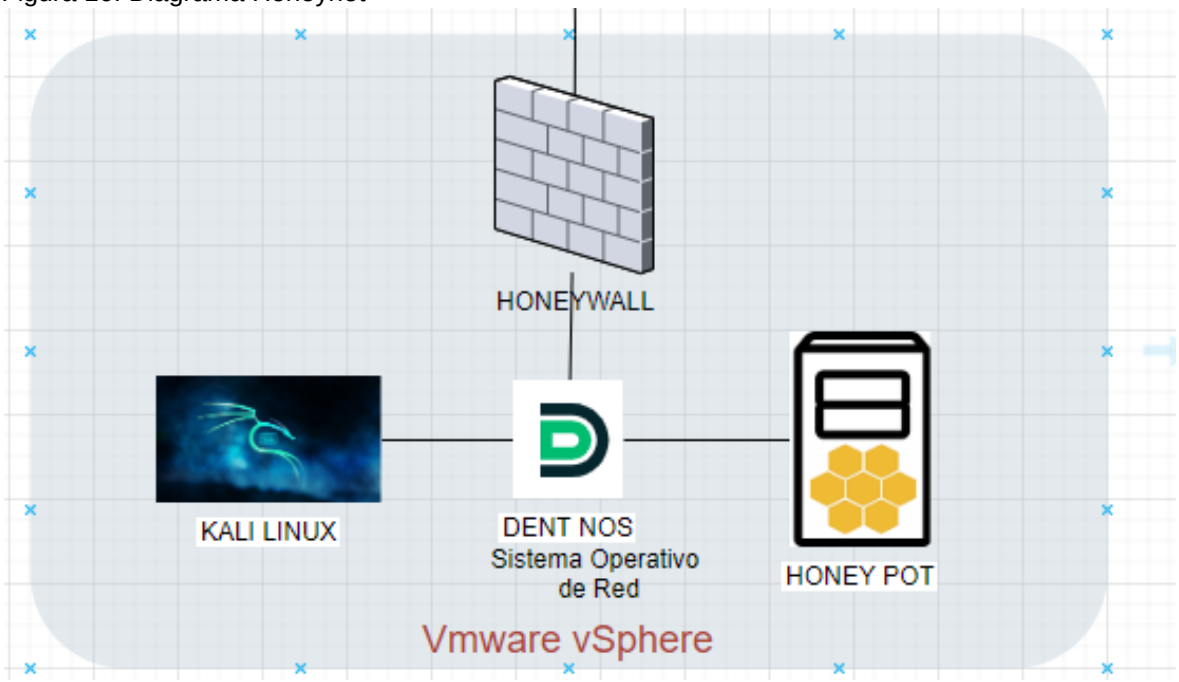
[36] MICROSOFT. (2020). Windows 10 Pro. Disponible en: https://www.microsoft.com/es-co/p/windows-10-pro/df77x4d43rkt?activetab=pivot:overviewtab

firewall y protecciones de internet, que evitan riesgos de virus, ransomware o malware.

- Sebek[37]. Herramienta de captura de datos, creada para capturar toda la actividad del atacante en un entorno trampa, sin que el atacante siquiera lo sospeche. Cuenta con dos componentes, uno que se ejecuta en los sistemas honeypot, recopilando, registros de teclado, tráfico de archivos y contraseñas, y el otro es el servidor al cual se envía de manera oculta toda la información recolectada.

- Valhala Honeypot[38]. Cuenta con los siguientes servicios para identificar atacantes: WEB, FTP, TFTP, POP3, ECHO, DAYTIME, SMTP, FINGER e PORT FORWARDING. Simula puertos de troyanos bien conocidos (Como el NetBus, SubSeven, etc).

Figura 16. Diagrama Honeynet



Fuente: Propia del autor

[37] HONEY PROJECT (2004). Página principal de Sebek. Disponible en: http://his.sourceforge.net/honeynet/tools/sebek/

[38] VALHALLA Honeypot - Honeypot de código abierto gratuito para el sistema Windows Disponible en: http://valhalahoneypot.sourceforge.net/

5.1.6 WatchThatPage[39]. Servicio que le permite recopilar automáticamente nueva información de sus páginas favoritas en Internet. Usted selecciona qué páginas monitorear, y WatchThatPage encontrará qué páginas han cambiado y recopilará todo el contenido nuevo para usted. La nueva información aparece en un mail y / o un sitio web personal. Puede especificar cuándo se recopilarán los cambios, de modo que estén actualizados cuando desee leerlos. El servicio es gratuito para cuentas más pequeñas.

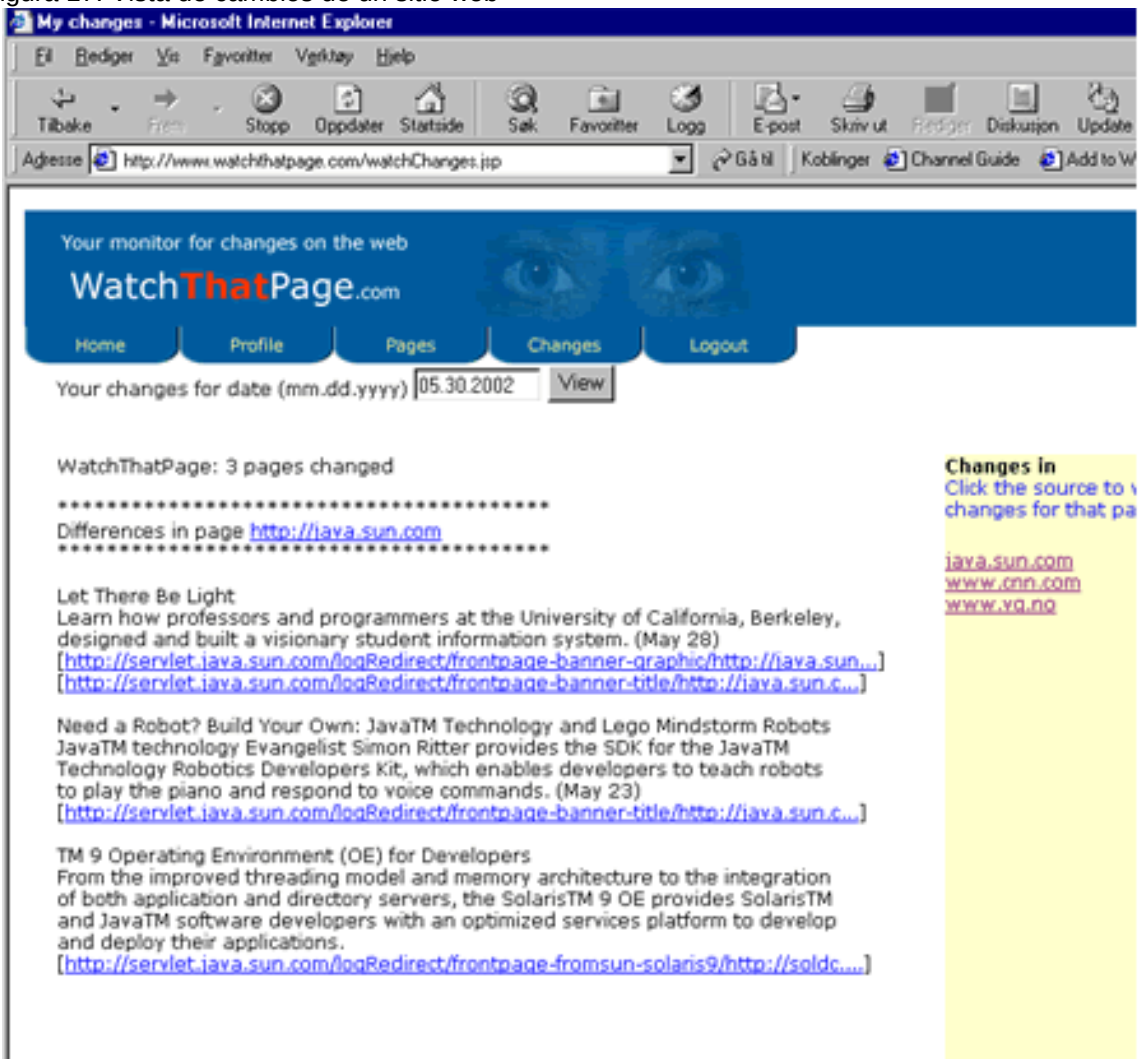
Esta herramienta permitirá al CSIRT, monitorear los cambios que se han presentado en determinados sitios web, que pueden ser los sitios más visitados por los empleados de la empresa de acuerdo con su función, los sitios web de empresas de la competencia, o que ofrezcan los mismos servicios de Cyber Security de Colombia Ltda. O incluso los mismos sitios web de la empresa, para descartar que se haya hecho un ataque de defacement o algún cambio de diseño, sin previo conocimiento de los administradores del sitio web.

La aplicación enviará un reporte a través de correo electrónico, que puede ser parametrizado con el fin de definir el tipo de reporte que se desea recibir, donde se puede definir que se entreguen reportes generales de cambios, o solamente los que coincidan con determinada palabra clave, los cambios más recientes o todos los cambios realizados. También se puede establecer el horario de entrega de los reportes y definir la frecuencia de entrega que puede ser diaria o semanal de acuerdo a las necesidades.

La herramienta permite agregar nuevas páginas para monitorear mientras se está navegando en la red, las cuales se pueden organizar por carpetas de acuerdo al tipo de sitio. Uno de los usos parametrizados puede ser monitorear la cantidad de usuarios activos que se encuentran visitando la página web oficial de la empresa, en rangos de tiempo determinados, para realizar un análisis estadístico de la actividad del sitio web y el interés que está generando alguna publicación en los clientes.

[39] WATCHTHATPAGE. (2017). Your monitor for changes on the web. Recuperado de: http://www.watchthatpage.com

Figura 17. Vista de cambios de un sitio web



Fuente: WATCHTHATPAGE. Your monitor for changes on the web. Visita guiada. Ver los cabios. [Consulta: 14 de junio 2020]. Recuperado de: http://www.watchthatpage.com/tutorialChanges.jsp

5.1.7 Listas de Control de Acceso ACL. Por sus siglas en inglés Access Control List, Es un elemento de seguridad informática que se usa para gestionar la separación de privilegios y establecer debidamente los permisos de acceso a un sistema o servicio determinado.

Como lo relata Campis Melendez[40], en su libro, se aplica en el ámbito de redes cuando se filtra de manera segura el tráfico de red, controlando en las interfaces de

[40] MELENDEZ CAMPIS, Camilo Andrés y TOUS TEJADA, Jesús Andrés. Listas de Control de Acceso (ACL) y Control de Acceso Basado en el Contexto (CBAC). [En línea]. Trabajo de grado. Universidad Tecnológica de Bolívar. Cartagena, 2012. [Consultado 29 de mayo 2020]. Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0063288.pdf

entrada y salida de los enrutadores o conmutadores, si los paquetes han sido enviados o bloqueados, en función de los criterios de la ACL. Por otro lado, también se puede aplicar ACL sobre políticas de un servidor Proxy, donde se puede controlar a quien se le permite acceso a ciertos contenidos de internet, y parametrizar limitaciones de ancho de banda, tiempo de uso, y horario.

Los siguientes son los tipos de ACL más comunes:

5.1.5.1 ACL Estándar: Sólo se especifica una dirección de origen y se compara con las direcciones configuradas en la ACL.

5.1.5.2 ACL Extendidas: Controlan el tráfico, comparando las direcciones de origen y destino de los paquetes, con las direcciones configuradas en la ACL.

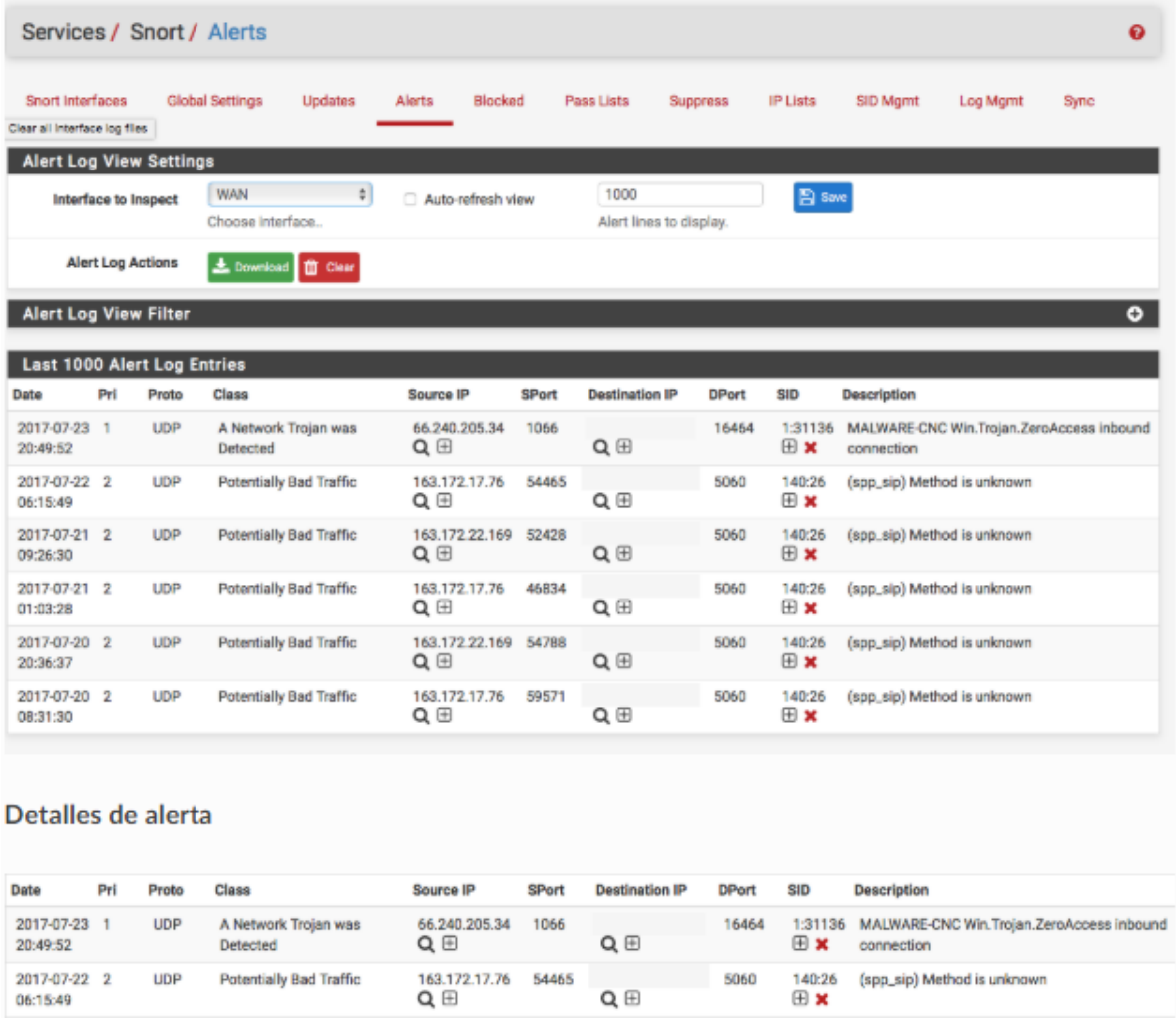
5.1.8 IDS Snort. Sistema de Detección de intrusiones IDS, basado en red. Utiliza un motor de detección de ataques y barrido de puertos, que permite registrar en tiempo real, cualquier evento extraño, determinado previamente por patrones relacionados con ataques. La enciclopedia colaborativa Ecured[41], manifiesta que esta herramienta es considerada como la más eficaz en la detección de intrusos y está disponible bajo licencia GPL, en versión libre y es compatible con los sistemas operativos Windows y UNIX/Linux. Cuenta con una gran cantidad de filtros y patrones previamente definidos, y actualizaciones constantes a medida que van apareciendo nuevas amenazas detectadas.

Snort permite dar de baja una conexión que emita tráfico malicioso a través del envío de un paquete con el flag RST activo, cumpliendo con esto, funciones de firewall en aspectos de IPS. La principal y más llamativa característica de Snort, es su subsistema flexible de firmas de ataques.

Cuenta con siete modos de alerta que se almacenan en el archivo alert.ids. Los usuarios pueden crear nuevas formas, basadas en características de ataques recibidos y cargarlas a la lista de firmas de Snort, para que todos los usuarios puedan beneficiarse, creando un ecosistema de conocimiento y experiencia compartidos.

[41] ECURED. Snort. Enciclopedia colaborativa en red del gobierno de Cuba. Disponible en: https://www.ecured.cu/Snort

Figura 18. Alertas de Snort

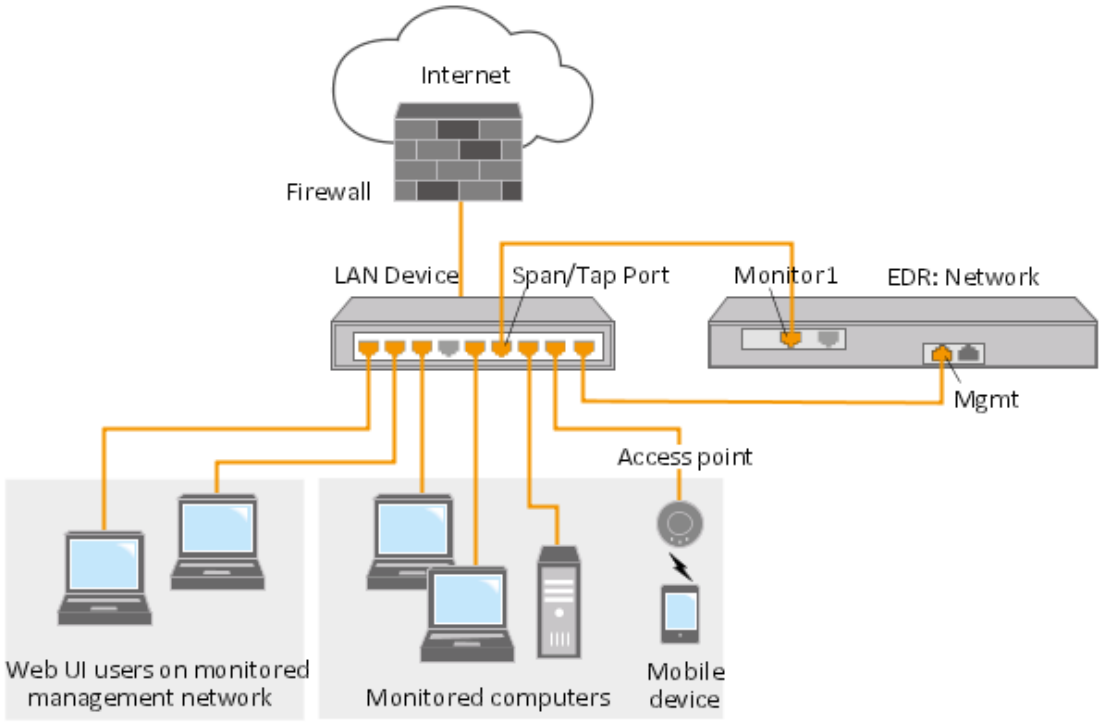


Fuente: NETGATE DOCS. Alertas de Snort. IDS/IPS Snort. [Consulta 14 de junio 2020]. Disponible en: https://docs.netgate.com/pfsense/en/latest/ids-ips/snort-alerts.html

5.1.9 EDR Symantec[42]. La herramienta Symantec Endpoint Security, es una protección multicapa para detener amenazas dependiendo de la manera como ataquen los endpoint. Puede ser gestionada totalmente en la nube de Symantec a través de una consola unificada, administrada de manera local instalando Symantec Protection Manager versión 14.1 o posterior, compatible con versiones de sistemas operativos Linux, Windows, Mac, IOS y Android. O puede ser administrada de forma hibrida con la instalación de Symantec Protection Manager y además inscribiendo cada dominio en la consola en la nube.

[42] SYMANTEC. (2020). [Sitio web]. Detección de punto final y respuesta. [Consulta: 30 de mayo 2020]. Disponible en: https://help.symantec.com/bucket/saep/edr?locale=EN_US

Figura 19. Ubicación appliance Symantec



Fuente: SYMANTEC, A división of broadcom. Donde colocar el appliance en su red para obtener mejores resultados. Symantec EDR 4.0. [Consulta:14 de junio 2020]. Disponible en: https://help.symantec.com/cs/SYMANTECEDR_4.0/EDR/v97213073_v128933990/D%C3%B3nde-colocar-el-appliance-en-su-red-para-obtener-mejores-resultados%7CSymantec-EDR?locale=ES_MX

Utiliza aprendizaje automático y análisis de comportamiento para detectar y exponer actividades sospechosas en la red. EDR alerta sobre una actividad potencialmente dañina, prioriza los incidentes para un Triage rápido y permite navegar por los registros de actividad del punto final durante su análisis forense de posibles ataques.

Permite contener eventos sospechosos, aislar puntos finales potencialmente comprometidos y eliminar archivos maliciosos y artefactos asociados. Proporciona seguridad a los endpoint de acuerdo a las siguientes fases de ataque: pre-ataque, ataque, violación y post-ataque. Cuenta con diversidad de características de acuerdo al tipo de gestión y a la suscripción de producto que se adquiera.

Aporta a la infraestructura, la capacidad de alerta anticipada de eventos sospechosos, lo cual permite prevenir la materialización de riesgos generados por dichos eventos. No está en la capacidad de detener un ataque, pero si puede generar distintos tipos de respuesta a los ataques.

Figura 20. Vista de resumen de eventos EDR Symantec

Fuente: SYMANTEC, A división of broadcom. Trabajar en la vista de Resumen de eventos. Symantec EDR 4.0. [Consulta:14 de junio 2020]. Disponible en: https://help.symantec.com/cs/SYMANTECEDR_4.0/EDR/v121261470_v128933990/Trabajar-en-la-vista-Events-Summary-(Resumen-de-eventos)?locale=ES_MX

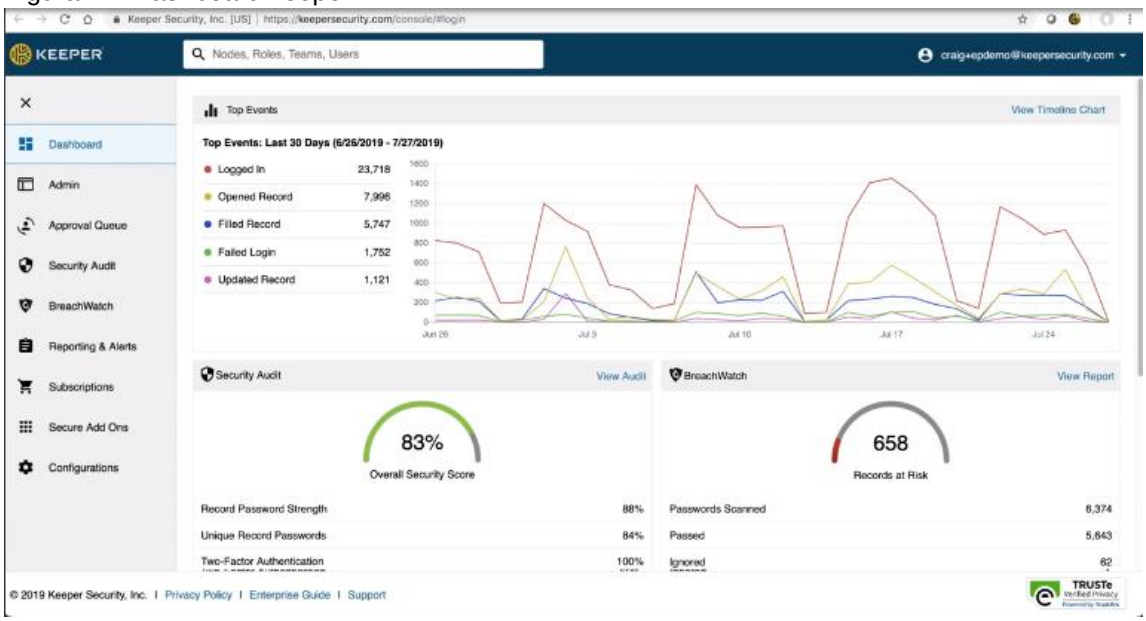
EDR Symantec[43], permite configurar notificaciones para alertar a los administradores a través de correo electrónico de manera automática, cuando se presentan incidentes con los usuarios finales, parametrizando el tipo de alerta y relacionando cuentas personalizadas de correo electrónico a donde se requiere enviar dicha información. Como se evidencia en el video tutorial de Configuración de notificaciones de alerta.

[43] SYMANTEC. A división of broadcom. Configuración de notificaciones de alerta. [Archivo de video]. 2017. 1.9 min. Disponible en: https://help.symantec.com/cs/SEPC/SEPC/v109630219_v101064224/Configuraci%C3%B3n-de-notificaciones-de-alerta?locale=ES_ES

5.1.10 KEEPER Gestor de Contraseñas. El gestor de contraseñas Keeper Business está creado para organizaciones de todos los tamaños, paro también puede ser usado como gestor de contraseñas personal. Cuenta con un sistema de conocimiento nulo, el cual garantiza que nadie, ni siquiera Keeper pueda acceder a la información de contraseñas almacenada por el usuario. Cifra la información antes de enviarla a la nube de keeper, la cual puede ser descifrada usando la contraseña maestra de usuario, haciendo uso de la autenticación de doble factor.

Cada usuario cuenta con un almacén cifrado privado para almacenar y gestionar contraseñas, credenciales, archivos e información confidencial. Es compatible con los controles basados en roles, el 2FA, la auditoría, los informes de eventos y el cumplimiento de la industria con HIPAA, DPA, FINRA, RGPD y más.
Compatible con plataformas Windows, Linux, MacOS y Android; admite los navegadores Chrome, Firefox, Internet Explorer, Microsoft Edge y Opera. Utiliza cifrado AES de 256 bits con PBKDF2-SHA2.

Figura 21. Dashboard keeper



Fuente: KEEPER. (2020). Gestor de contraseñas para empresas. [sitio web]. Keeper Security Inc. [consulta: 30 de mayo 2020]. Disponible en: https://www.keepersecurity.com/es_ES/business.html

5.2 RECURSOS HUMANOS

Para la correcta implementación del CSIRT, se debe establecer una estructura organizativa del personal, y una definición acertada de roles y responsabilidades asignadas a cada miembro del CSIRT, que se debe fundamentar en el tratamiento de incidentes.

Para el caso de la empresa Ciber Security de Colombia Ltda, se trata de un equipo de respuesta a incidentes distribuidos, donde se cuenta con una infraestructura distribuida a nivel nacional con sedes interconectadas a través de la mpls. Por lo tanto, debe existir un centro de respuesta integral, dividido en varios equipos, bajo la coordinación del equipo principal. Las tareas de respuesta se dividen según el área de conocimiento, según la ubicación geográfica donde se generan los incidentes o el objeto afectado.

Es esencial que el equipo coordinador, desarrolle trabajo estadístico de los incidentes para aumentar la sinergia y fomentar la colaboración entre los equipos a través del intercambio de conocimiento y lecciones aprendidas. Dicha interacción debe ser gestionada y facilitada por el equipo líder.

De acuerdo con la guía de buenas prácticas de la OEA[44], se deben tener en cuenta los siguientes elementos:

5.2.1 Roles y Responsabilidades. Se establecen los siguientes roles y responsabilidades para definir la estructura organizativa de los equipos de respuesta:

5.2.1.1 Director. Se encarga de la dirección estratégica del CSIRT, Supervisando a los equipos. Tiene a su cargo entrevistar y contratar a nuevos miembros del equipo, y asistir a reuniones con el concejo directivo de seguridad de la empresa.

5.2.1.2 Gerentes (Mandos medios). Asesora a la dirección, asume la posición de líder en las actividades diarias, asigna tareas, se encarga de autorizar los permisos de acceso a la información.

5.2.1.3 Gerente Triage. Realiza clasificación y asigna nivel de prioridad a los eventos de seguridad. Realiza asignación de los casos al personal técnico.

5.2.1.4 Gestor de incidentes. Encargado de realizar análisis de monitoreo, registro y respuesta a incidentes, coordina respuestas a incidentes, y ayuda a los equipos de respuesta a tratar los incidentes.

[44] OEA. (2016). Buenas prácticas para establecer un CSIRT nacional. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

5.2.1.5 Clasificador de eventos. Es el encargado de dar la asistencia inicial a las respuestas incidentes y clasificar la información de cada caso.

5.2.1.6 Analista / Investigador. Responsable de la investigación de casos específicos, y desarrollar nuevo material técnico para las tareas del equipo y capacitación. También realiza labores de monitoreo.

5.2.1.7 Gerente de Comunicaciones. Encargado de elaborar y socializar documentos del CSIRT, administra la página web del CSIRT, y las cuentas en redes sociales.

5.2.1.8 Administrador de red. Se encarga de administrar y gestionar la infraestructura de red del CSIRT y colabora a resolver incidentes cuando tienen que ver con la red.

5.2.1.9 Administrador de sistemas. Gestiona los sistemas de información de la plataforma CSIRT, y colabora en la respuesta a incidente cuando se necesita de sus conocimientos. Administra el acceso a la información.

5.2.1.10 Custodio de registro. Gestiona los repositorios de almacenamiento seguro de información.

5.2.2 Estructura Organizacional. El SIRT debe estar conformado por equipos de trabajo divididos por áreas y tareas específicas, a fin de integrar el cumplimiento de las funciones propias del CSIRT como: gestión de incidentes, gestión de vulnerabilidades, monitoreo del sistema, publicación de alertas y capacitación.

5.2.2.1 Dirección. La dirección del CSIRT, establece los lineamientos y el direccionamiento estratégico, establece acuerdos de trabajo con otras dependencias, es la conexión con las directivas de la empresa y actúa como vocero ante entidades de control externas y medios de comunicación.

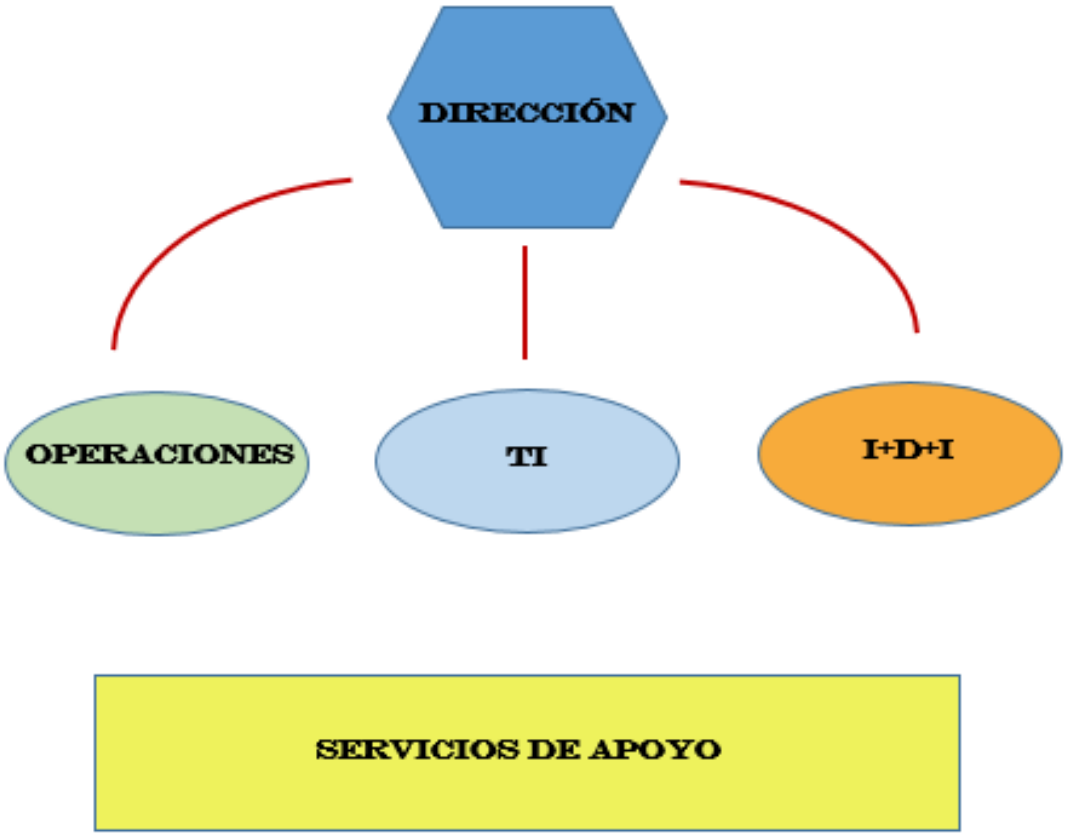
5.2.2.2 Operaciones. Son los encargados de gestionar los incidentes de seguridad. Su trabajo se tasa en la medida de que los usuarios del sistema conozcan los servicios que ofrece el CSIRT, y comiencen a enviar reportes de incidentes.

5.2.2.3 TI. El grupo de Tecnologías de Información, se encarga de administrar los sistemas y servicios como e-mail, página web, file server, gestión de casos, equipos de redes y la plataforma de seguridad del CSIRT. También proyecta el ajuste de la infraestructura y nuevas implementaciones.

5.2.2.4 Investigación desarrollo e Innovación. Es el área encargada de implementar las funciones secundarias de los equipos, tales como, desarrollo de herramientas, creación de cursos de capacitación, investigación de seguridad informática. También se encarga de la planificación, capacitación y desarrollo de cualquier nueva implementación.

5.2.2.5 Servicios de apoyo. Son dependencias que ayudan en gran parte a la ejecución correcta del CSIRT, se trata de apoyo jurídico, financiero y gestión de las comunicaciones.

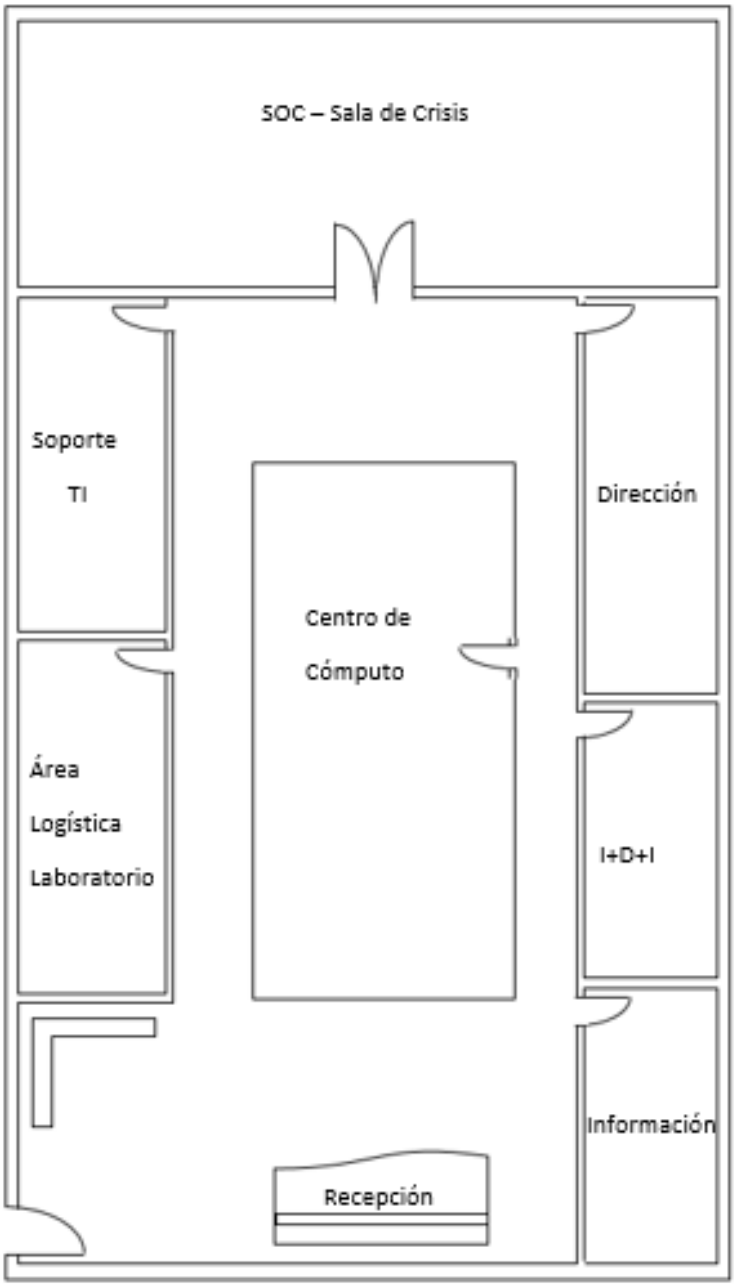
Figura 22. Diagrama Organizacional



Fuente: Propia del autor

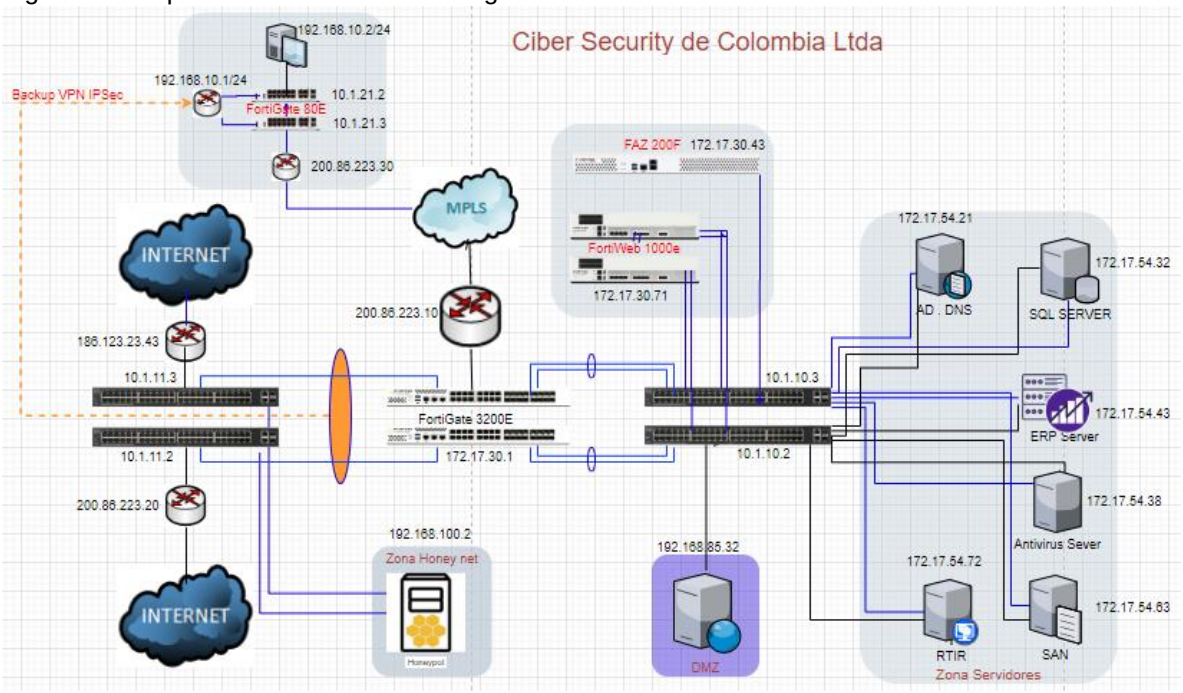
5.3 MAPA DE LA ESTRUCTURA TECNOLÓGICA

Figura 23. Plano de planta CSIRT



Fuente: Propia del autor

Figura 24. Mapa de la Estructura tecnológica



Fuente: Propia del autor

5.3.1 Inventario de equipos

Tabla 2. Inventario de equipos

DISPOSITIVO	MARCA Y MODELO	CARACTERISTICAS
SW CORE	HP Aruba 5400R[45]	Virtual Staking Baja latencia Multi Gigabit Ethernet PoE hasta 288 puertos
SW de Agregación	HP Aruba 3810	Backplane staking Baja latencia y resiliencia Multi Gigabit Ethernet PoE 48 puertos
SW Distribución	HP Aruba 2930M	Potencia Modular (hasta 1440 W) Uplinks modulares (10 – 40 GbE) Enrutamiento estático
Servidor de virtualización	DELL Poweredge R7425	Hasta 32 DIMM DDR4 Hasta 24 unidades NVMe Hasta 64 núcleos

[45] ARUBA. A Hewlet Packard Enterprise Company. Solución de Switching para campus de Aruba. Disponible en: https://www.arubanetworks.com/assets/_es/so/SB_CampusSwitching.pdf

Tabla 2. (Continuación)

DISPOSITIVO	MARCA Y MODELO	CARACTERISTICAS
Gabinete Blade	Chasis DELL Power Edge M1000e	Gabinete modular de 10u Capacidad hasta 16 blade altura media Conexiones usb (teclado,mouse) Conexión de video Controladora de administración CMC Estándar Interfaz web segura SSL y comandos Telnet/SSH SW Ethernet Modulares hasta 10 GB
Servidor DNS	Blade DELL PowerEdge M630	Procesador Intel Xeon Memoria 64 GB DDR4 2 SSD 1.8 pulgadas 10 TB c/u Windows Server 2019
Servidor DNS Replica	Blade DELL PowerEdge M630	Procesador Intel Xeon Memoria 64 GB DDR4 2 SSD 1.8 pulgadas 10 TB c/u Windows Server 2019
Storage	Dell Storage NX3230	Procesador: Intel® Xeon® E5-2609 v3 Arreglo de disco: Custom options 0,1,5,6,10,50,60 Slots: 6 (4x16 2x8)
Firewall	Fortigate 3200	Forti OS Concurrent Sessions (TCP) 50 M Políticas de Firewall: 200.000 Rendimiento VPN SSL: 8 Mbps Concurrent VPN SSL Users: 30.000 Rendimiento App Ctrl: 50 Gbps Rendimiento IPS: 26 Gbps
WAF	Fortiweb 1000E	AI-based Machine Learning Automatic profiling (white list) OWASP Top 10 API Security VM and Public Cloud Options Secured by FortiGuard
Análisis de Eventos	Fortianalyzer 200F	Advanced Threat Detection & Correlation Scalable Log Management Módulo SOC Detección de incidentes y respuesta Indicadores de Compromiso

Fuente: Propia del autor

En la implementación es de vital importancia tener en cuenta los siguientes ítem, que conforman un eje transversal del CSIRT:

5.3.2 Centro de cómputo: O Centro de procesamiento de datos, que corresponde a una adecuación física en un espacio dedicado especialmente, donde van a estar ubicados, aparte de los servidores de aplicativos misionales, core de comunicaciones, dispositivos de almacenamiento SAN, entre otros, también van a estar los equipos que componen la solución de CSIRT. Dicho espacio debe contar con las condiciones adecuadas de temperatura y humedad y con todos los controles de seguridad industrial.

El centro de cómputo debe contar con las siguientes características, de acuerdo con lo señalado por Adriana Cartagena[46], en su proyecto de grado:

5.3.2.1 Ubicación. Debe estar ubicado en un sitio en el que no tenga acceso personal no autorizado, que no ingrese aire natural y que cuente con una ruta de evacuación debidamente definida por seguridad de los administradores.

5.3.2.2 Control de acceso. El centro de cómputo debe contar con sistema de control de acceso electrónico con autenticación por controles biométricos como lector de huella e identificador facial. Además, el personal que ingresa debe ser debidamente autorizado por la dirección del CSIRT, y registrarse en la bitácora de ingreso.

5.3.2.3 Sistema de monitoreo. Debe contar con circuito cerrado de Tv, para ejercer un control del personal que ingresa al centro del cómputo y monitorear las acciones que realiza.

5.3.2.4 Aire acondicionado. Debe contar con equipamiento completo de refrigeración que garantice una temperatura de 18 grados centígrados. Funcionando de manera independiente a los demás sistemas de aire acondicionado las 24 horas del día, aun en invierno.

[46] CARTAGENA MUÑOZ, Adriana Lorena. Mejores prácticas para implementar un centro de cómputo. [En línea]. Tesis de grado. Universidad de la Sabana. Chía, 2014. [Consultado 21 de mayo de 2020]. Disponible en: https://intellectum.unisabana.edu.co/bitstream/handle/10818/11378/Adriana%20Lorena%20Cartagena%20Mu%c3%b1oz%20%20%28tesis%29.pdf?sequence=1&isAllowed=y

5.3.2.5 Sistema eléctrico. La red eléctrica debe contar con un adecuado calibre de cableado, distribución efectiva de contactos, balanceo de cargas eléctricas y una adecuada puesta a tierra, distribución por separado de los diferentes servicios que utilizan la red eléctrica como iluminación, racks, aire acondicionado y sistema contra incendios.

5.3.2.6 Sistema de control de incendios. Debe contar con detectores fotoeléctricos ubicados en el techo y el piso falso, separados el uno del otro a fin de dar alcance a cada centímetro del centro cómputo.

5.3.2.7 Fuente ininterrumpida de energía UPS. Para proteger los equipos en caso de fallas de energía eléctrica por parte del proveedor, y prevenir la pérdida de información, se debe contar con una UPS dedicada únicamente a los equipos del centro de cómputo con una capacidad mínima de 15 KVA.

5.3.2.8 Iluminación. Se debe contar con un sistema de iluminación en toda el área que facilite la administración de los equipos y la gestión de cableado en puntos de difícil acceso.

5.3.2.9 Piso falso. Se debe contar con un piso elevado de suelo a 30 cm aproximadamente, para garantizar la distribución del aire acondicionado de manera más eficiente, permitir el paso de cableado eléctrico y de datos. El cual se compone de cuadrados alineados que pueden ser removibles para tener alcance al cableado.

5.3.2.10 Segmentación de red. Es una estrategia que permite dividir las redes que forman parte de un sistema en “zonas de seguridad” o segmentos separados por cortafuegos. Cuando se configura correctamente; los segmentos separan las aplicaciones y evitan el acceso a los datos confidenciales.

Tabla 3. Segmentación de red

Vlan	***Interfaz***	Máscara	***Gateway***
Vlan 1 Equipos de red	10.1.10.0	255.255.255.240	10.1.10.1
Vlan 2 Zona Servidores	172.17.54.0	255.255.255.240	172.17.54.1
Vlan 3 DMZ	172.17.56.0	255.255.255.248	172.17.56.1
Vlan 4 Telefonía IP	172.17.42.0	255.255.255.192	172.17.42.1
Vlan 5 CCTV	172.17.53.0	255.255.255.192	172.17.53.1

Tabla 3. (Continuación)

Vlan 6 Equipos de seguridad	10.1.30.0	255.255.255.248	10.1.30.1
Vlan 7 Zona Usuarios	172.17.101.0	255.255.255.128	172.17.101.1
Vlan 10 MPLS	192.168.10.0	255.255.255.240	192.168.10.3
Vlan 13 Honeynet	192.168.200.0	255.255.255.240	192.168.200.1

Fuente: Propia del autor

5.3.3 Equipo I+D+I. El equipo de Investigación, desarrollo e innovación, estará asignado al grupo de Proyección de la oficina de sistemas de la compañía, serán los encargados de realizar estudios y análisis de las nuevas técnicas y tecnologías de la información, y presentarán proyectos a la alta dirección, relacionados con: seguridad, analítica, inteligencia artificial, machine learning, robótica, block chain, y otras temáticas, que permitirán a Cyber security de Colombia Ltda. , estar a la vanguardia de las grandes compañías multinacionales en cuanto al uso de tecnologías modernas.

Figura 26. Proceso I+D+I

Fuente: SANDE, José. 2010. I+D+I y el triángulo del conocimiento. Compartiendo conocimiento. [Consulta 22 de mayo 2020]. Disponible en: https://josesande.com/2010/02/19/tema-7-i-d-i-y-el-triangulo-del-conocimiento/

5.3.4 Sala de crisis: Salón o centro de monitoreo, donde a través de las herramientas graficas que proporcionan los equipos de seguridad, se realiza un seguimiento y análisis de los eventos que van ocurriendo, para dar respuesta oportuna a la amenaza.

La sala de crisis permite centralizar la información de alguna emergencia o incidente grave y de allí planificar y ejecutar respuesta o proponer acciones a tomar para actuar de forma oportuna para contrarrestar el incidente.

5.3.5 Centro de Operaciones: El centro de Operaciones SOC, por sus siglas en inglés (Security Operation Center), Es un lugar con múltiples pantallas, donde se visualiza, de manera automática los eventos de la infraestructura tecnológica, sistema de información, aplicativos, base de datos y demás, gracias a entornos gráficos y reportes personalizados de eventos, a través del uso de herramientas como, Sandbox, Siem, DDoS, Analizer, que nos permiten ejecutar archivos y url en un ambiente virtual controlado, realizar correlación de eventos de seguridad de acuerdo a los dispositivos de la empresa, determinar los niveles o topes de tráfico permitido en la red, y realizar análisis de logs en tiempo real.

El SOC ejecuta tareas las 24 horas del día, los siete días de la semana, para combatir las amenazas cibernéticas avanzadas, mediante procesos y procedimientos establecidos, documentando y registrando los incidentes en herramientas de SGSI, y generando las alertas a los responsables de la gestión de los eventos, y aportando la información necesaria en caso de requerirse una investigación forense.

El Centro de Operaciones de Seguridad, es fundamental en la adecuada implementación del Sistema de Gestión de Seguridad de la Información, sirviendo como herramienta de ayuda en los pasos del ciclo PHVA del SGSI, traducido del inglés PDCA (Plan, Do, Check, Act).

En el centro de operaciones se debe contar con una solución de Firewall completa que permita gestionar y monitorear los incidentes en tiempo real, para lo cual se propone utilizar una solución de Fortinet, la cual consta de los siguientes equipos:

- Fortigate 3200. Máquina que funciona como firewall principal, con capacidad para gestionar el control de accesos a nuestra red desde el exterior,

administra las interfaces y objetos de la red del CSIRT, incluye gestión de políticas en esquema de par de interfaces que hace más intuitivo y compacta la administración del mismo, puede controlar filtrado de contenido web a través de su módulo de web filter. Esta máquina se utiliza con redundancia para impedir perdidas de conexión en caso de que el principal llegara a fallar.

- Fortiweb. Dispositivo creado para dar seguridad a aplicaciones web, el brinda una protección de OWASP, previene intrusiones, identifica vulnerabilidades de seguridad de las aplicaciones.
- FortiSIEM. Correlacionador de eventos e incidentes de seguridad. Permite automatizar procesos de TI, y agiliza la respuesta del equipo ante cualquier evento.
- FortiDDoS. Herramienta que protege frente a ataques de denegación de servicio. Monitorea infinidad de parámetros al mismo tiempo.
- FortiSandbox. Máquina que posee un entorno de pruebas virtualizado, la cual cuenta con diferentes máquinas virtuales que se pueden configurar en las diferentes versiones de Windows, Linux, Mac, Android. Donde se ejecutan archivos sospechosos en un ambiente controlado.
-

Figura 25. Ciclo PHVA

Fuente: TORRUELA, Jordi. (2017). Conocimientos Fundamentales en Ciberseguridad. Asociación Nacional De Ciberseguridad. [Consulta 22 de mayo 2020] Disponible en: http://www.ancibe.com/documents/GuiaCCFC.pdf

5.4 SERVICIOS DEL CSIRT

5.4.1 Categorías de los servicios. Para efectos de contrarrestar el impacto de los incidentes de seguridad que se presenten en la empresa, el CSIRT está en la capacidad de proporcionar los siguientes servicios de acuerdo a su categoría:

5.4.1.1 Servicios Reactivos.

- Alertas y advertencias
- Tratamiento de incidentes
    - Análisis de Incidentes
    - Respuesta a Incidentes en sitio
    - Apoyo en la respuesta a incidentes
    - Coordinación de la respuesta a incidentes

- Manejo de Vulnerabilidades
    - Análisis de vulnerabilidad
    - Respuesta a vulnerabilidad
    - Coordinación en la respuesta a vulnerabilidad

- Manejo de Instancias
    - Análisis de instancias
    - Respuesta de instancias
    - Coordinación respuesta de instancias

5.4.1.2 Servicios Proactivos.

- Comunicados
- Observatorio de tecnología
- Evaluaciones o auditorias de seguridad
- Configuración y mantenimiento de herramientas de seguridad
- Desarrollo de herramientas de seguridad
- Servicio de detección de intrusiones
- Difusión de información relacionada con seguridad

5.4.1.3 Servicios de Gestión de calidad de la Seguridad.

- Análisis de Riesgos
- Plan de continuidad del negocio y recuperación de desastres
- Consultoría de seguridad

- Sensibilización
- Educación /Formación
- Evaluación o certificación del producto

5.4.2 Descripción de los servicios.

5.4.2.1 Servicios Reactivos Son aquellos que se realizan debido la detección de un evento de seguridad inesperado o por solicitud de algún miembro de la empresa que haya identificado alguna falla en la red de datos o sistemas de información. Estos servicios son el pilar fundamental de los CSIRT y tienen estrecha relación con los planes de gestión de seguridad o SGSI.

- Alertas y advertencias: Tiene como objeto la difusión detallada de ataques y otras alertas de seguridad como detección de intrusos, virus, entre otros. Y proporciona acciones a tomar a corto plazo para contrarrestar el problema detectado. Las notificaciones de alerta se difunden en reacción al incidente que se presenta y orienta a los usuarios o administradores de los servicios afectados, con información para proteger el sistema.

Tabla 4. Ranking de alertas Recibidas CSIRT-CL

Ranking de Alertas Recibidas			
Noviembre 2019	**Diciembre 2019**	**Tendencia**	**Cambio en el Ranking**
1.Vulnerabilidad	1.Recopilación de Información	▲	↑
2.Operaciones Ciberseguridad CSIRT	2.Código Malicioso	▲	↑
3.Código Malicioso	3.Vulnerabilidad	▼	↓
4.Fraude	4.Operaciones Ciberseguridad CSIRT	▼	↓
5.Intrusión	5.Fraude	▲	↓
6.Intentos de Intrusión	6.Información de Seguridad de Contenidos	▲	↑
7.Disponibilidad	7.Disponibilidad	▲	→
8.Información de Seguridad de Contenidos	8.Intentos de Intrusión	▼	↓
9.Contenido Abusivo	9.Contenido Abusivo	▲	→
9.Recopilación de Información	10.Intrusión	▼	↓
Simbología			
Tendencia: ▼ Disminuye ; ▶ Constante ; ▲ Aumenta			
Ranking: ↓ Baja; → Igual; ↑Sube			

Fuente: CSIRT-CL. (2020). Informe de seguridad Gestión CSIRT. Equipo de Respuesta ante Incidentes de seguridad Informática. Santiago, Chile. [Consulta 29 de mayo 2020]. Disponible en: https://www.csirt.gob.cl/media/2020/01/14IMT20-00018-01.pdf

- Tratamiento de incidentes: Se fundamenta en recibir reportes o solicitudes de eventos de seguridad, realizar un análisis y emitir una respuesta de acción, dentro de las que se encuentran las siguientes:
    - Tomar acciones para proteger sistemas atacados por intrusos
    - Proveer soluciones y estrategias de mitigación por medio de avisos

- Vigilar actividad de intrusos en el sistema
- Filtrar tráfico de red
- Reparación de sistemas
- Estrategias alternas de respuesta

- Manejo de Vulnerabilidades: Su función es recibir información acerca de vulnerabilidades de hardware y software. Realizar un análisis de sus características y emitir estrategias y medidas que permitan detectarlas a tiempo y contrarrestarlas.

- Manejo de Instancias: Una instancia es un objeto o archivo malicioso ubicado en el sistema, que tiene como tarea, recolectar información de la red, realizar ataques, o vulnerar los controles de seguridad. Dentro de los cuales se puede enumerar los virus, troyanos, gusanos, exploits, entre otros. Este servicio recibe información detallada de ataques anteriores que incluyen copias de las instancias, para realizar un estudio de su naturaleza, alcance y otras características, a fin de proponer estrategias de mitigación o eliminación, y hasta prevenir que se creen o multipliquen, haciendo uso de la creación de nuevas firmas que se pueden agregar al antivirus o el servicio de detección de intrusos IDS.

5.4.2.2 Servicios Proactivos. Fueron creados para entregar información que ayude a proteger la infraestructura tecnológica y optimizar los procesos de seguridad. Su objetivo principal es evitar ataques o incidentes. Dentro de sus tareas, se incluyen las auditorías y la verificación del correcto uso y mantenimiento de las herramientas de seguridad.

- Comunicados: Sirven para informar a los usuarios de las nuevas vulnerabilidades y técnicas de intrusión detectadas, por medio de alertas, y notificaciones. Esto con el fin de proteger los sistemas de información de los nuevos riesgos de seguridad antes de que se materialicen.

- Observatorio de tecnología: Consiste en la investigación y supervisión de actividades de intrusos y modernos métodos de identificación de amenazas. Lo cual permite integrar elementos legislativos, incidentes sociales o políticos con nuevas tecnologías, mediante la recopilación de información orientada a la seguridad de los sistemas y redes de datos. Dicha información se extrae de sitios web de seguridad informática, noticias y títulos periodísticos de índole científica y tecnológica. Una vez analizada la información recolectada se emite un comunicado son recomendaciones en cuanto a seguridad para aplicar a mediano o largo plazo.

- Evaluaciones o auditorias de seguridad: Se enfoca en el estudio de la estructura de seguridad de una organización, con fundamento en los requisitos exigidos por la misma organización o los determinados por las normas internacionales. Pasando por revisiones de las políticas de seguridad, verificación de la infraestructura física y lógica, revisión de buenas prácticas, pruebas de penetración, entre otras.

- Configuración y mantenimiento de herramientas de seguridad: Se relaciona detalladamente la guía para mantener una adecuada configuración de aplicativos y herramientas en general del CSIRT. Aunado a esto, el CSIRT puede actualizar o modificar la configuración y realizar el mantenimiento de herramientas de seguridad, servicios IDS, escaneo de red, firewall, redes privadas virtuales, y sistemas de autenticación. Por otro lado, también puede intervenir la configuración de servidores, computadoras, dispositivos inalámbricos, entre otros, de acuerdo las necesidades y dentro del marco de los lineamientos de seguridad.

- Desarrollo de herramientas de seguridad: Este servicio incluye la creación de nuevas herramientas para el mismo CSIRT, que contribuyan a reducir los riegos de seguridad, corregir las fallas actuales de las herramientas de software, y optimizar las que se encuentran en funcionamiento.

- Servicio de detección de intrusiones: Consiste en la supervisión de los registros que arrojan los sistemas de detección de intrusos de la empresa, lo cual incluye una ardua tarea con el análisis de una gran cantidad de datos que son capturados cada segundo. Lo cual requiere de herramientas y conocimientos especializados para poder interpretar el gran volumen de información, con el fin de identificar ataques o eventos de seguridad que pueden ser falsos positivos, para finalmente aplicar estrategias de respuesta.

- Difusión de información relacionada con seguridad: Se trata de la socialización de información fácil de asimilar, pero a la vez útil para mejorar la seguridad de la empresa. Las difusiones pueden ser creadas por el CSIRT, el grupo de administración TI o el grupo de comunicaciones, las cuales pueden incluir información de fuentes externas y que se pueden presentar en forma de directrices de comunicación, archivos de alertas, documentos de mejores prácticas, políticas y procedimientos, actualizaciones, estadísticas y tendencias, entre otros.

5.4.2.3 Servicios de Gestión de calidad de la Seguridad. Se trata de los servicios creados para el mejoramiento continuo de la seguridad de la organización. Donde se tienen en cuenta las lecciones aprendidas que deja la experiencia del manejo de eventos de seguridad, ataques y vulnerabilidades, con lo cual se busca mejorar la capacidad de respuesta de la organización a largo plazo. En articulo CSIRT Services, The Carnegie Mellon University[47], lista y describe los servicios que puede prestar un CSIRT:

- Análisis de riesgos: Los CSIRT puede contribuir a las evaluaciones y análisis de riesgos del SGSI de la empresa, optimizando la capacidad de la organización para evaluar amenazas reales mediante el uso de valoraciones cuantitativas y cualitativas reales de los riesgos.

- Plan de continuidad del negocio y recuperación de desastres: Este servicio contribuye en el plan de continuidad del negocio y recuperación en caso de desastres, en eventos relacionados con amenazas y riesgos de seguridad informática.

- Consultoría de seguridad: Hace referencia a la asesoría acerca de mejores prácticas de seguridad, donde el CSIRT actúa de forma directa, en la entrega de recomendaciones, identificación de requisitos de compra, implementación de nuevos sistemas como dispositivos, herramientas de software, o procedimientos comerciales.

- Sensibilización: Se encarga de la concientización de los usuarios sobre la importancia de la seguridad informática en sus labores diarias, con el objetivo de reducir la cantidad de ataques exitosos, y que los mismos usuarios puedan detectar los ataques. Esta sensibilización se realiza a través de boletines de seguridad, posters, wallpapers y otros medios presenciales como reuniones o foros grupales.

- Educación / Formación: este servicio provee a los usuarios información útil respecto a seguridad informática, incluyendo trasferencias de conocimiento a través de seminarios y tutoriales, donde se abordan temas como procedimientos de comunicación de incidentes, procesos de respuesta adecuados, herramientas disponibles para tratamiento de incidentes, entre otros.

[47] CARNEGIE MELLON UNIVERSITY. (2014). Software Engineering Institute. CSIRT Services. Disponible en: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

- Evaluación o certificación del producto: El CSIRT brinda el servicio de evaluar herramientas y aplicativos con el fin de garantizar la seguridad de los productos y el cumplimiento de los requisitos en materia de seguridad de la empresa.

6 RESULTADOS Y DISCUSIÓN

6.1 RESULTADOS

En este apartado se describen los resultados de la elaboración de la documentación técnica de un CSIRT para la empresa Cyber Security de Colombia Ltda. A través de los diferentes procesos propuestos en este documento así:

- Recolección de información relacionada con herramientas de software que permiten ejecutar actividades de CSIRT.
  Indicador: Informe de investigación herramientas de software
  Beneficiario: Cyber security de Colombia Ltda.
  - Listado de herramientas
  - Descripción de herramientas
  - Justificación del uso de las herramientas

- Establecimiento de la estructura organizacional y jerarquía, respecto del área de Recursos Humanos, relacionando el personal que conforma el CSIRT.
  Indicador: Estructura Organizacional definida
  Beneficiario: Cyber Security de Colombia Ltda.
  - Definición de cargos
  - Asignación de Roles y responsabilidades
  - Elaboración de la estructura organizacional

- Diseño del mapa de la infraestructura tecnológica de la empresa, incluyendo las nuevas herramientas de CSIRT.
  Indicador: Diagrama de red lógico de la infraestructura tecnológica
  Beneficiario: Cyber security de Colombia Ltda.
  - Levantamientos de activos de información de la empresa (servidores, equipos y servicios)
  - Identificación de riesgos y malas prácticas en la ubicación de equipos y distribución de red.
  - Elaboración de propuesta de nuevo diseño de arquitectura de red incluyendo las nuevas herramientas de CSIRT.

- Listado y descripción de los servicios de CSIRT a favor de la empresa Ciber Security de Colombia Ltda.
  Indicador: Relación detallada de los servicios de CSIRT
  Beneficiario: Cyber security de Colombia Ltda.
  - Listado de servicios de CSIRT según su categoría (reactivos y proactivos)
  - Descripción detallada de los servicios de CSIRT
  - Alcance de la ejecución de los servicios

6.2 DISCUSIÓN

Una vez se determina la necesidad de una solución de respuesta y tratamiento de incidentes de seguridad informática, y se establece la importancia y las ventajas que conlleva la implementación de un CSIRT, a través de la investigación y compilación de antecedentes de dichos equipos de respuesta a nivel mundial, con evidencia de resultados positivos en el manejo de incidentes, donde se comparte conocimientos e información para establecer un trabajo conjunto en la lucha contra la ciber delincuencia. Se procede a desarrollar los objetivos propuestos para la implementación, elaborando la documentación técnica necesaria, de todos y cada uno de los componentes necesarios del CSIRT.

Gracias a los esfuerzos de organizaciones internacionales, con el apoyo de instituciones descentralizadas y países preocupados por la seguridad de la información, se han elaborado diversas disposiciones de carácter legal y tecnológico, que han impulsado lo que hoy se conoce como equipos de respuesta a incidentes de seguridad informática. Los cuales han venido evolucionando con el paso del tiempo y el incremento de amenazas y nuevas técnicas de ataques a los sistemas de información, que exigen a los administradores TI y responsables de la seguridad, la creación y desarrollo de nuevas y modernas herramientas que permitan mitigar el riesgo y reducir el impacto en los activos de información.

Los equipos de respuesta a incidentes de seguridad informática, se constituyen como una de las opciones más viables para combatir los ataques y para reducir el impacto de los mismos en los activos de información. Que no solo atiende incidentes de seguridad propios, si no que permite la colaboración con otros CSIRT para unir esfuerzos y compartir casos solucionados, experiencias y conocimientos en un entorno de confianza.

Se identifican y reconoce que la legislatura colombiana, respecto a temas de delitos informáticos, cuenta con bases jurídico –penales que dotan a los organismos judiciales de un instrumento adecuado para proteger el bien jurídico de la información, mediante la ley 1273 de 2009, y adopción de directrices de legislaciones europeas como el tratado de Budapest. No obstante, el estado debe invertir más recursos en el fortalecimiento del aparato judicial, capacitación a fiscales e investigadores de policía judicial y dotación de tecnología necesaria a la fuerza pública con el fin de combatir y mitigar este flagelo de la ciberdelincuencia.

CONCLUSIONES

De acuerdo a lo abordado en este documento, podemos concluir, que la adecuada implementación de un CSIRT, requiere herramientas de hardware y software, que cuenten con características como: modernidad, eligiendo las versiones más vigentes y estables de cada una; Compatibilidad, que permita la adaptación a la infraestructura de red de la empresa y que pueda convivir con las diferentes versiones de sistemas operativos; versión libre, en lo posible herramientas open source que permitan modificar algunas características para una mejor adaptación a las necesidades de la organización, además de reducir costos en la compra de licencias y soporte continuo.

De igual forma, se logró establecer dentro de la plataforma tecnológica del CSIRT, 7 herramientas que proporcionan servicios proactivos así: una herramienta de cifrado y firmas digitales (GNU PG), una Honeynet, un instrumento de monitoreo de páginas web (WhatchThatPage), Listas de Control de Acceso (ACL), un gestor de contraseñas (Keeper), un firewall de aplicaciones web (Fortiweb), un entorno aislado de pruebas (FortiSandbox). Y 5 herramientas que proveen servicios reactivos: un administrador de incidentes (RITR), un sistema de detección de intrusos (Snort), un detector de amenazas en puntos finales (EDR Symantec), un correlacionador de eventos de seguridad (FORTISIEM).

Para establecer una correcta administración de los recursos humanos, se hizo necesario, el diseño de una jerarquía de cargos con sus respectivos roles y responsabilidades, con el fin de garantizar un óptimo desempeño en el cumplimiento de los objetivos y el desarrollo de las funciones, permitiendo un flujo apropiado de todos los procesos, a través de determinados niveles jerárquicos, que se encuentran interrelacionados entre sí, formando una sinergia que establece canales de comunicación, líneas de autoridad, supervisión y auditoria. La cual, cuenta con tres niveles: nivel directivo (Dirección); nivel operativo con tres elementos (Operaciones, Administración TI, I+D+I); y el nivel de servicios de apoyo (Jurídico, Financiero y Comunicaciones). Creando así un modelo organizacional, dentro del cual todos los miembros confluyen en el cumplimiento de la misión del CSIRT.

Respecto a los requerimientos de infraestructura tecnológica podemos concluir, que, para la correcta utilización de las diferentes herramientas y soluciones planteadas, se requiere un esquema que cuente con un diseño arquitectónico de la ubicación de los espacios asignados a las diferentes dependencias y/o grupos de trabajo, detallando las características particulares y su función dentro del CSIRT.

En consecuencia, de lo mencionado anteriormente, es posible indicar, que el diseño y estructura de la red de datos, debe adoptar estándares y protocolos que no se queden solo en monitoreo de tráfico y detección de errores, sino que implemente servicios heterogéneos que busquen un control eficaz de la red, para que pueda responder a las necesidades del CSIRT. De igual forma, es necesario incluir de manera asertiva, modernas herramientas de seguridad de la información sin que haya problemas de compatibilidad o conflicto con otros servicios, para lo cual se estableció una segmentación de red con 9 diferentes vlan, que garantizan la protección de cada segmento en caso de un ataque positivo a alguno de los servicios, para que no afecte la totalidad de la infraestructura.

El análisis expuesto, nos indica, que la gestión adecuada de las redes de datos juega un papel muy importante dentro del pilar de la seguridad de la información, puesto que abarca políticas y procedimientos previamente establecidos, orientados a reforzar la seguridad del CSIRT. Así mismo, se logró identificar, que una correcta administración de la red debe garantizar la disponibilidad de los servicios a todos sus usuarios, por lo que se implementaron canales de respaldo en cuanto a conexión a internet como dentro de la red Lan. De esta forma se implementaron equipos y servidores en HA, que garantizan la continuidad del negocio en casos de desastres o cualquier otro evento de seguridad. Para el caso, se cuenta con 5 equipos en alta disponibilidad: firewall principal, servidor de aplicaciones web, switch core, almacenamiento y controlador de dominio.

En última instancia, se pudo concluir, que uno de factores más importantes a la hora de plantear la implementación del CSIRT, es determinar los servicios que va a prestar, puesto que una adecuada elección, definición y administración de los mismos, es fundamental en la tarea de mitigar y prevenir incidentes de seguridad. La elección y administración se realizó de acuerdo a las necesidades del CSIRT, determinadas en un análisis previo del estado actual, las capacidades de respuesta y las herramientas con las que cuenta.

Finalmente, y de acuerdo a la necesidad de establecer los servicios que puede prestar el CSIRT. Se determinó la importancia de la inclusión de servicios reactivos y proactivos, los cuales hacen parte de un conjunto de medios y medidas de seguridad, cada uno con un papel muy importante, donde se establecieron 7 diferentes tipos de servicios proactivos, que responden ante un evento o notifican la detección de intrusos; 4 tipos de servicios reactivos que ofrecen asistencia e información para prevenir o proteger los sistemas de información de eventos que pueden llegar a ocurrir; y 6 tipos de servicios de gestión de calidad, orientados al mejoramiento continuo de la misión del CSIRT.

RECOMENDACIONES

Establecer políticas formales para salvaguardar la información de manera más ordenada para la ejecución de procedimientos.
Definir y aplicar los controles de seguridad en un entorno real, buscando mejorar las condiciones de seguridad según lo dispuesto en este documento.
Crear un centro de mando o puesto de control desde donde se pueda administrar de forma adecuada los servicios y procesos del CSIRT.
Establecer una guía que permita optimizar y agilizar los procesos del CSIRT, con el objeto de encontrar de manera más rápida y oportuna los incidentes de seguridad de la empresa.
Implementar el uso de métricas.

BIBLIOGRAFÍA

APCERT. Asia Pacific Computer Emergency Response Team. [sitio web]. Supporting the Internet Security in Asia Pacific. [consulta 27 de mayo de 2020]. Disponible en: https://www.apcert.org/about/mission/index.html

BEST PRACTICAL. Request Tracker for Incident Response (RTIR). Disponible en: https://bestpractical.com/rtir/

BISCHOFF, Paul. (2020). ¿Qué países tienen la peor (y mejor) ciberseguridad? Comparitech. Disponible en: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

CARNEGIE MELLON UNIVERSITY. (2014). Software Engineering Institute. CSIRT Services. Disponible en: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf

CAROZO B., Eduardo. Centro de respuesta a incidentes informáticos... ¿Para qué? En Revista Seguridad cultura de prevención para ti. Vol 16. (Ago 2018). Disponible en: https://revista.seguridad.unam.mx/numero-16/centro-de-respuesta-incidentes-informáticos-para-qué

COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. (2019). Resolución 93 de 2019. “Por la cual se delegan unas funciones, se conforman unos comités y se dictan otras disposiciones” Disponible en: http://legal.legis.com.co/document/Index?obra=legcol&document=legcol_6069d1a9118047e6a0c0e0050ac80965

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). Conpes 3854. Política Nacional de Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (2009). Ley 1273 de 2009. Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

------ ------. (2011). CONPES 3701 de 2011. Lineamientos de política para la Ciberseguridad y Ciberdefensa. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

CSIRT-CL. (2020). Informe de seguridad Gestión CSIRT. Equipo de Respuesta ante Incidentes de seguridad Informática. Santiago, Chile. [Consulta 29 de mayo 2020]. Disponible en: https://www.csirt.gob.cl/media/2020/01/14IMT20-00018-01.pdf

CSIRT Financiero. Aso bancaria. CSIRT Financiero un enfoque colaborativo a la Ciberseguridad. Disponible en: https://www.asobancaria.com/csirt/

CSIRT PONAL. Policía Nacional. Oficina de Telemática. Disponible en: https://cc-csirt.policia.gov.co/quienes-somos

DARPA. Defense Advanced Research Proyects Agency. Disponible en: https://www.darpa.mil/our-research

DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. (Colombia). (2019). Lineamiento para gestión de incidentes y Vulnerabilidades de seguridad de la información. Disponible en: https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/L-TI-26-Gestion-Incidentes-Vulnerabilidades.pdf

DIRECTIVA (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, sobre medidas para un alto nivel común de seguridad de redes y sistemas de información en toda la Unión. Disponible en: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

ECURED. Gusanos Informáticos. Enciclopedia colaborativa en red del gobierno de Cuba [Consulta: 24 de Octubre 2020]. Disponible en: https://www.ecured.cu/Gusano_(inform%C3%A1tica)

------ ------. Snort. Enciclopedia colaborativa en red del gobierno de Cuba. Disponible en: https://www.ecured.cu/Snort

ENISA. Agencia de la Unión Europea para la seguridad Cibernética. (2019). CSIRT en Europa. Disponible en: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

------ ------. (2019). Como crear un CSIRT paso a paso. Disponible en:

https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

FALCONE, Kevin. Request Tracker for Incident Response (RTIR). Best Practical. [Cosulta 14 de junio 2020]. Disponible en: https://www.terena.org/activities/tf-csirt/meeting38/falcone-rtir.pdf

FERNANDEZ, Lorena. (2020). Redes Zone. Qué son los Advanced Persistent Threats y cómo protegernos de los APT. [consulta 30 de mayo 2020] Disponible en: https://www.redeszone.net/tutoriales/seguridad/advanced-persistent-threats-apt-protegernos/

FIRST IMPROVE SECURITY TOGETHER. [sitio web]Foro Global de Respuesta a Incidentes y Equipos de Seguridad. [Consulta 27 de mayo 2020]. Disponible en: https://www.first.org/

FRANCO, José Pastor; SARASA LÓPEZ, Miguel Ángel y SALAZAR RIAÑO, José Luis. Criptografía Digital: Fundamentos y aplicaciones. Editorial Zaragoza. (2001). Disponible en: https://www.casadellibro.com/libro-criptografia-digital-fundamentos-y-aplicaciones-2-ed/9788477335580/798279

GARCÍA, R. D. M. (2009). Criptografía clásica y moderna. España: Septem Ediciones. P. 14 Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/102985

GNUPG. El GNU Privacy Guard. implementación completa y gratuita del estándar OpenPGP. Disponible en
https://www.gnupg.org/

GUOAN, Xiao. (2018). Una guía práctica para GPG - Parte 1 Genere su par de claves. Linuxbabe. [Consulta: 14 de junio 2020]. Disponible en:
https://www.linuxbabe.com/security/a-practical-guide-to-gpg-part-1-generate-your-keypair

INTERNATIONAL TELECOMUNICATION UNION. [Sitio web]. Individuals using the internet, 2005 – 2019. Naciones Unidas. [Consulta: 24 de Octubre 2020]. Disponible en: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

------ ------. (2019). The Global Cybersecurity Index. Geneva, Swtzerland. Disponible en:
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

IMPERVA. (2020). [sitio web]Amenaza Persistente Avanzada (APT). [Consulta: 30 de mayo 2020]. Disponible en: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

JURISCOL. (2013). Sistema Único de Información Normativa. Decreto 1377 de 2013. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081

KALI, By Offensive Security. (2020). About Kali Linux. Disponible en: https://www.kali.org/about-us/

KASPERSKY. (2020). Secure List. Desarrollo de las amenazas informáticas en el primer trimestre de 2020 Estadísticas. [Consulta 29 de mayo de 2020] Disponible en: https://securelist.lat/it-threat-evolution-q1-2020-statistics/90344/

------ ------. (2020). 5 Warning Signs of Advanced Persistent Threat and How to Prevent Advanced Persistent Threats. The Advanced Threat Lifecycle. [Consulta: 30 de mayo 2020]. Disponible en: https://www.kaspersky.com/resource-center/threats/advanced-persistent-threat

KEEPER. (2020). Gestor de contraseñas para empresas. [sitio web]. Keeper Security Inc. [consulta: 30 de mayo 2020]. Disponible en: https://www.keepersecurity.com/es_ES/business.html

LACNIC. (2012). Gestión de Incidentes de Seguridad Informática. Registro de Direcciones de Internet para América Latina y el Caribe. Proyecto AMPARO. [Consulta 29 de mayo 2020]. Disponible en: https://warp.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

MELENDEZ CAMPIS, Camilo Andrés y TOUS TEJADA, Jesús Andrés. Listas de Control de Acceso (ACL) y Control de Acceso Basado en el Contexto (CBAC). [En línea]. Trabajo de grado. Universidad Tecnológica de Bolívar. Cartagena, 2012. [Consultado 29 de mayo 2020]. Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0063288.pdf

MENDOZA, Miguel Angel. (2015). Welivesecurity by ESET. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?. Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

MOIRA West Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. Handbook for computer security incident response teams (csirts). Technical report, Software Engineering Institute, Carnegie Mellon University, 2003. Disponible en: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

MUÑOZ, Mirna, RIVAS, Lizbeth. Estado actual de equipos de respuesta a incidentes de seguridad informática. {en línea}. 7 marzo de 2015. {18 de noviembre de 2019} Disponible en: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952015000100002

MURQUINCHO PUMA, Diego Eduardo. Área de la energía las industrias y los recursos no renovables. [en línea] Seguridad Informática, Universidad de Loja Ecuador. [Consultado 29 de mayo 2020]. Disponible en: https://www.studocu.com/ec/document/universidad-nacional-de-loja/seguridad-de-la-informacion/resumenes/csirts-latinoamerica/3781244/view

NETGATE DOCS. Alertas de Snort. IDS/IPS Snort. [Consulta 14 de junio 2020]. Disponible en: https://docs.netgate.com/pfsense/en/latest/ids-ips/snort-alerts.html

OFICINA DE SEGURIDAD DE LA INFORMACIÓN. (2018). Appalachian State University. Equipo de respuesta a Incidentes de Seguridad Informática. Disponible en: https://security.appstate.edu/about-us/asu-csirt

OPENPGP INC. (2007). RFC 4880. Disponible en: https://tools.ietf.org/html/rfc4880

PRESIDENCIA DE LA REPUBLICA DE COLOMBIA. (2018). Ley 1928 del 24 de julio de 2018. Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação. [En línea]. Porto: Estado actual de equipos de respuesta a incidentes de seguridad informática. 2015 [Fecha de consulta 18 de noviembre de 2019]. Disponible en: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952015000100002

SANDE, José. 2010. I+D+I y el triángulo del conocimiento. Compartiendo conocimiento. [Consulta 22 de mayo 2020]. Disponible en: https://josesande.com/2010/02/19/tema-7-i-d-i-y-el-triangulo-del-conocimiento/

SECURE & IT. [sitio web]. CSIRT – Equipo de Respuesta a incidentes de seguridad. [Consulta: 12 de junio 2020]. Disponible en: https://www.secureit.es/csirt/#

SEGU INFO. 2020. Detección de Intrusos en tiempo Real. Noticias sobre seguridad de la información. [Consultado 20 de mayo 2020]. Disponible en: https://www.segu-info.com.ar/proteccion/deteccion

SYMANTEC. A división of broadcom. Configuración de notificaciones de alerta. [Archivo de video]. 2017. 1.9 min. Disponible en: https://help.symantec.com/cs/SEPC/SEPC/v109630219_v101064224/Configuraci%C3%B3n-de-notificaciones-de-alerta?locale=ES_ES

------ ------. (2020). [Sitio web]. Detección de punto final y respuesta. [Consulta: 30 de mayo 2020]. Disponible en: https://help.symantec.com/bucket/saep/edr?locale=EN_US

------ ------. Donde colocar el appliance en su red para obtener mejores resultados. Symantec EDR 4.0. [Consulta:14 de junio 2020]. Disponible en: https://help.symantec.com/cs/SYMANTECEDR_4.0/EDR/v97213073_v128933990/D%C3%B3nde-colocar-el-appliance-en-su-red-para-obtener-mejores-resultados%7CSymantec-EDR?locale=ES_MX

------ ------. Trabajar en la vista de Resumen de eventos. Symantec EDR 4.0. [Consulta:14 de junio 2020]. Disponible en: https://help.symantec.com/cs/SYMANTECEDR_4.0/EDR/v121261470_v128933990/Trabajar-en-la-vista-Events-Summary-(Resumen-de-eventos)?locale=ES_MX

TECNOLOGÍA. Así está Colombia en el ranking de ciberseguridad mundial. En revista Semana. (13 de febrero de 2019). Disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

THE HONEYNET PROJECT. (2019). Honeywall CDROM. Disponible en: https://www.honeynet.org/projects/old/honeywall-cdrom/

------ ------. (2019). Página principal de Sebek. [Consulta: 29 de mayo 2020]. Disponible en: http://his.sourceforge.net/honeynet/tools/sebek/

------ ------. (2019). Sobre nosotros. [Consulta: 29 de mayo 2020]. Disponible en: https://www.honeynet.org/about/

THE LINUX FUNDATION PROJECTS. (2020) DENT Un NOS para todos los demás. Disponible en: https://dent.dev/

TORRUELA, Jordi. (2017). Conocimientos Fundamentales en Ciberseguridad. Asociación Nacional De Ciberseguridad. [Consulta 22 de mayo 2020] Disponible en: http://www.ancibe.com/documents/GuiaCCFC.pdf

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO. (2018). Estadísticas. Incidentes por tipo en 2017. Disponible en: https://www.seguridad.unam.mx/estadisticas

VALHALLA Honeypot - Honeypot de código abierto gratuito para el sistema Windows Disponible en: http://valhalahoneypot.sourceforge.net/

VMWARE DOCS. Documentación de vMware vSphere. [Consulta: 14 de junio 2020]. Disponible en: https://docs.vmware.com/es/VMware-vSphere/index.html

VMWARE. (2011). VMware vSphere Ediciones de Enterprise y Enterprise Plus. Hoja de datos. Disponible en: https://www.vmware.com/files/es/pdf/VMware-vSphere-Entreprise-Edition-Datasheet.pdf

VMWARE. [Sitio web]. [Consulta: 21 de mayo de 2020]. vCenter Server. Disponible en: https://www.vmware.com/co/products/vcenter-server.html

WATCHTHATPAGE. (2017). Your monitor for changes on the web. Recuperado de: http://www.watchthatpage.com

WATCHTHATPAGE. Your monitor for changes on the web. Visita guiada. Ver los cabios. [Consulta: 14 de junio 2020]. Recuperado de: http://www.watchthatpage.com/tutorialChanges.jsp

ANEXOS

Resumen Analítico Especializado -RAE

Fecha de Realización:	22/12/2020
Programa:	Seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Diseño técnico de la implementación de un centro de respuesta a incidentes de seguridad informática Cyber security de Colombia Ltda.
Autor(es):	Leal Mendivelso Jhon Alexander
Palabras Claves:	Incidente, seguridad, riesgo, vulnerabilidad, amenaza
Descripción:	Trabajo de grado para optar al título de especialista en seguridad informática, que consta del desarrollo de un proyecto aplicado, basado en el diseño de la implementación de un centro de respuesta a incidentes de seguridad informática, para la empresa Ciber Security de Colombia Ltda. En el cual se realiza un estudio técnico de la necesidad y la viabilidad del csirt, y se describe detalladamente la documentación del proceso de implementación, donde se relacionan las herramientas de ´software libre, equipos de cómputo, y soluciones de tecnologías modernas, orientadas a gestionar y responder adecuada y oportunamente a los incidentes de seguridad.

Fuentes bibliográficas destacadas:

ENISA. Agencia de la Unión Europea para la seguridad Cibernética. (2019). Como crear un CSIRT paso a paso. Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

DAPRE. (2019). Lineamientos del Equipo de respuesta a incidentes de seguridad de la Información. Disponible en: https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/L-SA- 01-Lineamiento-Equipo-Respuesta.pdf

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. {en línea}. (2016). {Consultado el 15 de noviembre de 2019}. Buenas prácticas para establecer un CSIRT nacional. Disponible en:

https://www.sites.oas.org/cyber/Documents/2016%20%20Buenas%20Practicas%2 0CSIRT.pdf COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. (2016). Conpes 3854. Política Nacional de Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf	
Contenido del documento:	El documento, como ya se mencionó anteriormente, es el desarrollo de un proyecto aplicado, como trabajo de grado, que describe detalladamente la documentación técnica de la implementación de un csirt privado para la empresa ciber security de Colombia Ltda, donde se realiza una introducción al tema de seguridad de la información, amenazas, riesgos, vulnerabilidades, y otros conceptos relacionados con incidentes de seguridad informática. Se ubica al lector en el contexto actual de la seguridad de la información en el país, realizando el planteamiento del problema, Se elabora un marco referencial, que incluye marco teórico, Marco conceptual, Marco, Marco Histórico, Marco espacial, Marco metodológico y Marco tecnológico. En cuanto al desarrollo de los objetivos, se describen las herramientas de Hardware y Software necesarias, se realiza una definición de roles y responsabilidades del recurso humano, junto con la estructura organizacional y las diferentes áreas o dependencias que conforman el equipo de trabajo. Se elabora el diseño del diagrama de la infraestructura tecnológica. Se determinan los servicios que puede prestar el CSIRT, listando y describiendo cada uno de ellos según su categoría.
Marco Metodológico:	Para la elaboración de este proyecto se utilizó una metodología documental descriptiva, seleccionando y compilando información a través de la asimilación y crítica de títulos y documentos, y demás material de consulta con respecto a la implementación de Equipos de respuesta a Incidentes de seguridad Informática.

	La metodología es cuantitativa, puesto que uno de sus objetivos es la cuantificación, medición y análisis estadístico de datos recolectados, respecto la cantidad de incidentes, amenazas, riesgos, vulnerabilidades y ataques contra las infraestructuras tecnológicas de las organizaciones a nivel mundial. Por otro lado, la metodología también es cualitativa, cuando se indaga por las características de las diferentes funciones y equipos que conforman el CSIRT, para poder establecer condiciones de eficiencia y eficacia de las tareas de gestión ante incidentes de seguridad, al momento de garantizar la integridad, disponibilidad, y confiabilidad de la información. La técnica de recolección de información que se utilizó es documental, realizando análisis y estudio de casos de implementación de CSIRT en organizaciones públicas y privadas a nivel mundial, recolectando datos de incidencias y utilización de nuevas técnicas que permitan afinar las políticas de planteamiento, configuración y administración de un equipo de Respuesta a Incidentes de Seguridad Informática.
Conceptos adquiridos :	Al finalizar el desarrollo del trabajo se adquieren conocimientos generales respecto a los pasos para la implementación de un equipo de respuesta a incidentes de seguridad informática, junto con herramientas necesarias para llevar a cabo dicha implementación y adaptación de nuevas tecnologías de versión libre, que permiten monitorear tráfico y equipos para prevenir la materialización de incidentes de seguridad informática.
Conclusiones:	Todas las organizaciones ya sea públicas o privadas, deben contar con un equipo de respuesta a incidentes de seguridad informática, que pueda contrarrestar dichos eventos. Los servicios de CSIRT pueden estar a cargo de un proveedor o implementarlo de manera privada, pero definitivamente es necesario contar con este servicio.