DISEÑO TÉCNICO ESTRUCTURADO DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS

LUIS CARLOS MARTINEZ RINCON

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

DISEÑO TÉCNICO DE UN CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS - CIBERSECURITY DE COLOMBIA LTDA

LUIS CARLOS MARTINEZ RINCON

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

Yolima Esther Mercado
Tutora de Curso
Yolima Esther Mercado
Asesora

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

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 07 de abril de 2022

DEDICATORIA

Dedico este trabajo a mi familia, agradeciendo todo el esfuerzo, apoyo y motivación que me han llevado a cumplir mis proyectos, a pesar de las desavenencias y lo desaciertos, hemos logrado mantenernos unidos en el lazo fuerte de la fraternidad, amor y el deseo de lucha por cumplir nuestros sueños en este paso corto por la vida, en el que día a día vamos cimentando cada peldaño con esfuerzo y dedicación para dejar una huella en nuestra historia y aportar a la sociedad en los diferentes retos del presente y futuro.

AGRADECIMIENTOS

Un agradecimiento muy especial a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes, con su trabajo y dedicación nos apoyaron en el fortalecimiento de nuestros conocimientos, permitiéndonos adquirir competencias para abrir nuevas oportunidades laborales y aportar nuestros servicios a la sociedad, de otra parte, a mis tutores y asesores quienes me acompañaron en este proyecto que culmina en la etapa de aprendizaje e inicia en la práctica profesional.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

Activo de información: Es toda aquella información valiosa para una entidad u organización, la cual se puede encontrar en diferentes medios, regularmente en ámbito de la seguridad informática se tipifican en hardware, software, servicios, redes e instalaciones los cuales pueden contenerla y administrarla.

Amenaza: Situación negativa y latente que puede ser originada de forma natural o accidental o intencionalmente, la cual puede tener implicaciones en la seguridad de la información, si se combina con una debilidad en los activos de información.

Análisis de trafico de red: Es la actividad relacionada con el monitoreo de datos que pasan por una red informática con el fin de detectar intrusiones y comportamientos indebidos sobre la misma.

Análisis forense: Es el procedimiento que permite llevar a cabo actividades asociadas a la investigación y recopilación de evidencias en busca de establecer quien, como y cuando fue realizada alguna acción, hecho o delito sobre algún activo de información.

Apache: Servidor web http, que permite alojar, crear páginas web e implementar medidas de seguridad en los sitios creados.

Ataque de fuerza bruta: Es un proceso automatizado mediante el cual se lanza diferentes combinaciones de contraseñas mediante herramientas de software automatizadas, con el propósito de descifrar la contraseña y acceder a un sistema.

Auditoria de seguridad: Consiste en la evaluación de la conformidad de requisitos y controles implementados de un sistema de gestión de seguridad de la información.

Cifrado: Es una técnica de seguridad, la cual se fundamenta en una operación matemática que permite codificar la información y mantener la confidencialidad de un texto que solo puede ser descifrado con la llave que encriptó la información.

Comando: Instrucción u orden realizada en una terminal del sistema operativo para que ejecute una acción determinada.

Confidencialidad: Es el principio o atributo que posee la información de permanecer en secreto sin importar el medio en que el que se encuentre, para que solo el personal autorizado pueda conocer su contenido.

Control correctivo: Medidas de contención del riesgo materializado que buscan restablecer un servicio o mitigar el impacto.

Control preventivo: Son medidas de prevención que pretenden evitar la materialización de un riesgo.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.[1]

CSIRT: Equipo de respuesta a incidentes cibernéticos.

Disponibilidad: Es la capacidad que se tiene para acceder de manera oportuna a la información a través de un sistema, servicio, documento físico o el medio de soporte en el que se encuentre.

Evaluación de vulnerabilidades: Es un proceso por medio del cual a través de una herramienta o sistema se identifica y enlistan las debilidades de seguridad que posee un activo de información.

Exploit: Es una instrucción mediante código, que permite vulnerar un sistema informático para afectar su disponibilidad, lograr el control del sistema o escalar privilegios que no han sido autorizados.

Hash: Es un proceso matemático que convierte una entrada de datos en un código o cadena única de caracteres a partir de dicha transformación, la cadena se genera siempre con un número exacto de caracteres indistintamente de la cantidad de datos de entrada.

IDS: *Sistema de detección de intrusos,* el cual funciona a través de alertas que permiten identificar un intento de conexión que no ha sido autorizado.

Incidente de seguridad: es un evento no deseado que impacta la seguridad de la información principalmente a los atributos de confidencialidad, integridad y disponibilidad de la misma.

Integridad: Es el principio que busca mantener en el tiempo, con exactitud y legibilidad la información, de la misma forma en la que fue generada.

Metaisplotable: Es una máquina virtual que se encuentra preparada intencionalmente con vulnerabilidades conocidas, con el propósito de poder realizar pruebas de seguridad.

---

[1] **MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES** [Sitio Web] Bogotá MINTIC Glosario , P.12 [Consulta : 28 de mayo 2021]. ,Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html

Mejores prácticas: Conjunto de acciones que han sido implementadas con éxito en varias organizaciones, siguiendo principios y procedimientos adecuados.[2]

Pentesting: Se le denomina de esta forma, a las pruebas de seguridad que se realizan a una plataforma tecnológica, en búsqueda de vulnerabilidades conocidas con el propósito de mitigarlas.

Phishing: Es un ataque originado mediante el fraude o suplantación de sitios web, que busca la obtención de información confidencial para fines delictivos.

Política de seguridad: Son las directrices impartidas, adoptadas o implementadas en una organización, con el propósito de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.

Riesgo informático: Es la probabilidad de que una amenaza en combinación con una vulnerabilidad, genere un impacto sobre los activos de información afectando sus atributos de integridad, confidencialidad y disponibilidad.

SGSI: Sistema de Gestión de Seguridad de la Información, es un conjunto de requisitos implementados a partir del estándar de la Norma ISO IEC/27001

SSL (Secure Sockets Layer): Se trata de un protocolo de seguridad que permite que los datos de una conexión, transiten de manera segura .

Suplantación: Se refiere a la acción de un individuo que realiza para hacerse pasar por otro, con el objetivo de cometer algún tipo de fraude.

Topología de red: Esquema gráfico que presenta la distribución de una red informática y la conexión con su infraestructura tecnológica.

Vulnerabilidad: Debilidad presente en los activos de información que puede ocasionar la perdida de la integridad, confidencialidad y disponibilidad de la información.

XSS (*Cross site scripting*)**:** Este término traduce en su texto abreviado, secuencias de comandos en sitios cruzados, una vulnerabilidad propia de sitios web en los cuales se puede alojar un programa malicioso, que permite la obtención y control del sitio.

---

[2] **MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES** [Sitio Web] Bogotá MINTIC Documento Maestro del Marco de Referencia de Arquitectura Empresarial , P. 17 [Consulta : 25 de junio 2021]. Disponible en: https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8158_descargable_6.pdf

RESUMEN

Cibersecurity de Colombia LTDA, es una entidad que presta servicios en seguridad de la información, el propósito a 2021 es establecerse como un CSIRT enfocado a la gestión de incidentes y vulnerabilidades en seguridad de la información, la entidad requiere un diseño técnico el cual permitirá la ejecución de las actividades como Centro de Respuesta a Incidentes Cibernéticos a sus partes interesadas, a través de un modelo estructurado que permita responder a sus necesidades en materia de ciberseguridad, con metodologías y herramientas de software en este campo, que de forma planificada responda efectivamente a la gestión de seguridad digital.

Ofrecer un servicio de gestión de incidentes de seguridad de la información, de calidad, oportuno, confiable y acorde con las necesidades del sector, permitirá apropiar la prevención de la seguridad digital, dentro de la cultura del autocontrol aportando a la disminución de ataques cibernéticos y garantizando la eficacia de la política de seguridad digital.

Palabras clave:

Prueba
Ciberseguridad
CSIRT
Incidentes
Vulnerabilidades
Diseño técnico
Centro de Respuesta a Incidentes

ABSTRACT

Cibersecurity de Colombia LTDA, an entity that provides information security services whose purpose in 2021 is to establish itself as a CSIRT focused on the management of incidents or vulnerabilities, the entity requires a technical design which will allow the execution of activities as a Security Center. Response to Cyber Incidents to their stakeholders, through a strategy that will allow them to respond to their digital security needs with advanced tools and a tactical plan that effectively responds to digital security management.

Offering a service for the management of information security incidents of timely quality, reliable and in accordance with the needs of the sector, will allow the prevention of information security within the culture of self-control in the general public, positively affecting the index of cyber-attacks contributing to the effectiveness of the digital security policy

Keywords:

Test
Cybersecurity
CSIRT
Incidents
Vulnerabilities
Technical design
Incident Response Center

INTRODUCCIÓN

En el contexto de las Tecnologías de la Información y las Comunicaciones, surgieron diferentes amenazas y vulnerabilidades, que atentan contra la misma. es por ello, que de la misma manera se han abordado diferentes acciones para contrarrestar este fenómeno, el cual ha ido en aumento con la evolución tecnológica.

La necesidad de la conformación de un equipo de respuesta a incidentes de seguridad de la información CSIRT, se hizo prioritaria para el establecimiento de los esquemas de seguridad y como una medida necesaria para abordar aquellos incidentes, en los que no existía una instancia organizada que se ocupara en las entidades por este fenómeno.

El presente documento, expone un modelo de previsión de los recursos y procesos necesarios para la conformación de un CSIRT, que través de la metodología del proyecto aplicado, desarrollará aquellos aspectos necesarios para establecer un equipo de respuesta a incidentes de seguridad de la información CSIRT.

1 DEFINICIÓN DEL PROBLEMA

La Seguridad de la Información, se ha convertido en un punto crítico para todas las entidades, tanto en el sector público como en el privado, la perdida de la confidencialidad, integridad y disponibilidad de la información, puede acarrear desde perdida de la imagen institucional, hasta sanciones legales y económicas conforme a las leyes del marco regulatorio colombiano. El aumento del número de amenazas y vulnerabilidades de seguridad digital, se ha convertido en un riesgo inminente, que puede impactar tanto en las organizaciones, como en la ciudadanía en general.

Cada vez son más novedosos los ataques a los 3 principios de la seguridad de la información y pueden provenir de diferentes fuentes, tanto internas como externas, estos tienen el propósito de afectar con severidad los activos de información de las organizaciones, resultando imperativo contar con un equipo de respuesta que se encargue de atender los incidentes y vulnerabilidades de seguridad de la información, así como de realizar el seguimiento y control de los activos de información, para protegerlos, respaldarlos y asegurarlos en las entidades.

1.1 ANTECEDENTES DEL PROBLEMA

El CONPES 3854 de 2016[3] presenta en su análisis estadístico alrededor de 20 ataques cibernéticos al año, entre los más representativos se encuentra el Defacement, el cual se configura como un delito informático que busca generar una alteración en páginas web, aprovechando alguna vulnerabilidad para obtener privilegios del sitio, este delito posee un porcentaje de participación del 27.4%[4],en segundo lugar, se encuentra el Malware o código malicioso, el cual consiste en programas que simulan ser sistemas de algún fabricante reconocido y/ o códigos de programación que son remitidos por correos o páginas publicitarias que vulneran los equipos generando robos de información o daño en los sistemas, este delito presenta un 16% de participación, la infiltración lógica externa e interna manejan un 16% respectivamente entre otros.

1.2 FORMULACIÓN DEL PROBLEMA

¿Como establecer un diseño técnico estructurado para la gestión efectiva de incidentes y vulnerabilidades de seguridad informática en la empresa - CIBERSECURITY DE COLOMBIA LTDA?

[3] **DEPARTAMENTO NACIONAL DE PLANEACIÓN** [Sitio Web] Bogotá DNP, CONPES 3854 de 2016 Política Nacional De Seguridad Digital. P .44-45 [Consulta: 28 de mayo 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

2 JUSTIFICACIÓN

Dentro del análisis estadístico de incidentes de seguridad, se trae como referencia el incidente de seguridad de la información, sucedido en la empresa EBay[5], en la cual fue comprometida la base de datos de 128 millones de compradores de esta plataforma, en ese sentido cualquier entidad que no controle los riesgos de seguridad digital, es potencialmente expuesta a este tipo de escenarios que dependiendo del impacto podría ser catastrófico para la organización y acarrear sanciones económicas y disciplinarias de conformidad con la normatividad vigente.

El gobierno nacional, atendiendo esta problemática, ha volcado sus esfuerzos para combatir las constantes amenazas de seguridad digital, suministrando lineamientos para la protección de los activos de información, armonizados con leyes relacionadas al derecho de acceso de la información pública y la protección de los datos personales, Es por ello que desde la expedición de leyes como la Ley 1581 de 2012 " Ley de Protección de Datos Personales" o la Ley 1712 de 2014", Ley de Transparencia y Acceso a la Información Pública, hasta la expedición del CONPES 3701 "Lineamientos de política para ciberseguridad y ciberdefensa" y el CONPES 3854 de 2016 "Política Nacional de Seguridad Digital" entre otros, se busca priorizar y salvaguardar la seguridad digital de las organizaciones y la población en general.

Es importante destacar que el Ministerio de las TIC, abordó una importante estrategia en respuesta a la ciberdelincuencia, formulando el Modelo de Seguridad y Privacidad de la Información, en el cual articuló mejores prácticas en materia de defensa de la seguridad informática, basándose en la ISO 27001 de 2013 y formulando una serie de guías que permiten su implementación, de esta forma se permite cerrar brechas que existen entre las entidades y aumentar el nivel de madurez del SGSI.

[5] **INSTITUTO NACIONAL DE CIBERSEGURIDAD. 2014.** Intrusión en eBay [Sitio Web]. Madrid: INCIBE, [Consulta 21 de mayo 2014]. Disponible en: https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/intrusion-ebay

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Construir un diseño técnico estructurado para la conformación de Equipos de Respuesta a Incidentes de Seguridad de la Información CSIRT, en la empresa Cibersecurity de Colombia LTDA.

3.2 OBJETIVOS ESPECÍFICOS

1. Establecer herramientas para la gestión de incidentes y vulnerabilidades de seguridad digital.
2. Diseñar el modelo para la conformación del CSIRT de la empresa Cibersecurity de Colombia LTDA.
3. Implementar herramientas de gestión de incidentes y testar vulnerabilidades de seguridad digital en ambientes controlados.
4. Evaluar la efectividad del diseño técnico de seguridad digital del CSIRT de la empresa Cibersecurity de Colombia LTDA.

4 MARCO REFERENCIAL

Este proyecto se sustenta bajo el Modelo de Seguridad y Privacidad de la Información expedido por el Ministerio de las TIC, fundamentos técnicos de la GTC ISO /IEC 27035 de 2012 del ICONTEC, La guía de buenas prácticas para establecer CSIRT de la OEA, el marco de referencia CIS CONTROL, que incluye diversos controles para la defensa en la protección de la integridad, disponibilidad y confidencialidad de la información, las normas y leyes relacionadas con la seguridad digital colombiana vigente.

4.1 MARCO TEÓRICO

4.1.1 ¿Por qué El CSIRT es una necesidad en la Transformación Digital?

El mundo cada vez más se adentra en un cambio a la transformación digital, diferentes trámites y servicios son el punto de atención para esta transformación, por lo que el gobierno nacional de Colombia, le ha confiado a la tecnología una de las estrategias para la “Racionalización de trámites y servicios” , determinada como “Racionalización Tecnológica”, tarea importante que lleva a suponer un cambio en el modelo de operación de las organizaciones, que no solamente acapararía el sector público sino también el privado, en esencia, esta transformación busca facilitarle la vida a los usuarios, poniendo a su disposición en las plataformas digitales, aquellos trámites y servicios engorrosos a los que se someten diariamente, en ese sentido, las empresas u organizaciones que logren la transformación, otorgaran un valor agregado que se resume en la reducción del tiempo y los costos ocasionados por desplazamiento y gestión de los tramites y servicios a los grupos de interés. No obstante, este proceso de transformación digital solo será beneficioso para los usuarios, en la medida que las organizaciones tengan la capacidad de asegurar los datos y transacciones que se transfieren y transitan a través de la red y sus diferentes plataformas, teniendo en cuenta que la presencia de la ciberdelincuencia ha incrementado exponencialmente en los últimos años, con ataques más novedosos y mejorados, impactando la seguridad digital de los usuarios y las organizaciones.

La falta de confianza en los entornos digitales es notoria en la población colombiana, sin embargo, corresponde a la realidad, pues la capacidad de reacción ante los incidentes cibernéticos que expone el DNP en el CONPES 3995 es desalentadora, teniendo que los datos estadísticos referenciados en la Política Nacional de Seguridad Digital, con respecto a los resultados del National Cyber Security Index 2019, Colombia posee una capacidad de respuesta de incidentes cibernéticos del

50%[6], y un 0% en la protección de servicios digitales, tal como se presenta en la Figura 1, es por ello que teóricamente el problema de la transformación digital y el establecimiento de nuevas tecnologías en el país, radica en que las organizaciones no cuentan con las condiciones de seguridad informática para esta evolución tecnológica, debido la deficiente capacidad de respuesta a incidentes de seguridad y en la escasa identificación y corrección de vulnerabilidades de su infraestructura T.I., lo cual se convierte en un riesgo latente para aquellas organizaciones que dan este paso sin contar con un diseño técnico estructurado que pueda atender las emergencias y vulnerabilidades de seguridad, las cuales pueden afectar la continuidad de la operación, la imagen institucional y su economía.

Figura 1 Resultados del National Cyber Security Index 2019 Porcentaje de avance

Fuente 1: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

El equipo de respuesta a incidentes de seguridad informática (CSIRT)[7], tiene una función principal que se puede traducir en la prestación de servicios para la prevención, gestión y atención de incidentes de seguridad, respondiendo de manera oportuna y eficaz a los ataques e incidentes de seguridad de una organización, son la pieza fundamental a la cual se le confiaría un cambio tan importante como es la transformación digital en una organización, constituirlo de manera independiente o

[6] **DEPARTAMENTO NACIONAL DE PLANEACIÓN** [Sitio Web] Bogotá DNP POLÍTICA NACIONAL DE SEGURIDAD DIGITAL , P. 23 [Consulta : 01 de julio 2021]. ,Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[7] **ORGANIZACIÓN DE ESTADOS AMERICANOS** [Sitio Web] Washington DC. OEA abril 2016 ,Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

incorporarlo en una dependencia de la organización de acuerdo a los recursos, otorgarían la tranquilidad a las directivas para dar el paso firme a un cambio de tal envergadura.

4.1.2 El equipo de respuesta CSIRT como primera línea de defensa.

Los modelos y estándares de seguridad de la información han provisto de manera significativa las herramientas e instrumentos para la defensa de la disponibilidad integridad y confidencialidad de la información, sin embargo la gestión de los riesgos de S.I. establecidos aún son inmaduros, contienen algunas amenazas e incidentes y vulnerabilidades, pero no suelen responder de manera inmediata ante una emergencia de seguridad, regularmente se delega la responsabilidad de implementar los controles de seguridad al personal de las dependencias que no poseen la experticia para esta labor, es decir, hay una designación de responsabilidades arbitraria pero no estructurada, algunos modelos como el integrado de planeación y gestión MIPG8, del Departamento Administrativo de la Función Pública, define como estrategia 3 líneas de defensa basados en el modelo operación militar, estableciendo un sistema de control para el aseguramiento de la evolución del modelo y la evaluación del desempeño, pero no define en su primera línea, la forma como debería articularse los equipos de trabajo para cada política del modelo, es así que desde la estructura metodológica de la Guía de gestión de riesgos DAFP, incorpora un anexo técnico adicional de gestión de riesgos para la seguridad digital, donde existen particularidades, como el enfoque hacia activos de información, que es difícil de entender por el personal que no reconoce ni sabe aplicar las herramientas de control existentes en materia de seguridad digital, en ese sentido hay una necesidad de las organizaciones de fortalecer estructuras de operación, para la respuesta a los incidentes, amenazas y vulnerabilidades de seguridad digital, que serán fundamentales para la organización interna y la cohesión de habilidades de los expertos en la materia.

4.2 MARCO CONCEPTUAL

INCIDENTES: En el marco de la seguridad de la información, se llama incidente a toda aquella situación que afecta la continuidad de la operación de los sistemas, redes y demás activos de información, dentro de esta tipificación se encuentran los accesos no autorizados, interrupción indebida de un sistema y/o eliminación de información producida por el mismo hecho o evento, entre otros. Asimismo, la Guía Técnica Colombiana GTC 27035, del Instituto Colombiano de Normas Técnicas y Certificación ICONTEC, lo define como "Un evento o una serie de eventos de seguridad de

[8] **DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA**, Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG [Sitio Web] Bogotá DAFP, 24 de julio 2018 ,Disponible en: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34268003

la información no deseados o inesperados que tienen una probabilidad significativa de poner en riesgo las operaciones del negocio y de amenazar la seguridad de la información"[9].

VULNERABILIDADES: Es importante para este marco teórico, profundizar sobre la identificación y análisis de vulnerabilidades, entendidas como aquellas atribuibles a las debilidades o falencias que posee la infraestructura tecnológica de una organización, la cual podría ser explotada por una amenaza si no se toman las medidas correctivas respectivas. las vulnerabilidades se pueden asociar desde una falta de actualización de un sistema operativo o software de bases de datos o en la deficiente configuración de permisos y controles que generan brechas de seguridad, posibilitando accesos no autorizados y poniendo en riesgo la confidencialidad, disponibilidad e integridad de la información.

CSIRT: Este concepto ha sido abordado con diferentes nombres de acuerdo a la ubicación geográfica, algunos de los nombres conocidos son: SERT Security Emergency Response Team, Equipo de respuesta a emergencias de seguridad); CERT o CERT/CC (Computer Emergency Response Team / Coordination Center; equipo de respuesta a emergencias informáticas / Centro de coordinación); IRT (Incident Response Team, equipo de respuesta a incidentes)[10] ,no obstante todos buscan un mismo propósito, atender y responder los incidentes cibernéticos, a través un equipo de especialistas que se encargan de las emergencias cibernéticas, la GTC 27035 aborda este equipo como el ISIRT, el cual se considera como : "Equipo conformado por miembros confiables de la organización, que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información, durante el ciclo de vida de éstos"[11].

SEGURIDAD INFORMÁTICA: Es el conjunto de herramientas, medidas, y acciones de control que se implementan para mitigar los riesgos informáticos y garantizar la protección de los activos de información de una organización.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: Es un marco de referencia de buenas prácticas en materia de seguridad de la información diseñado por el MINTIC, que reúne diferentes fuentes de conocimiento definiendo directrices para la protección de la infraestructura crítica de las entidades del estado colombiano, que a través de guías metodológicas orientan a las entidades para la implementación de medidas de seguridad y privacidad de la información.

CISCONTROL: Es un marco de referencia construido por diferentes expertos en seguridad, que identifica 20 controles críticos en materia de ciberseguridad, en los

[9] **ICONTEC** GTC 27035 - TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN , P. 3 ,2012

[10] **AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN** [Sitio Web] Attiki ENISA Cómo crear un CSIRT paso a paso , P. 6 [Consulta : 31 de julio]. ,Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

[11] Ibit ., p. 2

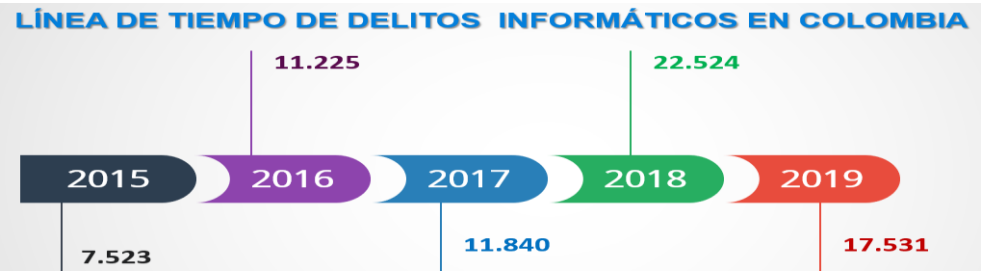
cuales incluyen los asociados a la respuesta y manejo de incidentes y pruebas de penetración o *pentesting*. los Ciscontrol constituyen mejores prácticas de seguridad para prevenir y responder a ataques más representativos en contra de los sistemas informáticos y redes de una organización.[12]

4.3 MARCO HISTÓRICO

Desde hace tiempo ya, la tecnología ha permitido mejorar el desempeño de las organizaciones, con la automatización de sus procesos productivos y el mercadeo de sus bienes y servicios, hoy en día las nuevas estrategias de las organizaciones, le han apostado a una evolución tecnológica más agresiva, con el fin de adquirir más usuarios y facilitar la gestión en la venta de sus productos. Lo anterior ha conllevado a abrir portales digitales de las organizaciones como páginas web y aplicaciones, donde desarrollan sus operaciones transaccionales, asimismo, la delincuencia ha evolucionado con los nuevos cambios de la modernidad, identificando fallos de seguridad y vulnerabilidades en estos sitios y en sus operaciones digitales, que han penetrado la seguridad, tanto de las organizaciones como de los usuarios, a través de diferentes modalidades, categorizadas en un nuevo concepto denominado ciberdelincuencia.

Existen precedentes de la ciberdelincuencia en el registro histórico de la Policía Nacional, de acuerdo al informe de tendencias del cibercrimen en Colombia, se ha pasado de 7.523 incidentes reportados en el año 2015 a 17.531 al 2019, los delitos más representativos en esta línea del tiempo es el hurto por medios informáticos, que reporta 31.058 casos, precedido de la violación de datos personales con 8.037 casos y el Acceso abusivo a sistema informático con 7.994 casos[13], discriminados como se muestra en la Figura 2.

Figura 2 Línea de tiempo



Fuente 2 Elaboración propia

[12] **CENTRO DE RESPUESTAS A INCIDENTES CIBERNÉTICOS** [Sitio Web] Paraguay CERT CIS Controls Spanish Translation , P. 5 [Consulta : 28 de mayo 2021]. , Disponible en: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

[13] **POLICIA NACIONAL DE COLOMBIA** [Sitio Web] Bogotá PONAL Tendencias cibercrimen en Colombia, [Consulta : 30 de mayo 2021]. ,Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Con la llegada del COVID -19 en la vigencia 2020, una temporada de cuarentenas y demanda de servicios virtuales fueron el factor predominante ante la emergencia sanitaria, asimismo el contexto de la pandemia disparó el número de ataques cibernéticos posicionando el Phishing entre uno de los más destacados, pues la suplantación de los sitios web de acuerdo al balance cibercrimen 2020[14], generó un incremento del 358% para esa vigencia, concentrando la mayor afectación en la ciudad de Bogotá con 12.981 casos y un 37% de participación de las ciudades más afectadas.

De otra parte en la vigencia 2021, en Colombia se desató un estallido social por algunos proyectos de reformas que afectarían a la canasta básica de alimentos, en medio de la protesta social y denuncias por uso desmedido de la fuerza por parte de la Policía Nacional, el grupo ciber activista llamado Anonymous infiltra 168 cuentas de correos electrónicos del Ejercito Nacional de Colombia y provoca la caída de la página de la misma entidad en comunicación realizada por el periódico TIEMPO[15] , de lo que podemos interpretar, que sin importar la justificación del acto en sí , es claro que los medios tecnológicos son el objetivo principal de las amenazas cibernéticas y sus vulnerabilidades son el eslabón más débil por donde se quebranta a las organizaciones, con estos ataques que cada vez cobran más triunfos para el cibercrimen.

4.4 ANTECEDENTES O ESTADO ACTUAL

Teniendo como base de conocimiento la Investigación en ingeniería de sistemas e informática publicada en 2011[16]; Los CSIRT tuvieron origen en el año de 1988 luego de ser liberado el gusano informático llamado Morris, que trajo como consecuencia la necesidad de conformar el primer equipo de respuesta de emergencias informáticas (CERT), fundado por la organización DARPA (Defence Advanced Research Projects Agency), una agencia de Investigación de Proyectos Avanzados de Defensa, quienes se dedicaban a atender este tipo de emergencias, desde esa época el modelo fue adoptado en Europa y se siguió extendiendo bajo otros nombres como el CSIRT pero con un mismo fin.

[14] **POLICIA NACIONAL DE COLOMBIA** [Sitio Web] Bogotá PONAL Balance cibercrimen 2020 , P. [Consulta : 30 de mayo 2021]. ,Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

[15] **EL TIEMPO** [Sitio Web] Bogotá 30 de mayo 2021 ,Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/anonymous-revela-correos-y-contrasenas-de-miembros-del-ejercito-de-colombia-585874

[16] **ZAPATA PUERTA ,Luis Norberto y RECAMAN CHAUX**, Hernando, Investigación en ingeniería de sistemas e informática [En línea].Investigación Universidad Pedagógica y Tecnológica de Colombia2011[Consultado el 30 de mayo 2021] Disponible en:https://www.researchgate.net/profile/Jair-Otero/publication/220017085_Excalibur_Software_para_la_Administracion_de_Mecanimos_de_Seguridad_y_Servicios_de_Red_en_Sistemas_Operativos_Linux/links/0deec528bc07062c7c000000/Excalibur-Software-para-la-Administracion-de-Mecanimos-de-Seguridad-y-Servicios-de-Red-en-Sistemas-Operativos-Linux.pdf#page=117

Colombia en la actualidad estableció el colCERT, como un grupo de respuesta a emergencias cibernéticas, bajo el cual, se delegó la responsabilidad de la coordinación de la ciberseguridad y ciberdefensa nacional, que tendría como propósito la protección de la infraestructura del Estado, así como la asesoría a los CSIRT del sector público y privado entre otras de sus funciones, asimismo trabaja con aliados estratégicos con otras entidades del gobierno nacional como el MINTIC La Superintendencia Financiera ,la Presidencia de la Republica y el Centro Cibernético Policial, quienes trabajan en conjunto para atender las diferentes emergencias que giran en el contexto de la ciberdelincuencia.

La diversidad de los enfoques y alcances de los CSIRT es amplia, debido a que los equipos de respuesta, aunque manejan un modo de operación similar, atienden emergencias específicas de su interés de acuerdo con su misionalidad, es así que la OEA, ha realizado la siguiente clasificación, a través de la Guía de buenas prácticas para CSIRT: [17]

CSIRT PARA INFRAESTRUCTURAS CRÍTICAS: Concentra sus esfuerzos, en la protección de infraestructura tecnológica de la nación, en esta se incluye el suministro energético que sustenta la misma, sin importar que sea o no administrado por entes privados o públicos.

CSIRT ACADÉMICO: este equipo de respuesta nace en apoyo a la academia sustentando las necesidades en la atención y respuesta de emergencias cibernéticas para universidades quienes trabajan en cooperación con investigadores de la misma academia y su tamaño es proporcional a los integrantes que participan.

CSIRT GUBERNAMENTALES: Los equipos de respuesta de esta clase priorizan sus servicios para proteger y respaldar la infraestructura de los entes gubernamentales que prestan servicios públicos a los ciudadanos y se pueden estructurarse a partir de sectores independientes.

De otra parte, existen algunos CSIRT que se han creado bajo nuevos preceptos, y en respuesta al incremento desmedido de los fraudes financieros, es así, que, en Colombia fue creado el CSIRT Financiero por la Asobancaria, aterrizando el modelo a la protección de la infraestructura critica del sector financiero, en beneficio de los usuarios de la banca digital.

[17] **ORGANIZACIÓN DE ESTADOS AMERICANOS,** [Sitio Web] Washington DC. OEA abril 2016 ,Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

4.5 MARCO LEGAL

COLOMBIA. EL CONGRESO DE COLOMBIA, LEY 1273 (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”, esta ley establece cuales son los delitos informáticos en el estado colombiano, asimismo dicta las penas a las que serán sometidos quienes atenten contra la infraestructura tecnológica del sector público y privado, bajo ese contexto los ataques que serán objeto de análisis y mitigación por parte del CSIRT, se tipifican como delitos en la legislación colombiana.

COLOMBIA. EL CONGRESO DE COLOMBIA, Ley 1581 (17 de octubre de 2012) "Por la cual se dictan disposiciones generales para la protección de datos personales", la protección de la confidencialidad de la información, que requieren las organizaciones y que será demandada al equipo de respuesta CSIRT, es fundamentada bajo ley 1581 del 2012, en donde se considera como una obligación, mantener los datos relacionados con las condiciones de salud, origen racial, orientación sexual e inclinación política de los usuarios, bajo estricta reserva, en tal sentido aquellas medidas de control como el cifrado de la información son consecuentes y pertinentes para este propósito.

COLOMBIA. EL MINISTERIO TIC, Resolución 500 (10 de marzo de 2021). "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", Es aplicable la presente resolución de conformidad con el numeral 10 del art.6, el cual establece que las entidades del sector público deben realizar un análisis de riesgo y determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital, de otra parte, el art.9 establece pautas para la gestión de incidentes, así como también el deber de reportar cualquier incidente al CSIRT del gobierno nacional.

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN , CONPES 3995 (01 de julio de 2020). "Política Nacional de Confianza y Seguridad Digital", esta política brinda el contexto actual de la seguridad digital en Colombia y asimismo establece la importancia de la respuesta oportuna a incidentes y amenazas afirmando en su diagnóstico, que Colombia no ha mejorado en este aspecto, determinando una pérdida de capacidad en la confianza de la Seguridad Digital[18].

[18] **DEPARTAMENTO NACIONA DE PLANEACIÓN** [Sitio Web] Bogotá DNP "Política Nacional de Confianza y Seguridad Digital", P. 21,22 [Consulta : 31 de julio]. ,Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

5 DISEÑO METODOLÓGICO

Este trabajo posee un desarrollo metodológico basado en la investigación aplicada, la cual busca la solución del problema planteado, a través de la consulta de fuentes e instrumentos en el campo de la seguridad informática, que posteriormente serán implementados y documentados desarrollando de forma organizada las prácticas que ejemplificaran la estructura y diseño técnico de la conformación de un CSIRT, como centro de respuesta de incidentes cibernéticos, asimismo se abordaran cada uno de los objetivos propuestos, permitiendo un desarrollo estructural del proceso de investigación.

La presente investigación también es acompañada por el método mixto con la relación de variables cuantitativas y cualitativas que apoyan la justificación y el problema a analizar y se determina en la aplicación de las técnicas y conocimientos adquiridos en la especialización de seguridad informática.

El alcance del presente proyecto, parte de la investigación y análisis de la problemática, se desarrolla en el marco de los objetivos planteados, hasta la aplicación de escenarios de laboratorios controlados y el análisis de los mismos.

El abordaje de los objetivos de este proyecto de investigación, se desarrollarán a través de fases que se enmarcan en el ciclo PHVA, la adopción de las mejores prácticas referidas en el Modelo de Seguridad y Privacidad de la Información de MINTIC, la GTC ISO 27035 de 2012, los controles de la ISO 27001:2013, CIS Control, como la hoja de ruta que permitirá el desarrollo de los objetivos específicos y la concreción del objetivo general

Es pertinente y valioso el método seleccionado, porque reúne tanto el conocimiento teórico como el práctico, de los cuales el segundo suele estar ausente en los modelos y estándares que ofrece la academia.

6 DESARROLLO DE LOS OBJETIVOS

6.1 FASE I IDENTIFICACIÓN DE HERRAMIENTAS Y MÉTODOS PARA LA GESTIÓN DE INCIDENTES Y ANÁLISIS DE VULNERABILIDADES DE SEGURIDAD DIGITAL

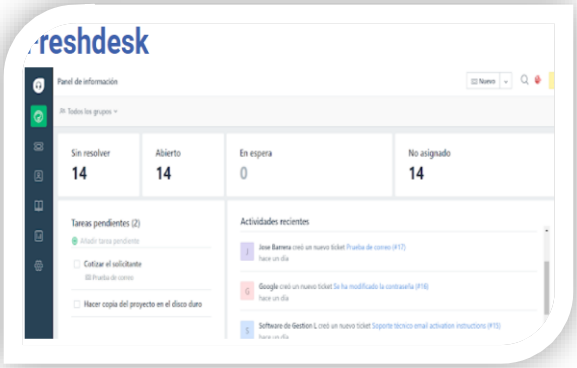
6.1.1 Herramientas de Software

El CSIRT dentro de su inventario de software para soportar las diferentes funciones se equipará de las siguientes herramientas para dar respuesta a los servicios reactivos y proactivos.

6.1.1.1 Herramientas de servicio proactivo

FRESHDESK: La atención de incidentes de seguridad, requiere de un sistema de registro y reporte escalable, que permita la trazabilidad de los casos que se registran, en tal sentido y como primera medida, se requiere una herramienta para la administración de los casos del CSIRT, es por ello que se propone la herramienta de Freshdesk de opensource, la interfaz se puede observar en la Figura 3.

Figura 3 Interfaz Freshdesk



Fuente 3 https://Freshdesk.com/

OPENVAS: Este es un software de análisis de vulnerabilidades, el cual se ofrece en la red en la modalidad open source, incluye más de 50.000 pruebas de vulnerabilidades, este software permite realizar el escaneo de las vulnerabilidades de los diferentes sistemas y equipos, a través de una interfaz intuitiva y amigable, el logo se puede identificar en la Figura 4.

Figura 4 Logotipo OpenVAS

Fuente 4 http://openvas.org/

NMAP: Es un potente software que permite realizar entre sus funciones principales, el escaneo de puertos y servicios de los equipos, permitiendo detectar posibles vulnerabilidades que posee una máquina en la red, convirtiéndose en una herramienta indispensable para escaneo de vulnerabilidades, el logo se puede identificar en la Figura 5.

Figura 5 Logo NMAP

Fuente 5 https://nmap.org/download.html

WIRESHARK: Wireshark es uno de los sistemas más adecuados para realizar análisis de protocolo de red, la cual nos permite realizar seguimiento a los datos de red, posibilitando encontrar fluctuaciones que revelen ataques de otras máquinas en el equipo anfitrión, en búsqueda de puertos abiertos entre otros, el logo se puede identificar en la Figura 6.

Figura 6 Logo Wireshark

Fuente 6 https://www.wireshark.org/

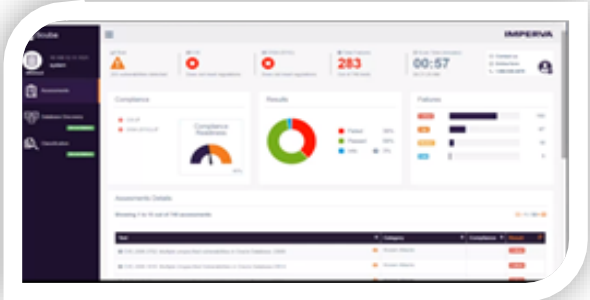
METASPLOIT: Esta herramienta es una de las más usadas para realizar test de penetración en el Hacking ético, la cual detectando una vulnerabilidad la aprovecha y a través de los exploit que almacena son quebrantados los esquemas de seguridad, siendo valiosa para auditar la seguridad en los equipos el logo del software se puede observar en la Figura 7

Figura 7 Logo Metasploit

Fuente 7 https://www.metasploit.com/

SUCUBA IMPERVA: Esta aplicación permite el análisis de vulnerabilidades en las bases de datos, por tal motivo es necesaria incluirla en el inventario de herramientas de análisis de vulnerabilidades debido a su función específica, de otra parte, el programa propone solución a las vulnerabilidades la interfaz se puede observar en la Figura 8.

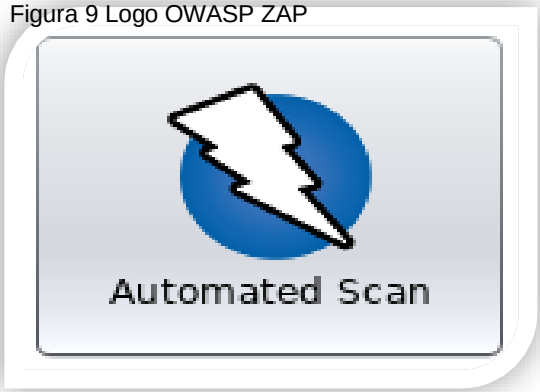
Figura 8 Logo Imperva



Fuente 8 https://www.imperva.com/

OWASP ZAP: Esta aplicación usada para realizar pruebas de seguridad siendo parte de las herramientas más útiles del Proyecto Abierto de Seguridad en Aplicaciones Web, la cual permite detectar riesgos y vulnerabilidades en aplicaciones web basadas en el TOP 10 de OWASP, esta herramienta es de código abierto , fácil de instalar y configurar, sus siglas en ingles especifican *Zed Attack Proxy.*

Figura 9 Logo OWASP ZAP



Fuente 9 Elaboración propia

6.1.1.2 Herramientas de servicio reactivo

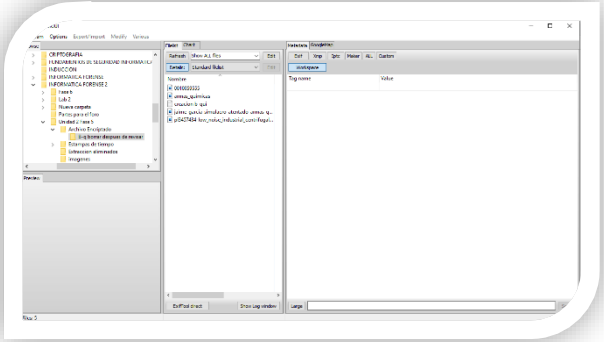
AUTOPSY: En los softwares para el análisis forense de tipo Open Source se destaca Autopsy, este sistema permite realizar extracción de la metadata y de información de los discos duros con el fin de realizar inspecciones respecto a la modificación eliminación de información entre muchas de las funcionalidades que ofrece , por este motivo es esencial para el CSIRT en respuesta a los servicios de reactivos de los incidentes de seguridad que se requieran atender, el logo del software se puede observar en la Figura 9

Figura 10 Logo Autopsy

Fuente 10 https://www.autopsy.com/support/training/

EXIFTOOL: Este software se caracteriza por su excelente análisis y revisión de la metadata en los diferentes tipos de archivos el cual puede ser usado en apoyo de otras herramientas de análisis forense, asimismo puede ser usada con una interface Gui, el logo del software se puede observar en la Figura 10

Figura 11 Interfaz Exiftool



Fuente 11 https://exiftool.org/

6.2 FASE II MODELO DE OPERACIÓN Y ESTRUCTURA DEL CSIRT

Los CSIRT, tal como se establece en la Norma ISO 27035, (*Computer Security Incident Response Team),* son el "Equipo de Respuesta a Incidentes de Seguridad de Tecnología de la Información"[19], Estos son conformados por una serie de expertos que analizan los diferentes incidentes y/o vulnerabilidades, que son tratadas a través de diferentes técnicas, que permiten mitigar el impacto en las organizaciones.

Existen diferentes nombres otorgados a esta clase de equipos de respuesta de incidentes informáticos, por ejemplo:

- CERT (*Computer Emergency Response Team*), Equipo de respuesta ante emergencias de tecnología de información.

- ISIRT *(Information Security Incident Response Team*), Equipo de respuesta a incidentes de seguridad de la información, entre otros.

Tabla 1 Estructura del CSIRT (Conformación del Equipo)

Rol	Responsabilidad	Gráfico
Líder de proceso CSIRT	Encargado de dirigir y coordinar la planeación estratégica y el Equipo de Respuesta de Incidentes de Seguridad de Tecnología de la Información	
Referente Jurídico CSIRT	Encargado del análisis de los casos y situaciones de responsabilidad legal y el marco jurídico que se encuentra en el contexto de la seguridad informática.	
Referente de Comunicaciones CSIRT	Responsable de la gestión de comunicaciones, estrategias y relaciones públicas en el contexto de la seguridad informática.	
Administrador de incidentes CSIRT	Es el responsable clasificar, evaluar, eventos, incidentes y vulnerabilidades, así como realizar el seguimiento y respuesta de los mismos	
(Técnico) Gestor de Incidentes y vulnerabilidades	Encargado de erradicar contener y dar respuesta a los incidentes y vulnerabilidades de seguridad.	

[19] **ICONTEC** GTC 27035 - TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN , P. 3 ,2012

Forense CSIRT	Responsable de realizar el análisis forense de los incidentes, de seguridad que son escalados por el administrador, y generación de informes de los casos escalados.	

Fuente 12 elaboración propia con base Manual de buenas prácticas CSIRT
https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

6.2.1 Servicios del CSIRT

Los servicios que ofrece un CSIRT, se orientan al sector objetivo y el propósito de la organización, de tal forma que exista coherencia con la planeación estratégica y los servicios que ofrece el equipo de respuesta.

De acuerdo al "*Manual de Buenas Prácticas para Establecer un CSIRT Nacional de la OEA (Organización de Estados Americanos"*[20] los servicios que se deben contemplar se refieren a continuación en Tabla 2 y Tabla 3

Tabla 2 Servicios del CSIRT

Servicios proactivos	Servicios Reactivos	Servicios de valor agregado
Monitoreo externo	Análisis post mortem	Capacitación y educación
Monitoreo Interno	Asistencia en el sitio	Concientización
Desarrollo de herramientas de seguridad	Asistencia en el sitio	Análisis de riesgos y continuidad de negocio
Reportes y alertas de seguridad	Respuesta a vulnerabilidades	Apoyo a emprendimientos de seguridad
Auditorías de seguridad.	Respuesta a artefactos maliciosos	

Fuente 13 elaboración propia con base Manual de buenas prácticas CSIRT
https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Tabla 3 Servicios Proactivos y Reactivos

Servicios Proactivos Monitoreo y Alertas	Servicios Reactivos Gestión de Incidentes
Escaneo de vulnerabilidades	Análisis forense
Escaneo de artefactos maliciosos.	Respuesta a incidentes
Monitoreo de tecnología.	Tratamiento a incidentes
Análisis de artefactos	Alertas y advertencias

Fuente 14 elaboración propia con base en el Manual de buenas prácticas CSIRT
https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[20] **ORGANIZACIÓN DE ESTADOS AMERICANOS** [Sitio Web] Washington DC. OEA abril 2016 ,Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

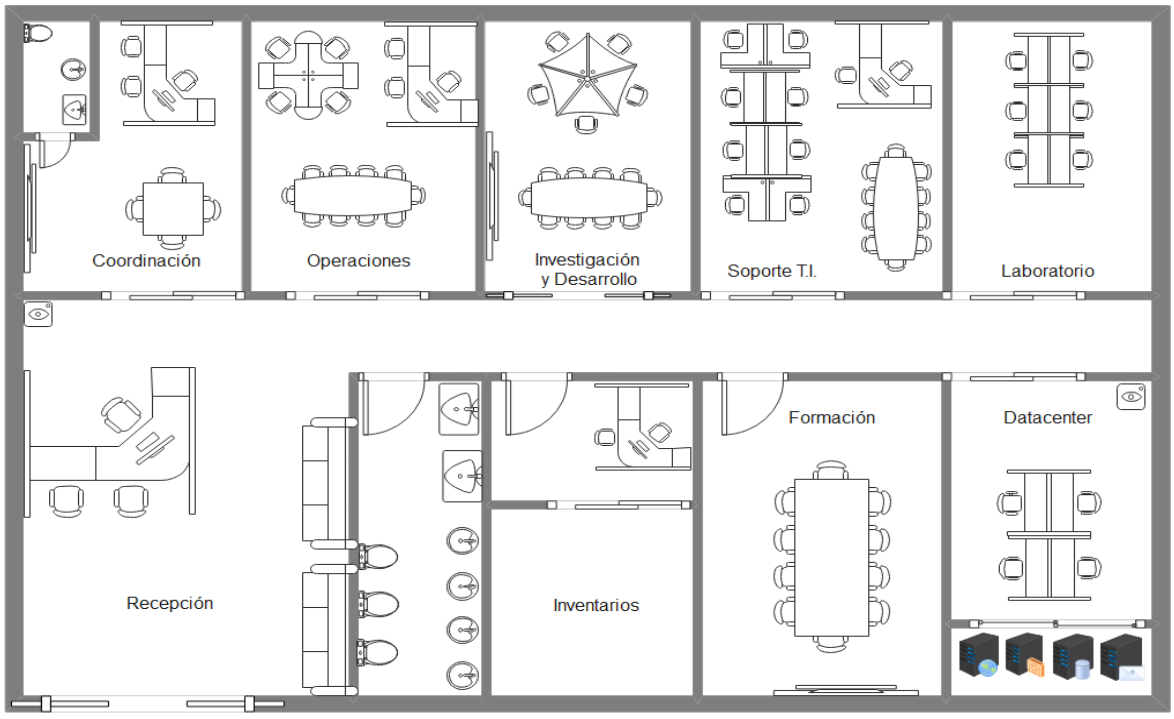
6.2.2 Distribución FÍSICA

El CSIRT, deberá tener unas áreas adecuadas para la correcta operación, entre ellas se debe disponer de las siguientes:

- Soporte de TI
- Operaciones
- Investigación y desarrollo
- Laboratorio
- Inventarios
- Sala de formación
- Centro de Datos
- Recepción
- Coordinación

A continuación, se expone en la Figura 12 la distribución física propuesta para el CSIRT.

Figura 12 Plano CSIRT

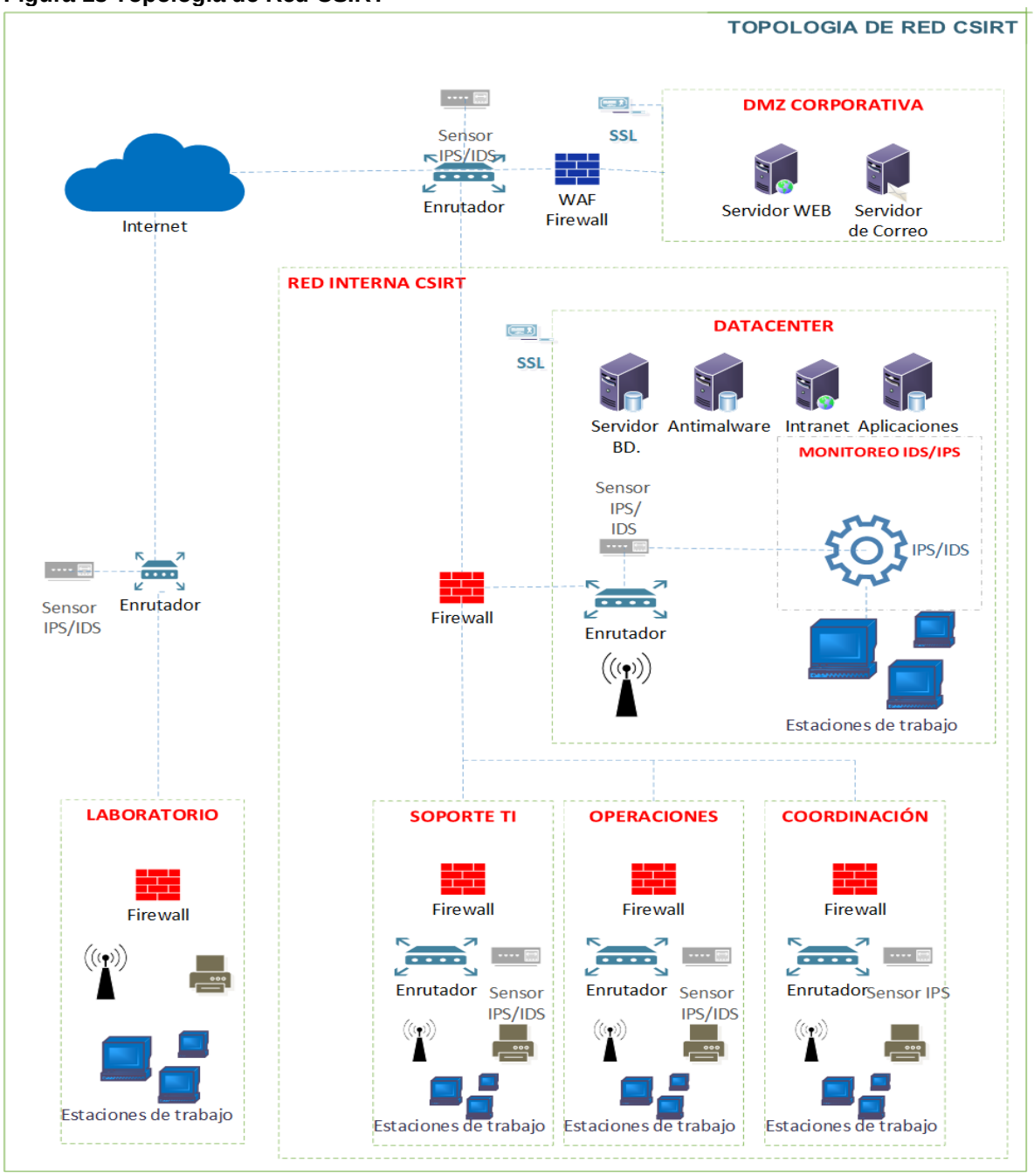


Fuente 15 elaboración propia con base en Manual de buenas prácticas CSIRT
https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

6.2.3 Diagrama de Red

El diagrama de red expuesto en la Figura 13, permite identificar una infraestructura de hardware básica necesaria para garantizar la operación del CSIRT

Figura 13 Topología de Red CSIRT



Fuente 16 elaboración propia

6.2.4 Procedimiento de Gestión de Incidentes y Análisis de Vulnerabilidades

La gestión de los incidentes, eventos y vulnerabilidades de seguridad de la información que atiende el CSIRT, exige que sea a través de un modelo eficiente que permita dar tratamiento adecuado a los reportes que se reciban, en el MSPI [21]y la GTC ISO /IE 27035 de 2012[22], Se plantea los siguientes pasos que serán necesarios para una adecuada gestión, tal como se presenta en la Figura 14.

Figura 14 Pasos para la Gestión de Incidentes

Fuente 17 elaboración propia con base en GTC-ISO-IEC 27035 de 2012

6.2.4.1 Detectar y contener

La etapa de detección y contención, es ejecutada a nivel de herramientas de software, capaces de detectar y contener incidentes de seguridad, también en esta etapa se debe considerar otros tipos de detecciones, como por ejemplo: la identificación de direcciones de correos electrónicos que están ejecutando ataques de phishing, números telefónicos ejecutando ataques de smishing o IP intrusas generando algún tipo de escaneo de vulnerabilidades, que asimismo deben ser identificadas y categorizadas. para la etapa de detección y contención, se debe contemplar las siguientes herramientas:

- Herramientas de detección y contención
    - Antivirus
    - IDS/IPS Sistemas de detección y prevención de intrusiones

[21] **MINTIC** [Sitio Web] Bogotá, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. , P. 9 [Consulta : 18 de julio 2021]. ,Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150509_G21_Gestion_Incidentes.pdf

[22] **ICONTEC,** Bogotá GTC 27035 -TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN , P. 4

- Analizadores de trafico de red
- Sistemas Hash

Una vez realizado el proceso de detección y contención, debemos documentar los incidentes a través herramientas help desk, que nos permita administrar la información de estos eventos e incidentes de seguridad, con el fin de que posteriormente aporte la información requerida. Para el análisis de esta clasificación se recomienda:

6.2.4.2 Categorizar y clasificar

Los incidentes deben ser clasificarlos con el fin de priorizar aquellos que generan un mayor impacto al sistema, de tal forma que las medidas de control que son inefectivas o ausentes, puedan ser fortalecidas o implementadas con la finalidad de que estas no se vuelvan a presentar, esta clasificación podría darse de la siguiente manera:

- Categoría del activo afectado
  - Software
  - Hardware
  - Servicios
  - Personas
- Clasificación de la incidencia:
  - Grave
  - Alta
  - Moderada
  - Baja

Es importante que dentro de la línea técnica la organización, se establezca la importancia de la clasificación, a fin de que no se quede en la subjetividad, teniendo en cuenta que, lo que se considera grave para una Organización, para otra podría ser moderada, no obstante, la organización podrá articular estas tipificaciones con el nivel de criticidad del (los) activo(s) de información afectado(s).

6.2.4.3 Eliminar

En esta fase o etapa se procede a eliminar la fuente generadora del riesgo, llámese virus, vulnerabilidad o cualquier situación que pueda comprometer la seguridad de la red y los datos, así las cosas, se debe proceder a establecer y realizar las acciones para las diferentes situaciones presentadas, sea la eliminación de un virus o bloqueo de un correo de ataques de phishing o alguna IP intrusa que este

ejecutando escaneo de vulnerabilidades, a manera de ejemplo se exponen las siguientes acciones:

- Bloquear direcciones de correo Phishing
- Bloquear números smishing
- Bloquear IP intrusas en el firewall
- Eliminar virus (Se recomienda hacer backup antes de realizar este proceso)
- Eliminar vulnerabilidades
- Eliminar permisos no autorizados

6.2.4.4 Analizar y reportar

El análisis y reporte de los incidentes y vulnerabilidades es muy importante para identificar el tamaño de la brecha de seguridad, en esta fase se deberá establecer Que sucedió, Como sucedió, Cuando y Porqué sucedió el incidente, luego de determinar la respuesta a estos cuestionamientos y registrar las medidas correctivas y preventivas, se deberá reportar los incidentes a aquellas instancias y/o partes interesadas, donde se exponen las situaciones de seguridad de la información, realizando las retroalimentaciones necesarias y recomendaciones a nivel de medios de comunicación interna y a los aliados que pueda interesar dicho análisis.

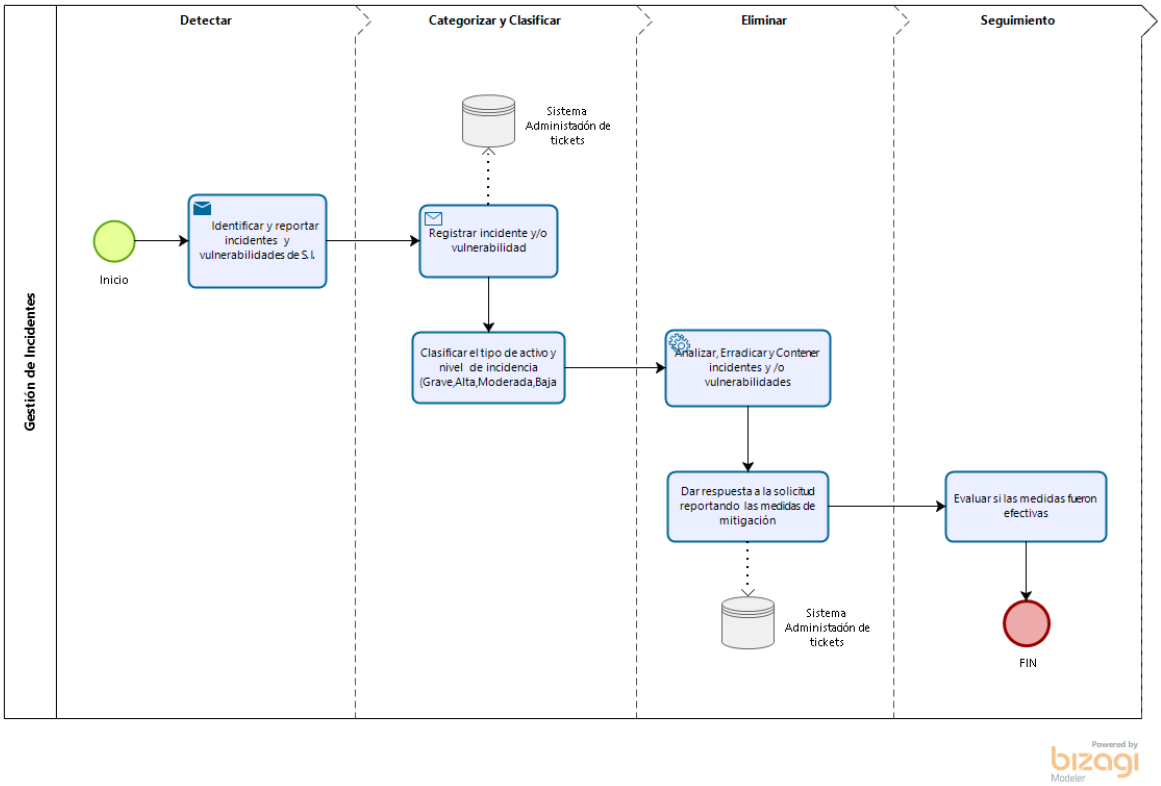
6.2.4.5 Hacer Seguimiento

El seguimiento de los incidentes y vulnerabilidades tratadas no debe dejarse de lado, pues es necesario efectuar evaluaciones periódicas de las medidas implementadas, a fin de que se pueda comprobar que dicha situación se ha controlado y no volverá a suceder. Si la organización lo considera puede incorporar en sus auditorías internas este tema, para optimizar los recursos que el seguimiento pueda acarrear.

6.2.4.6 Diagrama de Flujo

Es importante manejar un diagrama que describa de forma gráfica la secuencia de actividades para la atención de incidentes y vulnerabilidades, asimismo es importante divulgar la información a quienes son parte del procedimiento y en lo posible realizar actividades lúdicas para la apropiación de conceptos y adherencia al procedimiento, procurando que todos sus actores tengan el conocimiento previo de que hacer, cuando y donde en el momento de que se presenten, a continuación se presenta el flujo del procedimiento en la Figura 15.

Figura 15 Flujograma



Fuente 18 elaboración propia

6.3 FASE III IMPLEMENTACIÓN DE HERRAMIENTAS DE GESTIÓN DE INCIDENTES Y ANÁLISIS DE VULNERABILIDADES EN AMBIENTES CONTROLADOS

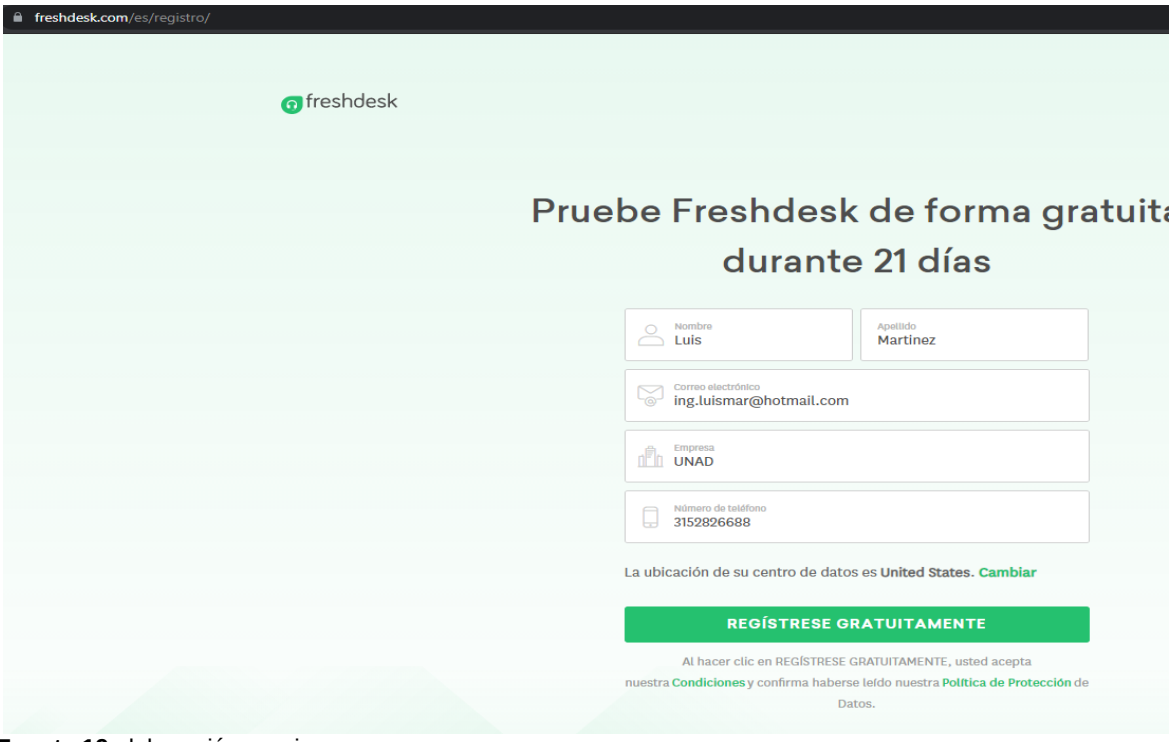
El escalamiento de los incidentes y vulnerabilidades será prioritario para el centro de respuesta CSIRT, cada profesional realiza funciones particulares, que deben ser escaladas de forma organizada, a través de un sistema que le permita a la organización administrar los casos que sean reportados, permitiendo una correcta administración de los casos que demanden al equipo de respuesta CSIRT.

6.3.1 Configuración del Sistema para la Gestión de Incidentes

Es importante contar con una herramienta para la administración y control de los incidentes en el CSIRT, de esta manera se podrán recibir, administrar y escalar los incidentes de seguridad que se reporten, para el caso práctico se expone a continuación la implementación del sistema Freshdesk, la implementación de este sistema procede a través del siguiente enlace https://Freshdesk.com/es/ donde se

registran los datos del administrador de casos del CSIRT a través de una cuenta de correo electrónico, como se expone en la Figura 16

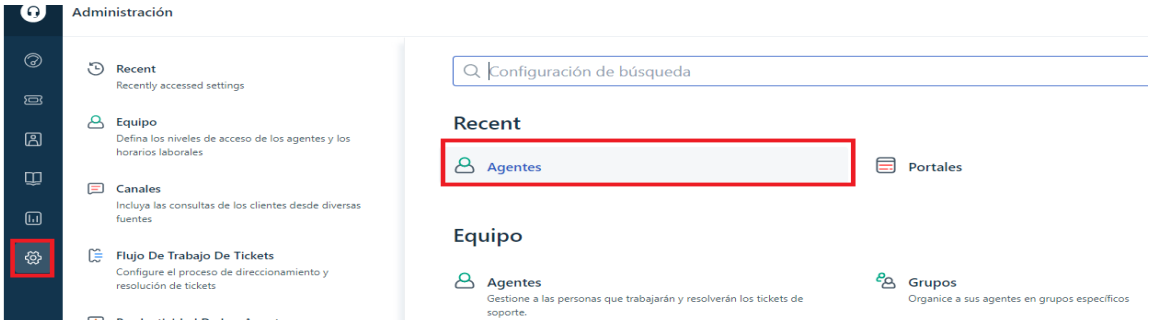
Figura 16 Registro Freshdesk



Fuente 19 elaboración propia

Se ingresa en la opción admin y luego en el icono de agentes, con el fin de poder configurar los roles del CSIRT correspondientes a la estructura del equipo de respuesta, tal como se puede apreciar en la Figura 17.

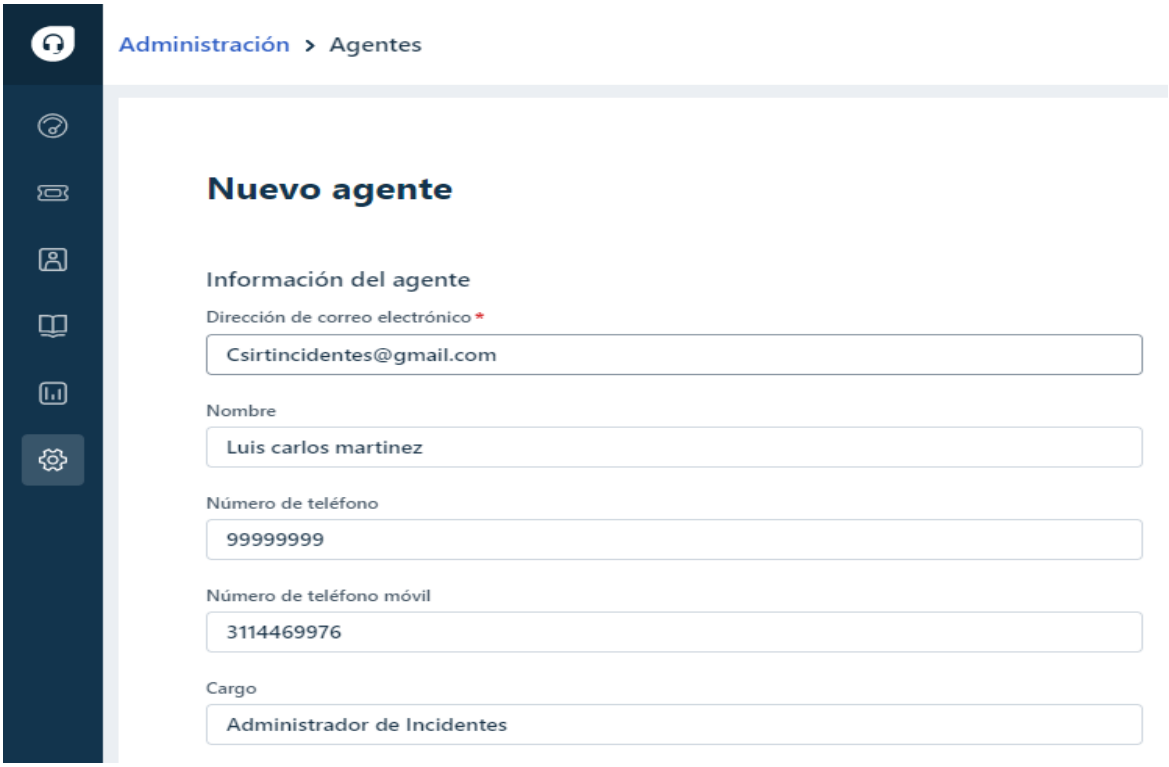
Figura 17 Creación de agentes Freshdesk



Fuente 20 elaboración propia

Se crean los roles vistos en la estructura del CSIRT, registrando los campos del formulario nuevo agente, asignando los correos respectivos, como se expone en la Figura 18.

Figura 18 Creación de Nuevo Agente Freshdesk

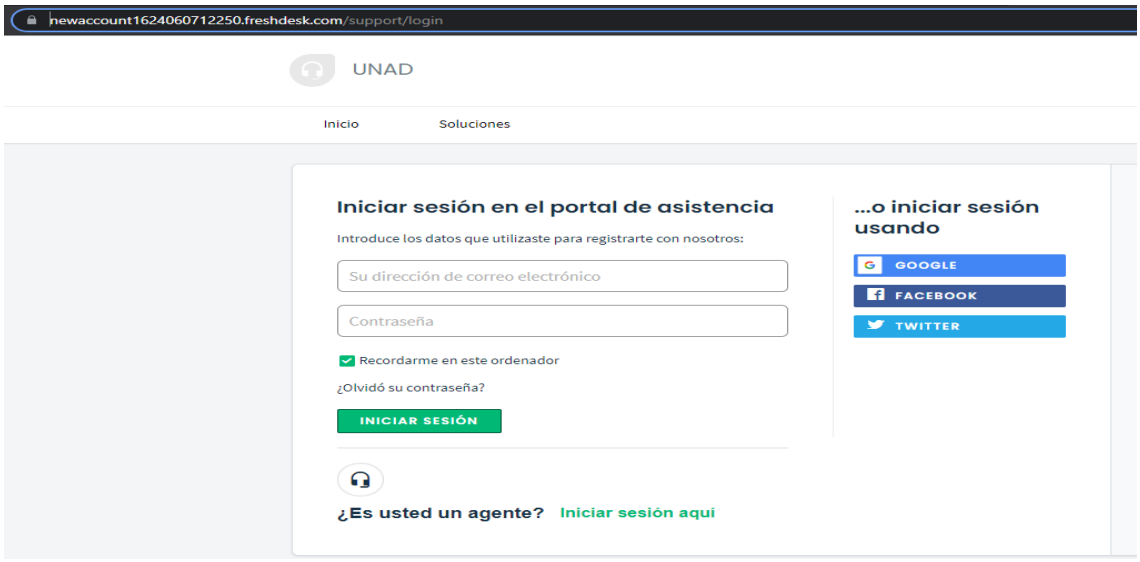


Fuente 21 elaboración propia

Una vez configurados los agentes, se guarda el enlace del sitio creado para el portal helpdesk y se remite a los usuarios de los perfiles creados para que puedan acceder, quienes visualizarán el acceso de la aplicación como se expone en la Figura 19 y 20.

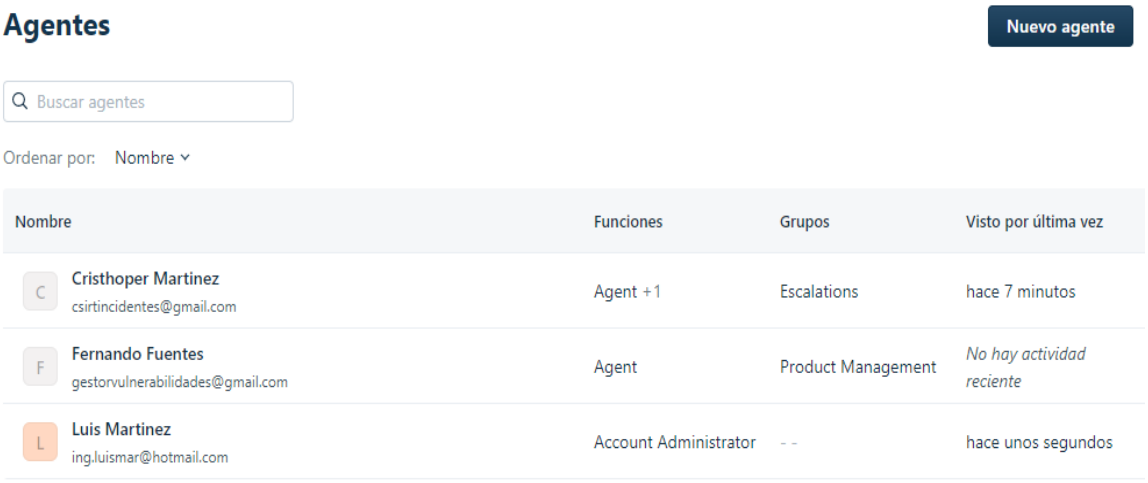
https://newaccount1624060712250.Freshdesk.com/support/login

Figura 19 Inicio de Sesión Freshdesk



Fuente 22 elaboración propia

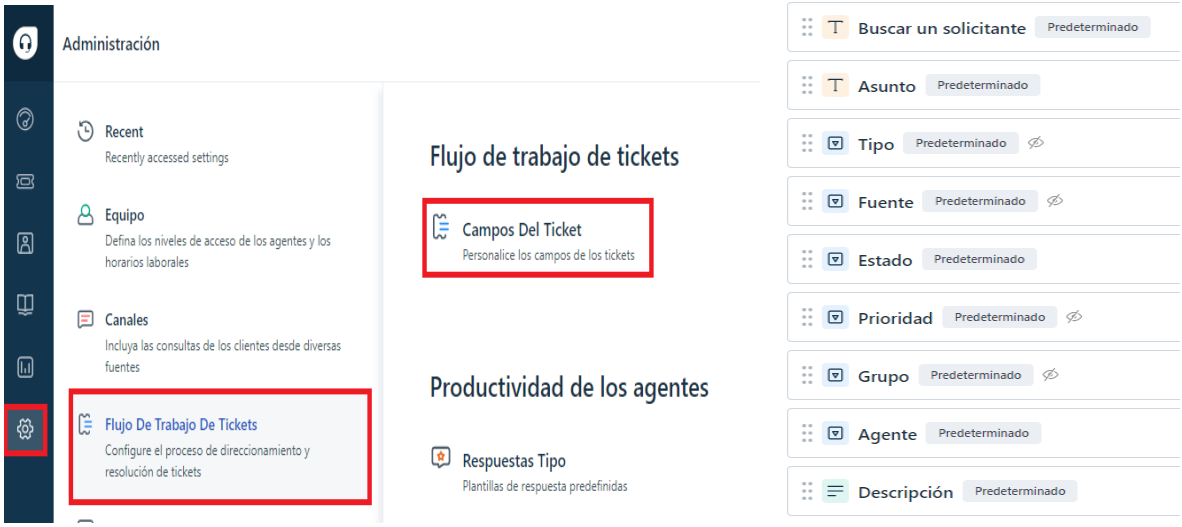
Figura 20 Listado de Agentes



Fuente 23 elaboración propia

Una vez creados los usuarios que soportarán el CSIRT, se deberán configurar los tipos de servicios administrados, la herramienta Freshdesk, permite incorporar los tipos de incidentes desde la opción admin/ Flujo de Trabajo De Tickets/Campos del Ticket, como se puede apreciar en la Figura 21.

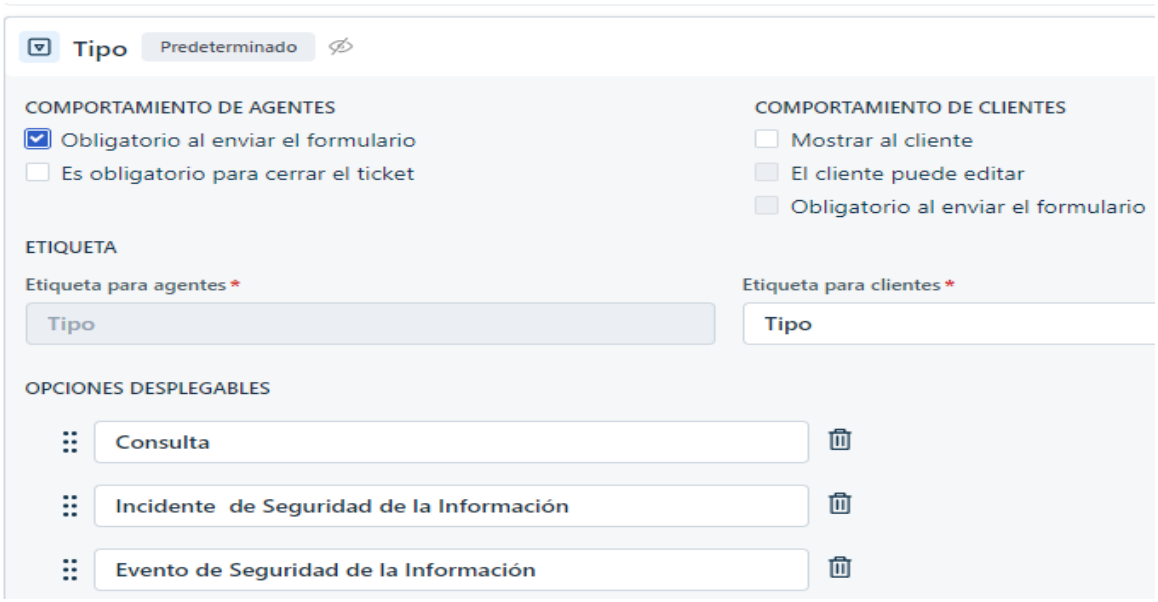
Figura 21 Configuración de Ticket Freshdesk



Fuente 24 elaboración propia

Seleccionando la opción tipo, se parametriza las clases de reporte que administra el CSIRT. Para el caso del ejemplo se crean Consulta, Incidente de Seguridad de la Información y Evento de Seguridad de la Información, como se expone en la Figura 22.

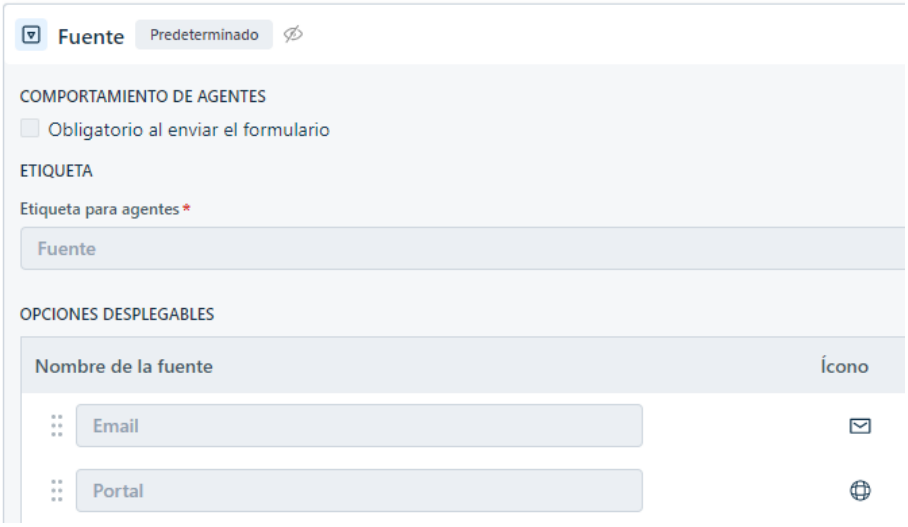
Figura 22 Parámetros tipo de soporte



Fuente 25 elaboración propia

En la opción fuente, se expone los pasos de configuración de los canales por donde se recibirán los casos, esta opción es parametrizable de acuerdo a los lineamientos establecidos en el CSIRT, como se puede apreciar en la Figura 22.

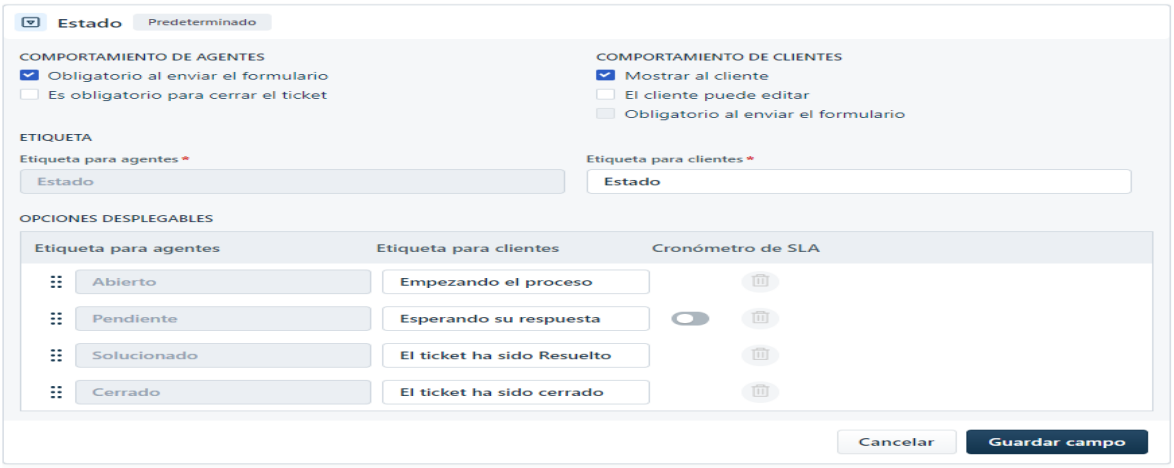
Figura 23 Configuración de canales de atención



Fuente 26 elaboración propia

Es importante dar a conocer el estado de los casos a los usuarios y también realizar seguimiento a los mismos, la herramienta Freshdesk, permite esta parametrización en el campo estado, como se expone en la Figura 24.

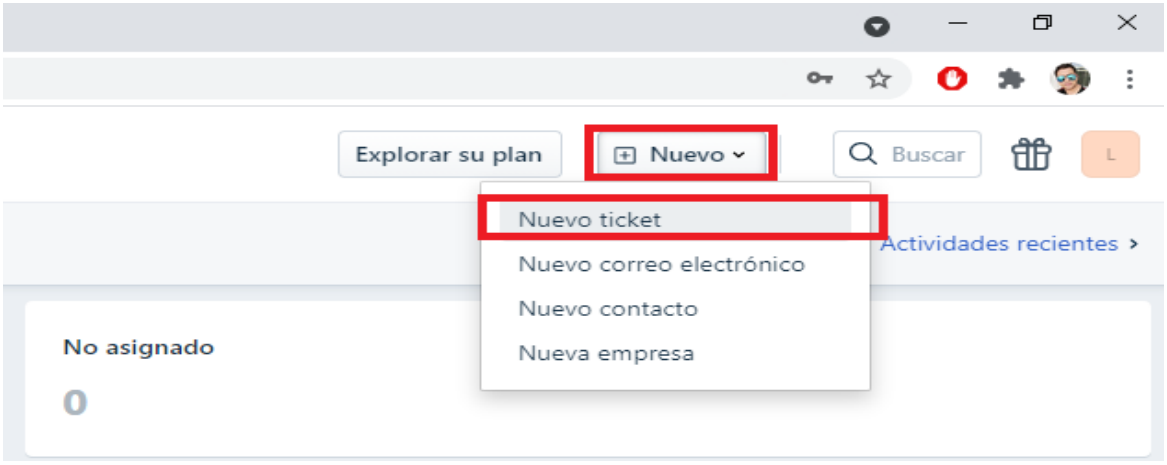
Figura 24 Estados de Caso



Fuente 27 elaboración propia

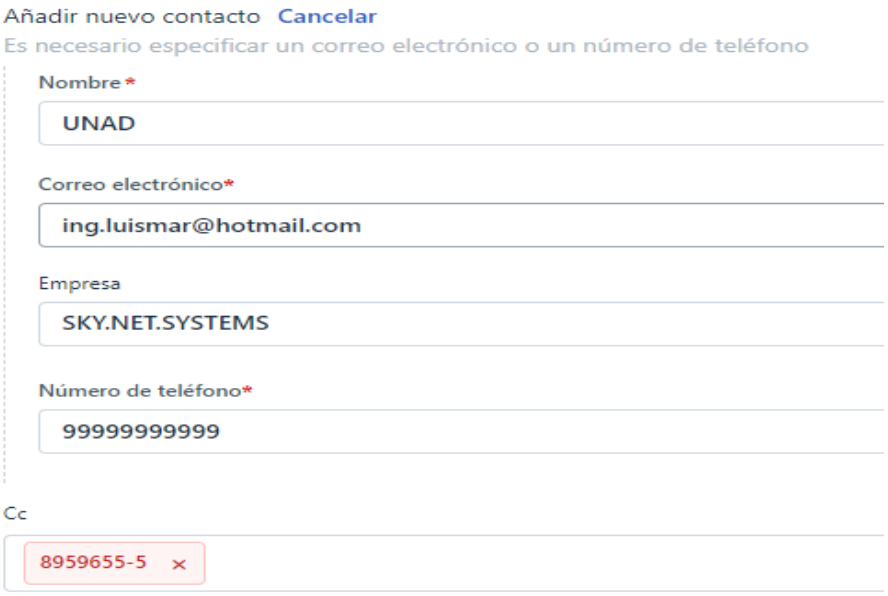
Una vez parametrizado el sistema, creados los roles que administrarán los casos del CSIRT y dispuestos los tipos de incidentes que gestionarán, se disponen los agentes que recibirán y clasificarán los casos, a continuación, se expone la creación de un caso para el CSIRT en las Figuras 25 a la 28.

Figura 25 Creación Ticket



Fuente 28 elaboración propia

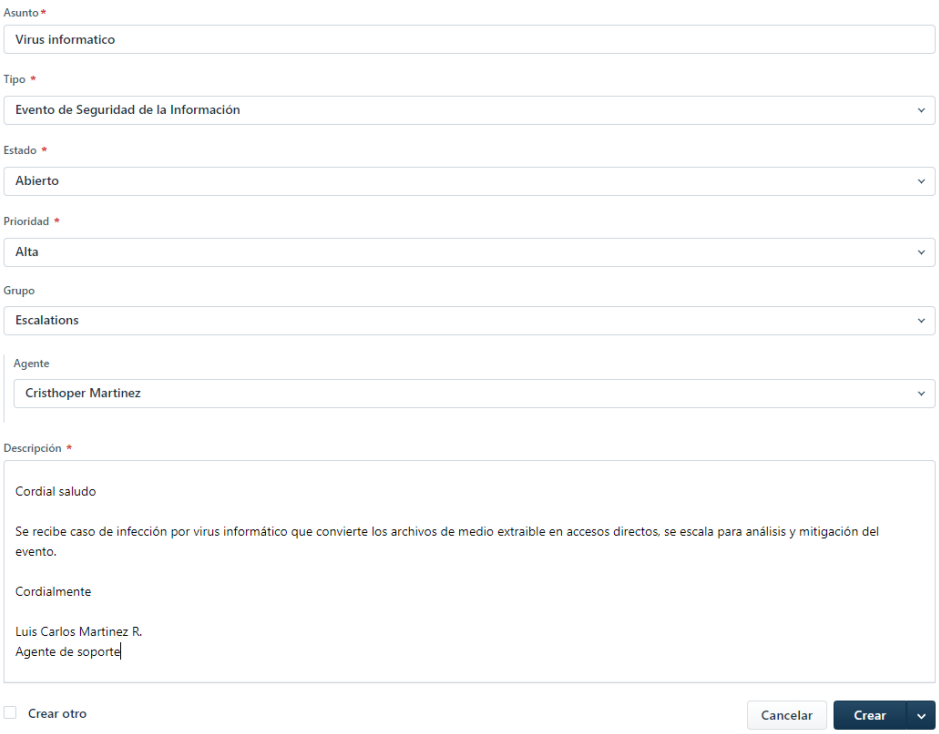
Figura 26 Registro de contacto del caso



Fuente 29 elaboración propia

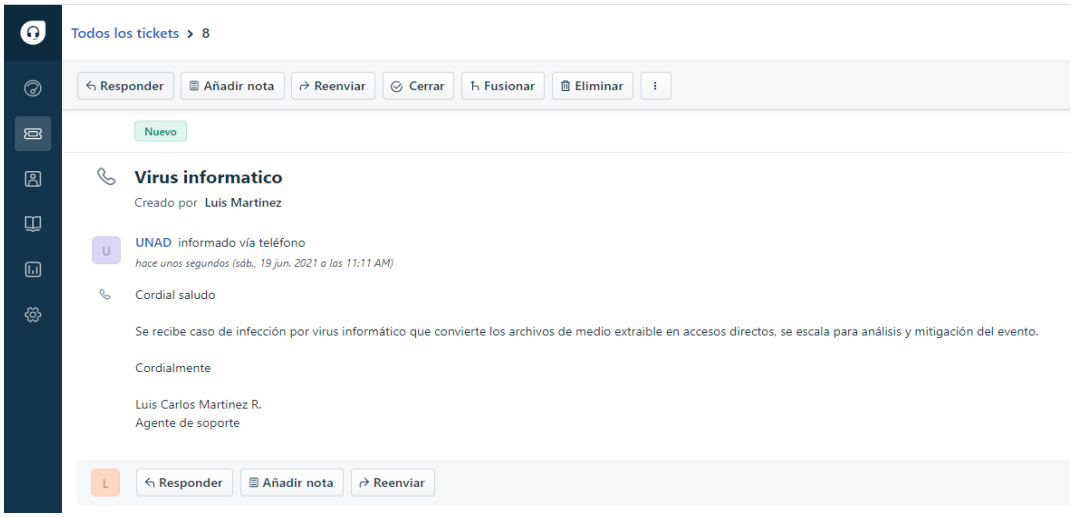
Se registra los datos del caso, precisando que los campos en * son obligatorios, por lo que se deberán registrar como se presenta en la Figura 27 y 28.

Figura 27 Registro de Caso



Fuente 30 elaboración propia

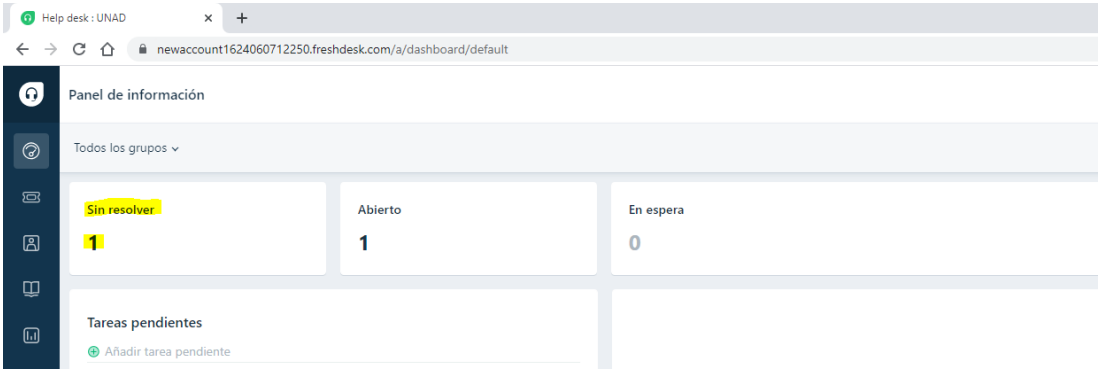
Figura 28 Creación del Ticket



Fuente 31 elaboración propia

Se verifica en el panel de información el número de casos abiertos sin respuesta, en el cual, los agentes de la operación podrán realizar el seguimiento, así como también, el Líder del CSIRT, la plataforma incluye otras funcionalidades en su versión free, como la fusión de casos, notificación de las alertas a correo electrónico, entre otros, a continuación, se expone la interfaz de reportes de estado de los casos de la aplicación en la Figura 29.

Figura 29 Reporte de Estado de Casos Freshdesck



Fuente 32 elaboración propia

Para dar respuesta a la solución del caso, el analista al que se realizó el escalamiento, podrá ingresar desde su usuario a la opción sin resolver y allí podrá dar respuesta al evento reportado, cambiando el estado solo sí el usuario ha confirmado que el caso fue solucionado, tal como se observa en la Figura 30.

Figura 30 Respuesta de caso

Fuente 33 elaboración propia

6.3.2 Análisis de vulnerabilidades y metodologías

Los análisis de vulnerabilidades se ejecutan a través de herramientas especializadas, que permiten realizar análisis exhaustivos para identificar vulnerabilidades y poderlas corregir antes de que sean aprovechadas por la ciberdelincuencia, asimismo existen marcos de referencia que van un poco más allá del análisis, donde se culmina con la explotación de la vulnerabilidad denominados pentesting, el CSIRT podrá aplicar o no este tipo de métodos de acuerdo a las necesidades de la organización, todos estos marcos de referencia tienen un factor diferencial que permite inclinarse al que más se adecue a la infraestructura tecnológica de la organización, dentro de los más conocidos podemos referenciar las siguientes:

OWASP: Definido como el "Proyecto Abierto de Seguridad En Aplicaciones Web"[23], Es un estándar de aplicaciones, el cual fue desarrollado por una fundación sin ánimo de lucro, conformada por una comunidad de ingenieros y diferentes expertos que se unieron para aportar sus conocimientos, a tal punto que hoy se ofrece un compendio de herramientas, estándares y otros contenidos en materia de seguridad de aplicaciones web, para que todo aquel que se encuentre interesado en asegurar sus desarrollos y aplicaciones web, puedan tener las herramientas necesarias para hacerlo.

Dentro de las herramientas más conocidas en OWASP se presenta el marco de referencia denominado TOP 10 de OWASP, este instrumento fue elaborado producto de un análisis de riesgos, en donde se evaluó las vulnerabilidades más comunes, fáciles de explotar y con mayor grado de impacto en las organizaciones, de esta manera se prioriza y ordena de forma organizada aquellos riesgos que deben ser mitigados, determinando el primero como el más probable y de mayor impacto, Esta metodología se enfoca en la seguridad digital.

OSSTMM: Se le llama Manual de Metodologías de Pruebas de Seguridad de Código Abierto [24], los derechos de la propiedad intelectual de esta metodología le pertenecen a ISECOM y desarrollada por Pete Herozq, su propósito es identificar vulnerabilidades, para determinar el estado de la seguridad y posteriormente implementar las medidas que permitirán fortalecer sus esquemas, esta metodología propone 7 pasos para su despliegue y su enfoque es la seguridad física.

NIST: Es el marco de ciberseguridad para infraestructuras críticas, el cual fue elaborado por el Instituto Nacional de Estándares y Tecnologías establecido en

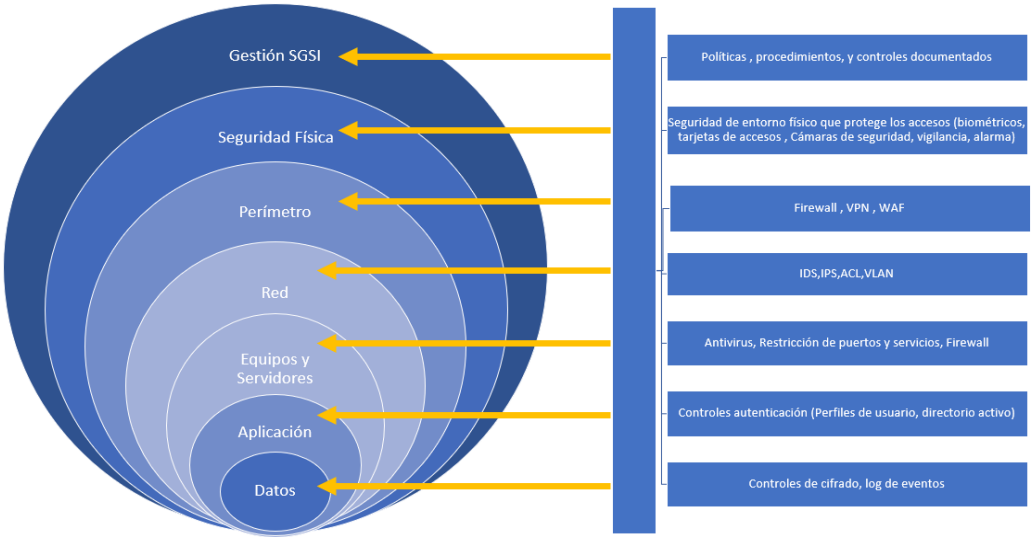
[23] **OWASP TOP 10 2017** Los diez riesgos más críticos en aplicaciones web Disponible en: https://owasp.org/www-pdf-archive/OWASP-Top-10-2017-es.pdf

[24] **INSTITUTO DE SEGURIDAD Y METODOLOGIAS ABIERTAS** [Sitio Web] Barcelona ISSECOM Manual de metodología de pruebas de seguridad de código abierto , [Consulta : 19 de junio 2021]. ,Disponible en: https://www.isecom.org/research.html#content5-9d

Estados Unidos, este marco prioriza los sectores críticos que en todo gobierno son sensibles por su naturaleza, el marco establece 16 sectores en los cuales se incluye el sector salud, financiero, comunicaciones, químico, sistemas de transporte entre otros, la abreviatura como se le conoce es CSF o (Cibersecurity Frameworks), se estructura a través de 3 componentes, Framework Core, Niveles de Implementación y perfiles. su Core se centra en 5 actividades principalmente que son: Identificar, Proteger, Detectar, Responder y Recuperar[25].

Es pertinente que el centro de respuesta a incidentes CSIRT, tenga un panorama general de la infraestructura tecnológica de la entidad y un conocimiento de las áreas, ubicaciones y activos de información, donde identificar las vulnerabilidades de seguridad para poderlas intervenir, para este análisis, el equipo deberá reconocer las debilidades y fortalezas de su sistema defensivo, en el cual se recomienda hacer uso de la metodología de defensa en profundidad[26], la cual permitirá orientar al equipo donde identificar los controles de seguridad existentes o ausentes de la organización y asimismo los que deberían encontrarse implementados, a continuación se presenta en la Figura 31 el esquema de defensa en profundidad con algunos de los controles relacionados

Figura 31 Defensa en Profundidad



Fuente 34 elaboración propia

[25] **INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGIAS** [Sitio Web] NIST Cibersecurity Framework CSF , P. 4-6 [Consulta : 19 de junio 2021]. ,Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

[26] **Escrivá Gascó G.** Seguridad informática [En Línea]. Madrid: Macmillan Iberia, S.A. 2013 [consultado 26 Jul 2021]. P.175 - 216 Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=1

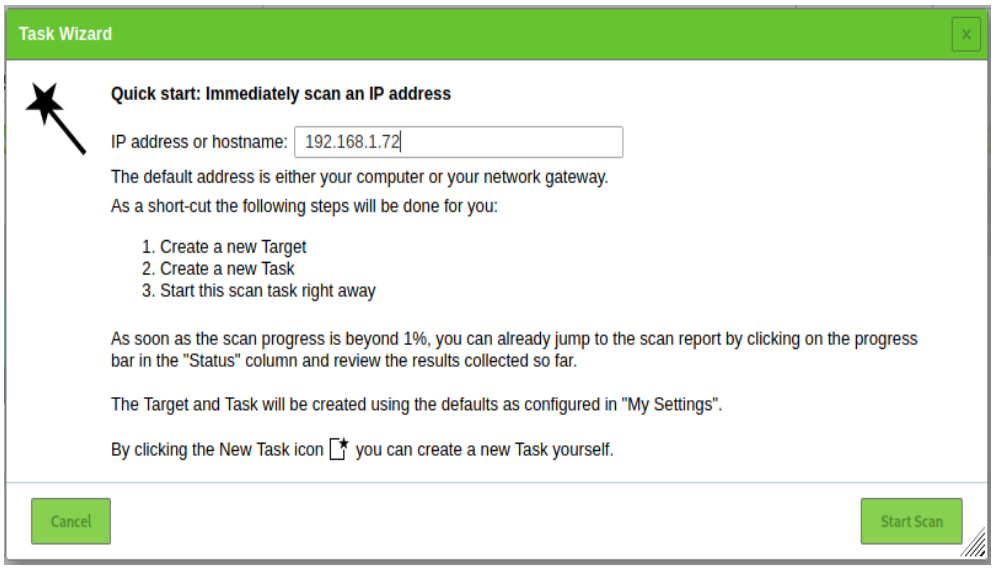
Las vulnerabilidades se pueden consultar en el organismo de regulación de vulnerabilidades llamado mitre, el cual mantiene una relación con los proveedores de software, que de lograrse comprobar la misma, será publicada en la base de datos del sitio web asignándose un CVE y especificando sus características en dicha publicación. Las vulnerabilidades se publican en la url https://cve.mitre.org/ , asimismo, existen otras páginas web donde es posible consultarlas, entre ellas se encuentra https://nvd.nist.gov/ y https://www.details.com.

6.3.3 Análisis con Openvas

El CSIRT debe determinar y aplicar las herramientas especializadas para el análisis de vulnerabilidades, sus opciones pueden ser aplicaciones de pago como Nessus o su antecesor Openvas de *Open Source,* OPENVAS(Escáner de Evaluación de Vulnerabilidad Abierta)[27] Es una aplicación reconocida por los pentester para ejecutar operaciones de análisis de vulnerabilidades, permite realizar escaneo de la red, puertos, seguridad de aplicaciones web y bases de datos, asimismo identifica las vulnerabilidades las confronta con su base de datos y brinda las posibles soluciones que se requieran para la eliminación de vulnerabilidades identificadas.

A continuación, se expone a manera de ejemplo la operación del software Openvas sobre una máquina Metaisplotable 3, que permite identificar algunas vulnerabilidades encontradas como un ejercicio exploratorio, para adentrarnos en las labores del CSIRT, como se aprecia en la Figura 32 y 33.

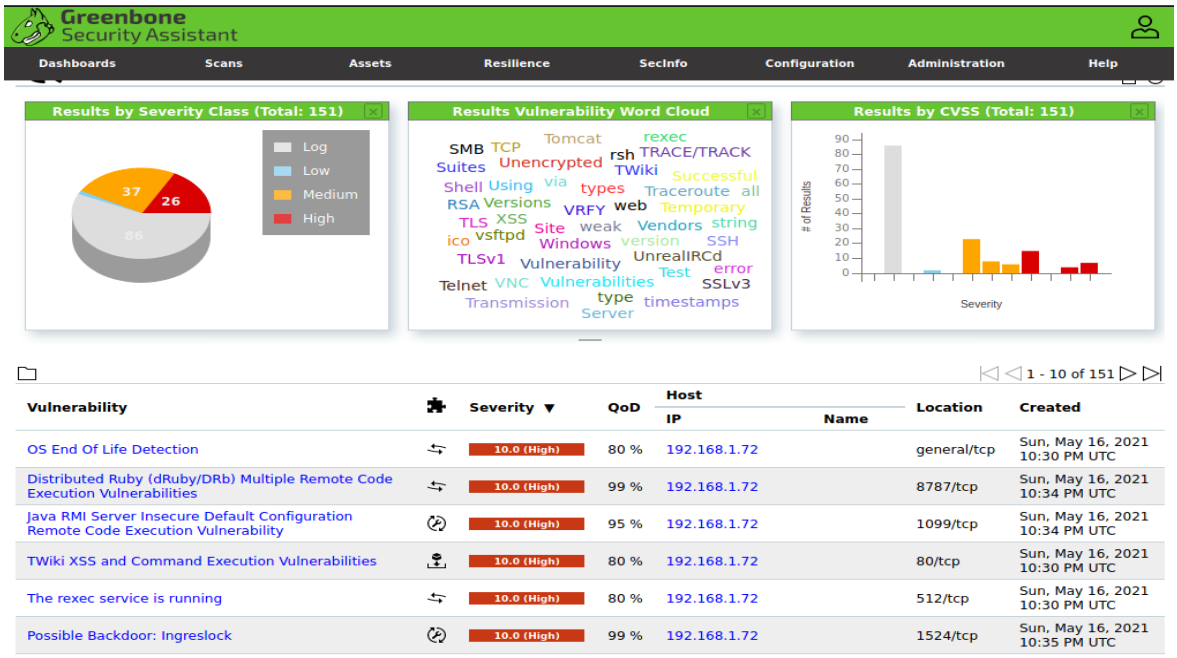
Figura 32 Registro IP para escaneo en Openvas



Fuente 35 Elaboración propia

[27] **GREENBONE, OpenVAS** - Escáner de evaluación de vulnerabilidad abierta [Sitio Web] Osnabrück 19 de mayo 2021,Disponible en: https://www.openvas.org/

Figura 33 Reporte de vulnerabilidades Openvas



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
OS End Of Life Detection	10.0 (High)	80 %	192.168.1.72		general/tcp	Sun, May 16, 2021 10:30 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.1.72		8787/tcp	Sun, May 16, 2021 10:34 PM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.1.72		1099/tcp	Sun, May 16, 2021 10:34 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.1.72		80/tcp	Sun, May 16, 2021 10:30 PM UTC
The rexec service is running	10.0 (High)	80 %	192.168.1.72		512/tcp	Sun, May 16, 2021 10:30 PM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.1.72		1524/tcp	Sun, May 16, 2021 10:35 PM UTC

Fuente 36 Elaboración propia

Una vez identificadas las vulnerabilidades más críticas que lista el software, se debe proceder con la mitigación de las mismas, esta herramienta provee acciones de mitigación basadas en la lista de CVE , a continuación, se listan las vulnerabilidades , ataques asociados, causas e impacto y solución expuestas en la Tabla 4.

Tabla 4 Análisis de vulnerabilidades

Vulnerabilidad	Ataque Asociado	Causa	Impacto	Mitigación
Os End Life Detection	Ataque de script y o exploit que al ser ejecutado recopila información sobre el sistema operativo	Fin de la vida útil del sistema operativo, no recibirá más actualizaciones sobre las vulnerabilidades nuevas por el proveedor	El atacante podría tomar control del equipo eliminar información o dejarlo inutilizable.	Esta vulnerabilidad se mitiga realizando un upgrade en el sistema operativo Ubuntu que presenta la vulnerabilidad.
Possible Backdoor: Ingreslock	Ataque de Exploit Este ataque instala una puerta en el host remoto, en el cual permitiría la ejecución de algunos comandos que ejecutarían acciones no autorizadas.	Problema de seguridad asociado al puerto 1524/TCP el cual se utiliza como puerta trasera por software que explotan servicios RPC.	Obtención de accesos con privilegios al atacante.	Para mitigar esta acción se requiere realizar limpieza de todo el sistema con un antivirus actualizado.

Java RMI Sever Insecure Default ConFiguration Remote Code Execution Vulnerability	Ataque de Exploit Permite cargar clases desde cualquier URL remota.	Falla de Configuración predeterminada del servidor RMI Java	Este tipo de ataque brinda acceso no autorizado a los privilegios del servidor o equipo.	Esta vulnerabilidad generada en servicios de JAVA, es subsanable deshabilitando la carga de clases.
TWiki XSS and command Execution Vulnerabilities	Croos-site Scripting XSS, ataque de secuencia de comandos que de ejecutarse puede suministrar acceso a las contraseñas de los usuarios a través de las cookies comprometiendo la seguridad de la información	la variable% URLPARAM {}% no se desinfecta adecuadamente	Acceso no autorizado a los privilegios del servidor o equipo, riesgo de pérdida de confidencialidad integridad y disponibilidad.	Esta vulnerabilidad se mitiga actualizando la aplicación a una versión 4.2.4 o mayor.
The rexec service is running	Ataque de Exploit	El servicio rexec se está ejecutando	Permite al atacante ejecutar comandos en Shell desde un equipo remoto generando malfuncionamiento del sistema y cierre total del equipo afectado, perdida de integridad	Esta vulnerabilidad se puede identificar en la CVE-1999-0618, y detecta que se está ejecutando un servicio rexec, su mitigación está en la desactivación del mismo

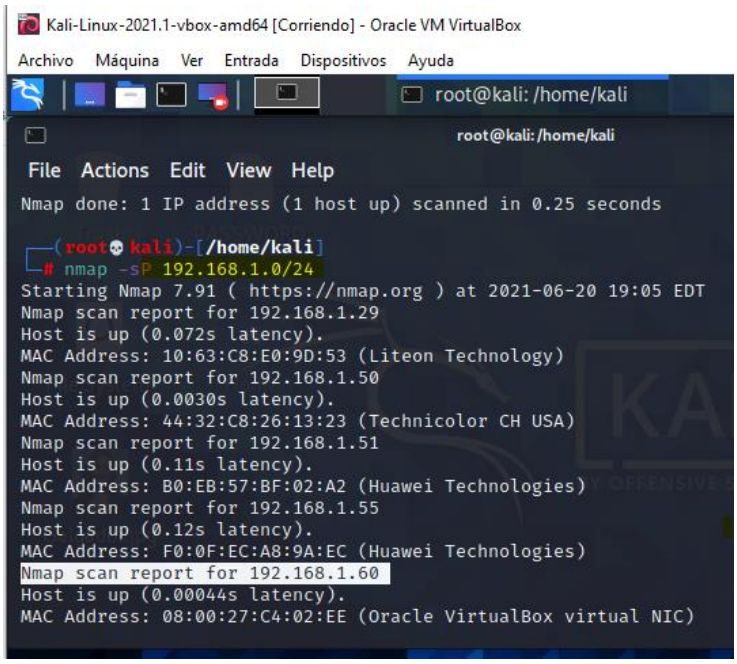
Fuente 37 elaboración propia con base en la información del software Open Vas

6.3.4 Análisis con NMAP

Los análisis de vulnerabilidades parten de la obtención de la mayor cantidad de información que nos pueda proveer una infraestructura tecnológica, pues entre mayor información se obtenga, mayor será el riesgo de ser explotada una vulnerabilidad. Por ejemplo, mantener el servicio web en el mismo puerto predeterminado se podría considerar dentro de los parámetros normales en una organización, no obstante, esta práctica es un error critico de las organizaciones, pues es fácil atacar lo que siempre encontramos en un mismo lugar, a continuación se expone un ejercicio práctico, donde se realizará el escaneo de la red con nmap, para identificar una IP objetivo que corresponde a una máquina metaisplotable y luego lanzaremos un escaneo de puertos.

A través del comando nmap 192.168.1.0/24 se identifican todas las IP que se encuentran en la red interna y se selecciona una de ellas como se observa en la Figura 34.

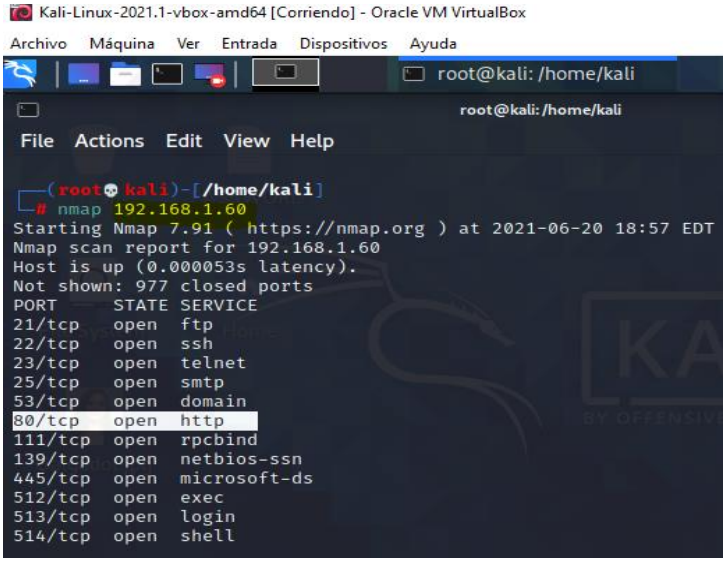
Figura 34 Escaneo de IPS en Terminal Linux



Fuente 38 elaboración propia

Luego de haber identificado la IP que se analizará, se ejecuta el comando nmap 192.168.1.60, para obtener información de los puertos abiertos, identificándose el puerto 80 abierto y configurado para el servicio web http y el ssh en el puerto 22 entre otros, como se observa en la Figura 35.

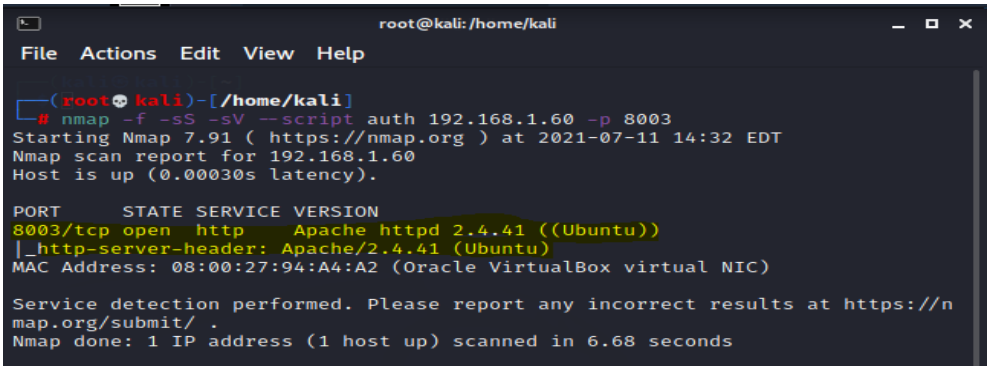
Figura 35 Escaneo de Puertos Nmap



Fuente 39 elaboración propia

Otro de los scripts convencionales para el análisis de vulnerabilidades conocido del sistema NMAP, es el nmap -f –script vuln + IP, este script ejecuta un escaneo de los puertos abiertos y servicios de una máquina con IP conocida, en la cual también podrá reconocer las vulnerabilidades e información, como la versión de apache, la MAC address entre otros, como se presenta en la Figura 36.

Figura 36 Escaneo de Vulnerabilidades NMAP



Fuente 40 elaboración propia

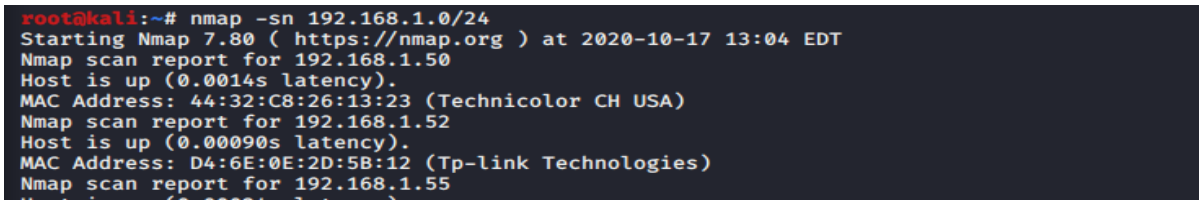
6.3.5 Análisis con Wireshark

El CSIRT tendrá a cargo dentro de sus funciones, realizar análisis de tráfico de red con el fin de detectar intrusiones de seguridad, a través de la herramienta Wireshark se podrá realizar dicho análisis, permitiendo un seguimiento en tiempo real de todos los paquetes y protocolos que transitan por la red de datos.

A continuación, se realiza un escaneo de puertos con la herramienta NMAP y asimismo se pone en funcionamiento Wireshark con el fin de detectar el evento.

En modo root se ejecuta el comando nmap sn- 192.168.1.0/24 para escanear los equipos conectados a la red, con el fin de identificar una máquina objetivo. en el escaneo se logra identificar diferentes IP conectadas a la red, como se puede observar en la Figura 37.

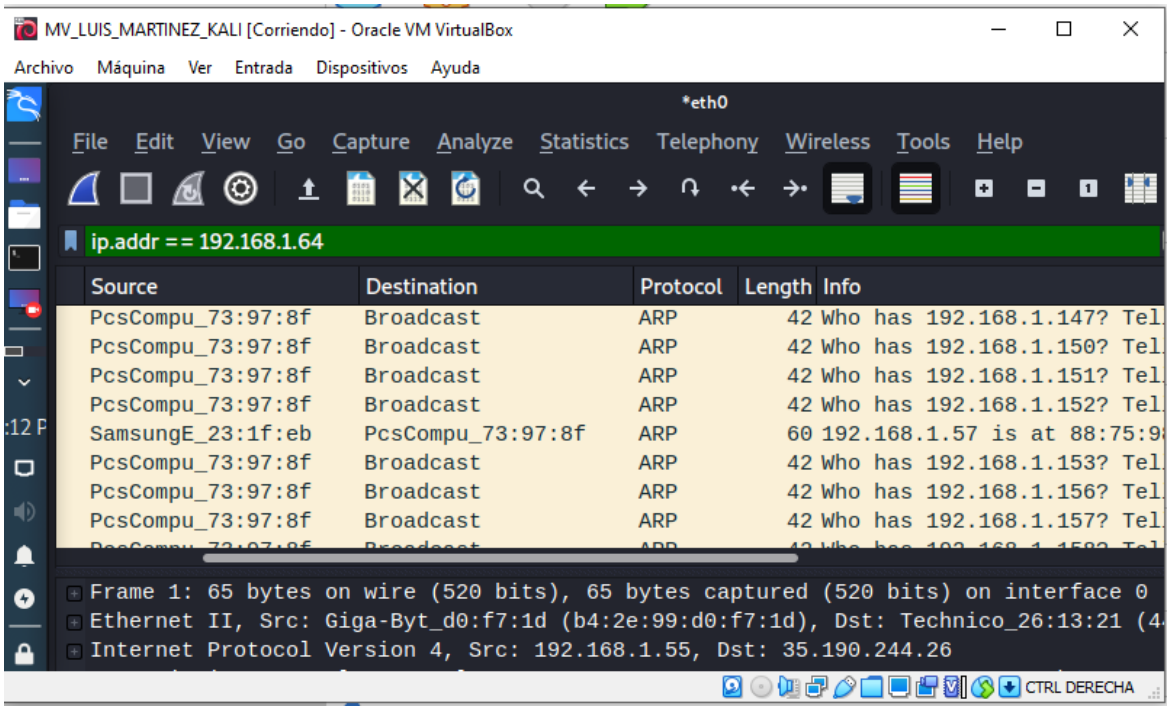
Figura 37 Escaneo NMAP



Fuente 41 elaboración propia

Simultáneamente se encuentra operando el sistema de detección de intrusos Wireshark, el cual automáticamente detecta tráfico del protocolo ARP, que usualmente suele utilizar el router para identificar los equipos conectados a la red, como se muestra en la Figura 38.

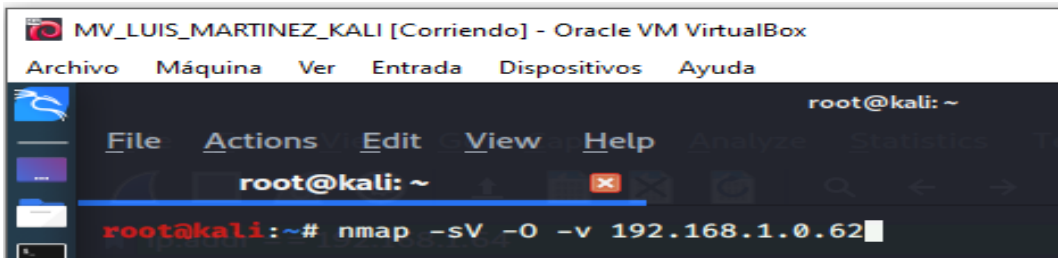
Figura 38 Análisis Wireshark Protocolo ARP



Fuente 42 elaboración propia

Una vez identificada una IP objetivo por NMAP, es ejecutado el comando nmap -Sv -O -v 192.168.0.62, con el fin de conocer el sistema operativo que maneja el equipo, mientras Wireshark continúa activo y en alerta, como se observa en la Figura 39.

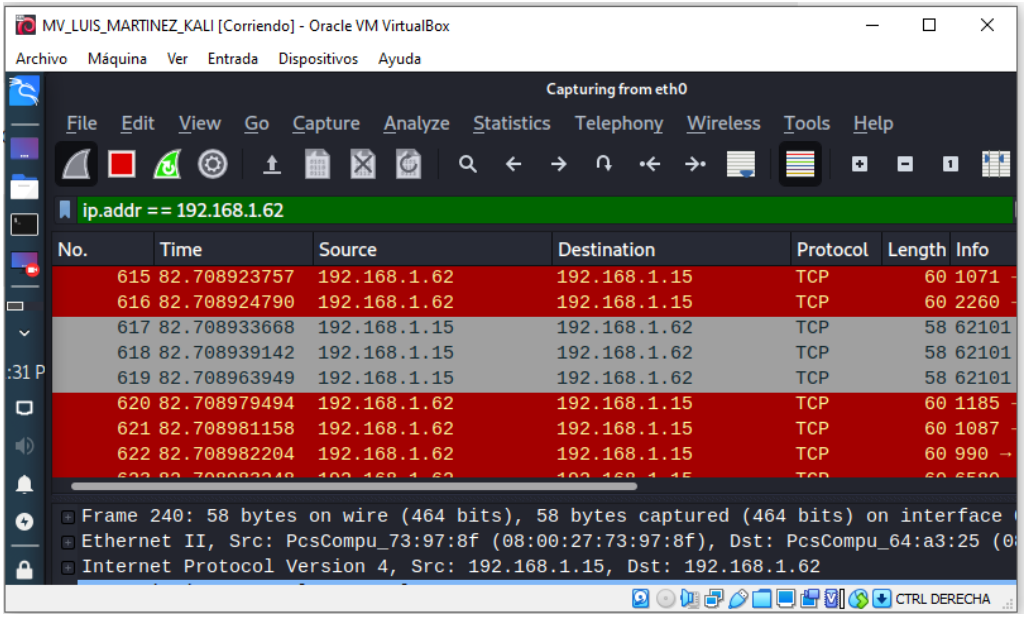
Figura 39 Escaneo de Versión S.O. Nmap



Fuente 43 elaboración propia

El sistema Wireshark detecta automáticamente protocolo TCP, proveniente de la IP del atacante, que se identifica con la IP 192.168.1.62, como se observa en la Figura 40.

Figura 40 Detección Wireshark

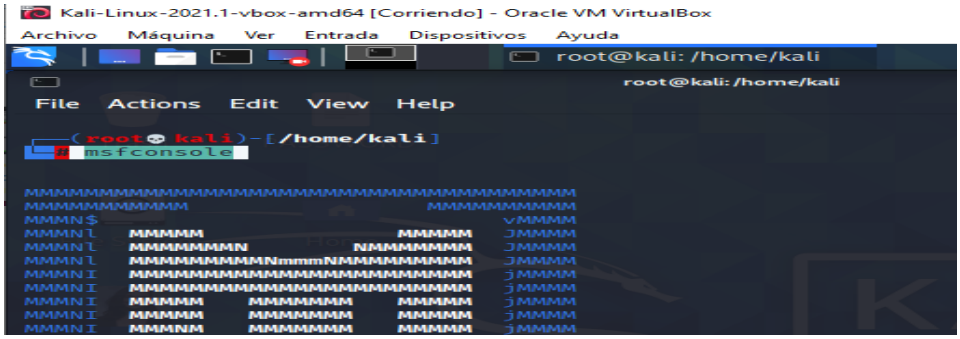


Fuente 44 elaboración propia

6.3.6 Análisis con Metaesploit

Con Metaesploit es posible explotar vulnerabilidades para acceder al control remoto de una máquina, como parte práctica se expone a continuación una prueba de vulnerabilidad de conexión remota a través de metaexploit, en la cual se inicia la aplicación a través del comando mfconsole, como se observa en la Figura 41.

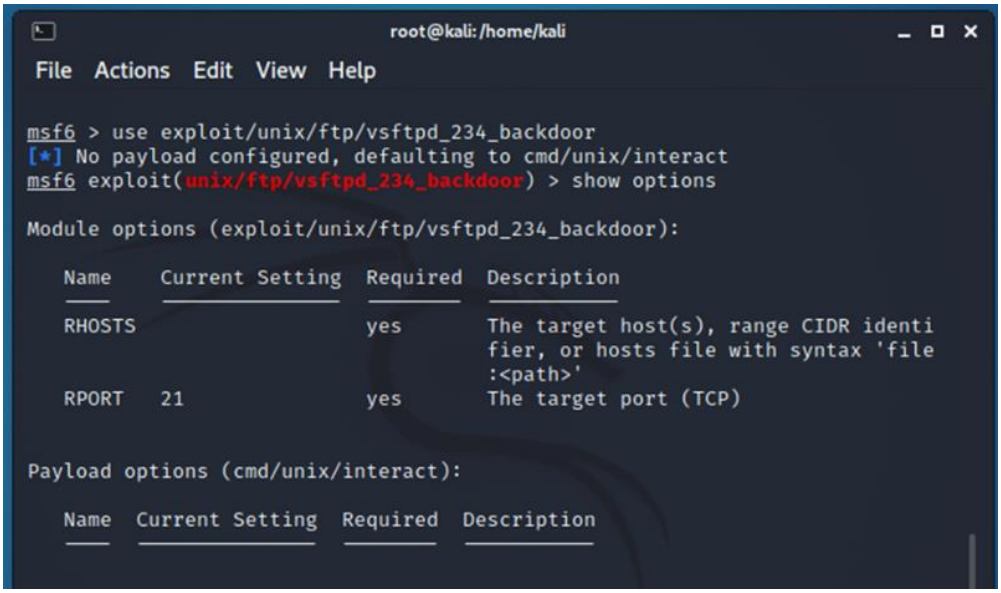
Figura 41 Interface Metasploite



Fuente 45 elaboración propia

En esta interface se selecciona el exploit para servicio ftp, sin embargo, es potestad del analista usar el que haya identificado sobre la máquina objeto de análisis, para el caso práctico se ejecuta el comando: *use exploit/unix/ftp/vsftpd_234_backdoor* y posteriormente *show options,* para conocer las opciones, como el puerto sobre el cual trabaja el exploit, tal como se muestra en la Figura 42.

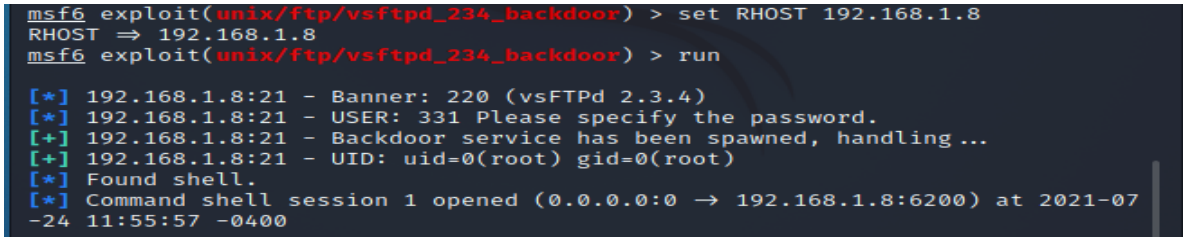
Figura 42 Configuración Metaesploit



Fuente 46 Elaboración propia

A través del comando set RHOST + IP de la máquina objetivo, se establece los parámetros para iniciar el test y luego con el comando run, se inicia el intento de conexión para inicio de una sesión remota, así como se observa en la Figura 43.

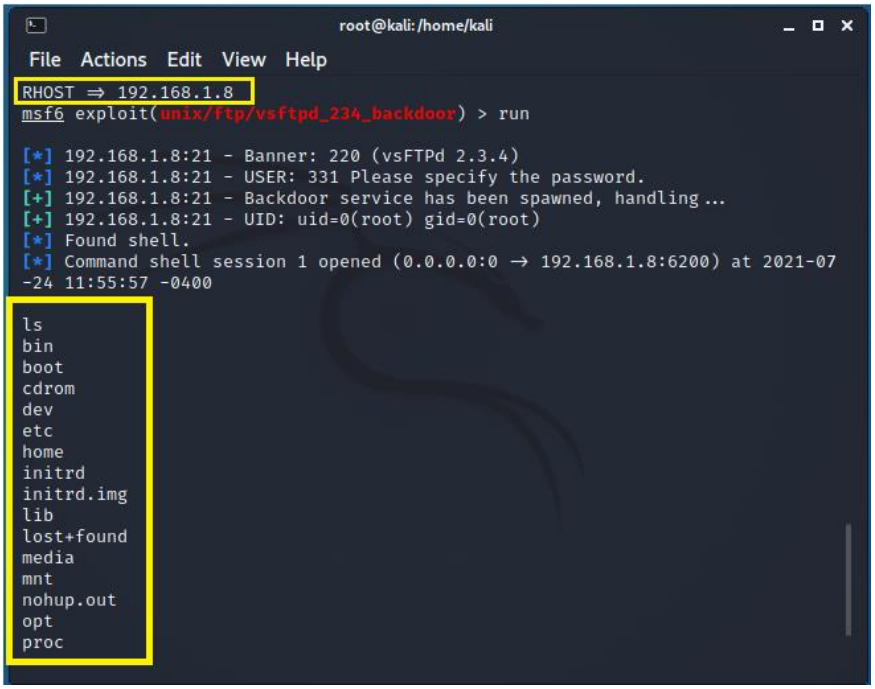
Figura 43 Conexión Metaesploit



Fuente 47 Elaboración propia

Después de establecida la sesión con el comando ls, se logra consultar los archivos de la máquina objetivo, logrando realizar la explotación de la vulnerabilidad, como se muestra en la Figura 43.

Figura 44 Explotación

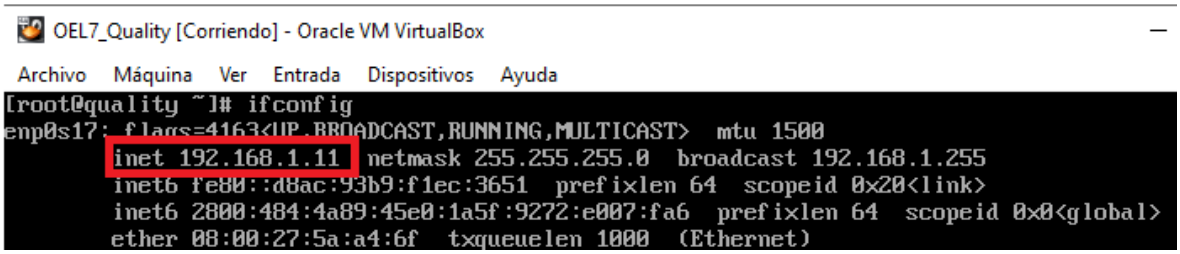


Fuente 48 elaboración propia

6.3.7 Análisis con IMPERVA

En la siguiente practica se realizará un escaneo de vulnerabilidades a una base de datos Oracle, la cual se encuentra alojada en una máquina virtual que posee dirección IP 192.168.1.11, como se muestra en la Figura 45.

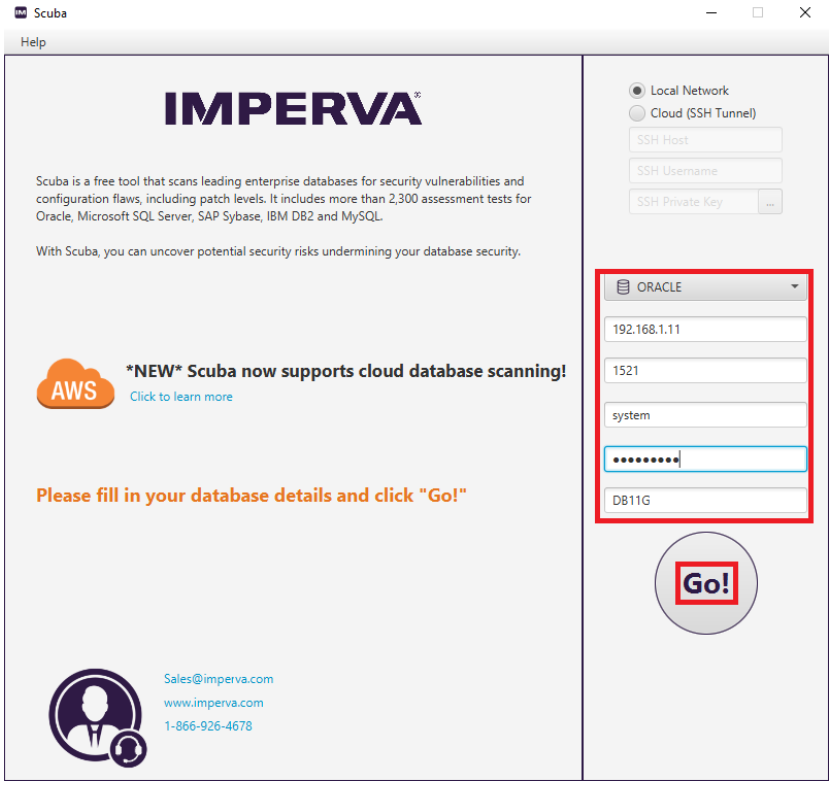
Figura 45 Ventana comandos Linux Identificación IP



Fuente 49 Elaboración propia

Se inicia la aplicación IMPERVA y registran los datos de la ip, puerto, usuario y contraseña para acceder al escaneo, así como se muestra en la Figura 46.

Figura 46 Interfaz de Software Imperva



Fuente 50 Elaboración propia

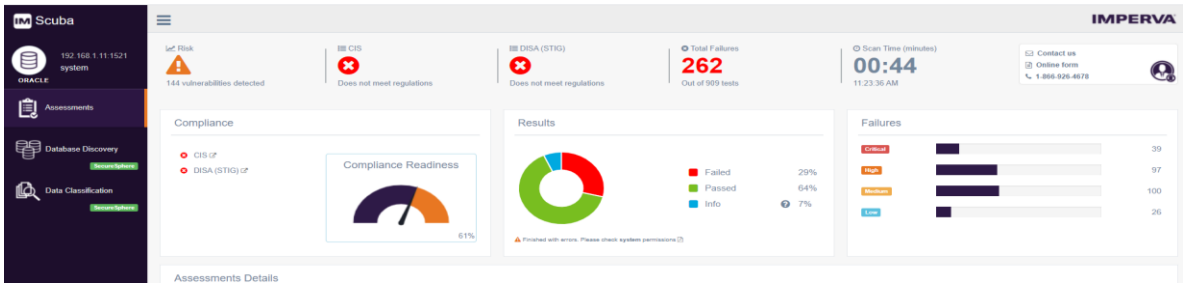
El sistema iniciará el escaneo y se mostrará una ventana de progreso en la cual se muestra la ejecución de los test que realiza el escáner de vulnerabilidades, como se muestra en la Figura 47.

Figura 47 Ventana de Progreso Escaneo de Vulnerabilidades Imperva

Fuente 51 Elaboración propia

Al terminar el escaneo abrirá el explorador web, mostrando la cantidad de vulnerabilidades encontradas en la base de datos, como se observa en la Figura 48.

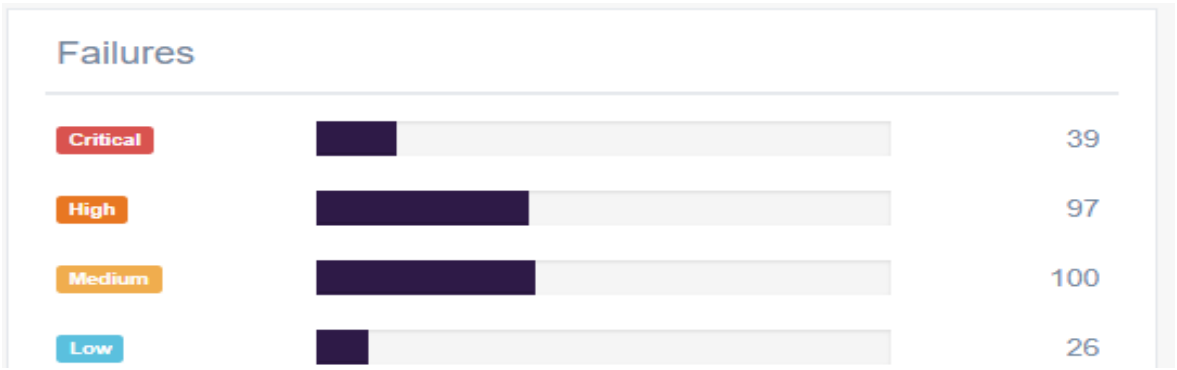
Figura 48 Interfaz de Reporte de Vulnerabilidades de Imperva



Fuente 52 Elaboración propia

El reporte ofrece un informe detallado del número de vulnerabilidades categorizadas por niveles, dentro de los cuales se puede apreciar los siguientes : critico, alto, medio y bajo, tal como se observa en la Figura 49, este reporte permite ofrecer un panorama de la seguridad de la base de datos que se administra, lo cual permitirá realizar las intervenciones que se requieran.

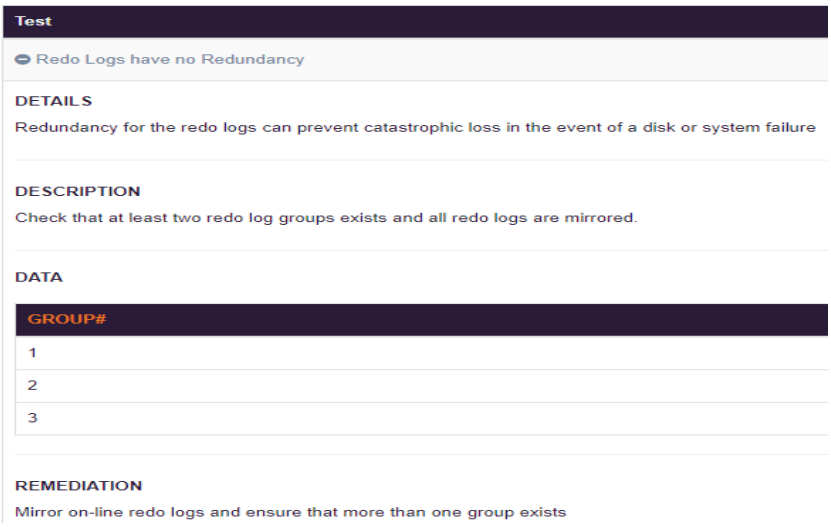
Figura 49 Clasificación de Vulnerabilidades Escaneadas con Imperva



Fuente 53 Elaboración Propia

De otra parte, el sistema Imperva ofrece dentro del detalle del reporte, información detallada de la vulnerabilidad y la solución a la misma, tal como se muestra en la Figura 50.

Figura 50 Información Detallada de Vulnerabilidad y Remediación



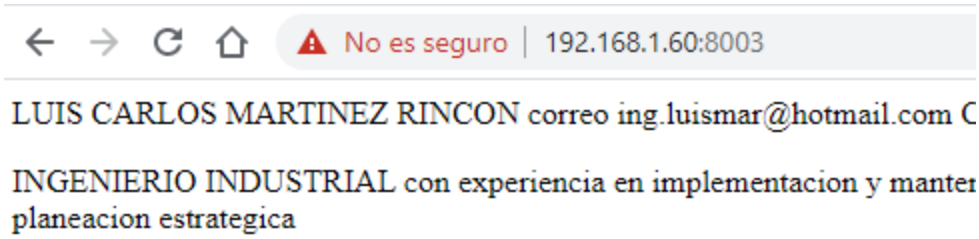
Fuente 54 Elaboración propia

El sistema IMPERVA, se encuentra articulado con el marco de referencia CIS CONTROL y CVE Mitre, lo cual posibilita conocer a fondo la vulnerabilidad y su remediación, ofreciendo de esta manera no solamente la posibilidad de conocer las vulnerabilidades, sino también la solución de las mismas.

6.3.8 Análisis con OWASP ZAP

En el siguiente ejemplo, observamos una página web de prueba como se observa en la Figura 51, creada para efectuar un escaneo de vulnerabilidades con la aplicación OWASP ZAP, la página de prueba cuenta con algunas medidas de control, como direccionamiento a un puerto especifico, bloqueo de puertos y certificado de seguridad, las cuales son medidas básicas de control, no obstante dichos controles, se realiza una comprobación con la aplicación OWASP ZAP, para identificar otras posibles vulnerabilidades que se puedan presentar con el sitio web.

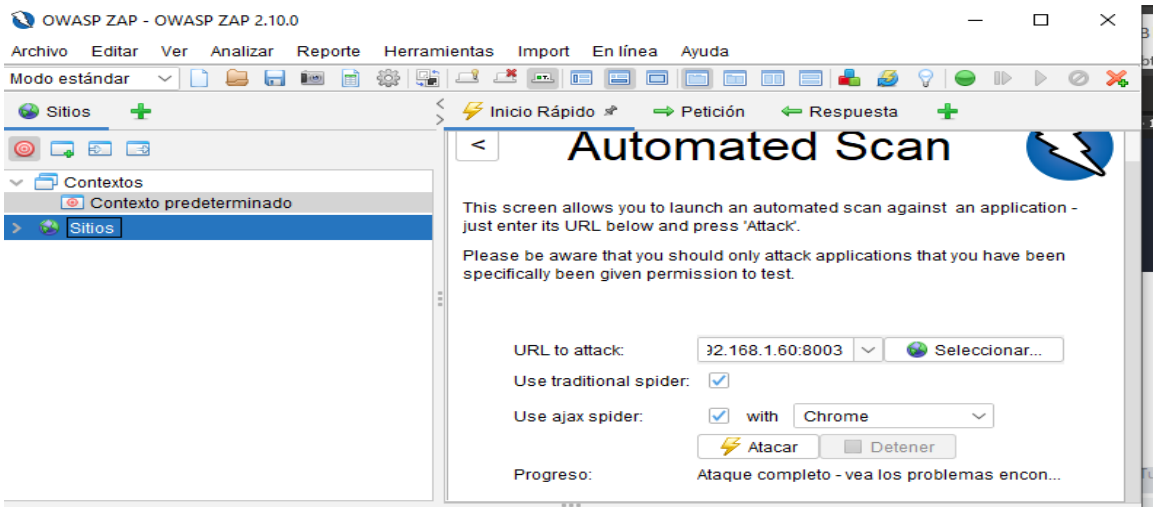
Figura 51 Página Web de Prueba



Fuente 55 Elaboración propia

En la Figura 52, se observa la interfaz de la aplicación OWASP ZAP, la cual posee unos campos de parametrización del sitio que se desea escanear, en él se ingresa la url, puerto especifico, se tildan las opciones de *use tradicional spider* y *use Ajax spider,* las cuales son las herramientas con las que se ejecutará el escaneo y se inicia con el botón atacar, esta acción ejecutará el escaneo de vulnerabilidades que posee el sitio web y que posteriormente se podrá analizar de acuerdo al reporte del sistema.

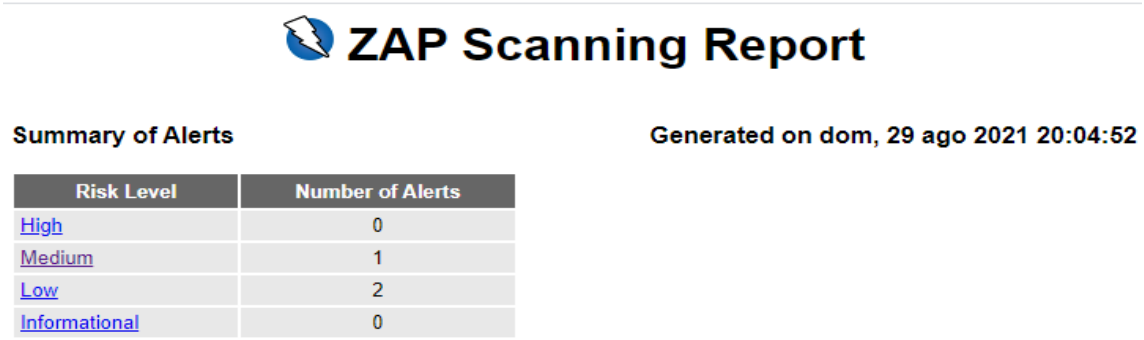
Figura 52 Interfaz OWASP ZAP



Fuente 56 Elaboración propia

La aplicación OWASP ZAP, posterior al escaneo, genera un reporte clasificando el nivel del riesgo de las vulnerabilidades que encuentra en el portal web analizado, en la Figura 53, se puede observar el reporte realizado por la aplicación, el cual indica la fecha y hora de generación y el número de vulnerabilidades encontradas, que son clasificadas en los niveles Alto, Medio y Bajo.

Figura 53 Reporte de Escaneo OWASP ZAP



ZAP Scanning Report

Summary of Alerts **Generated on dom, 29 ago 2021 20:04:52**

Risk Level	Number of Alerts
High	0
Medium	1
Low	2
Informational	0

Fuente 57 Elaboración propia

El sistema OWASP ZAP, permite generar un reporte detallado del escaneo, describiendo cada vulnerabilidad encontrada y una propuesta de solución, tal como se puede apreciar en las Figuras 54,55 y 56.

Figura 54 Reporte Vulnerabilidad Media

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://192.168.1.60:8003
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Source ID	3

Fuente 58 Elaboración propia

Figura 55 Reporte de Vulnerabilidad Baja

Low (Medium)	Incomplete or No Cache-control Header Set
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content.
URL	https://192.168.1.60:8003
Method	GET
Parameter	Cache-Control
Instances	1
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
CWE Id	525
WASC Id	13
Source ID	3

Fuente 59 Elaboración propia

Figura 56 Reporte de Vulnerabilidad Baja

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://192.168.1.60:8003
Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Source ID	3

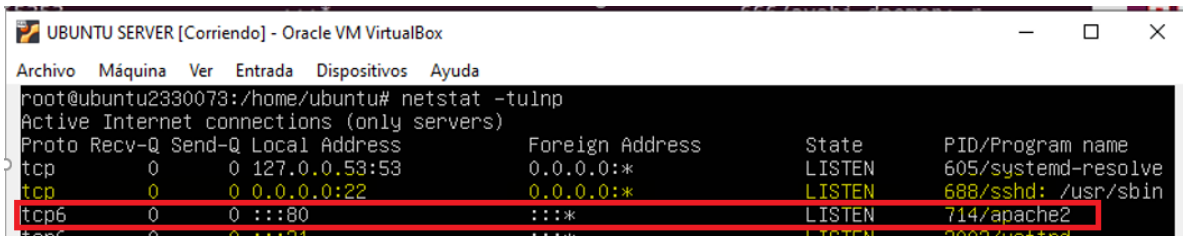
Fuente 60 Elaboración propia

6.3.9 Eliminando Vulnerabilidades con IPTABLES

La implementación de políticas en los servidores es necesaria para subsanar muchas de las vulnerabilidades, no obstante, deben cambiarse los puertos predeterminados de algunos servicios para completar la mitigación, a continuación, se expone la forma en que se modifica el puerto 80 del servicio web apache en un servidor y se configuran políticas para rechazar cualquier conexión

A través de la instrucción *netstat -tulnpd*, se accede a la ventana de información de los puertos, donde se encuentran configurados los servicios en la terminal Linux, identificando el servicio apache configurado en el puerto 80, tal como se presenta en la Figura 57.

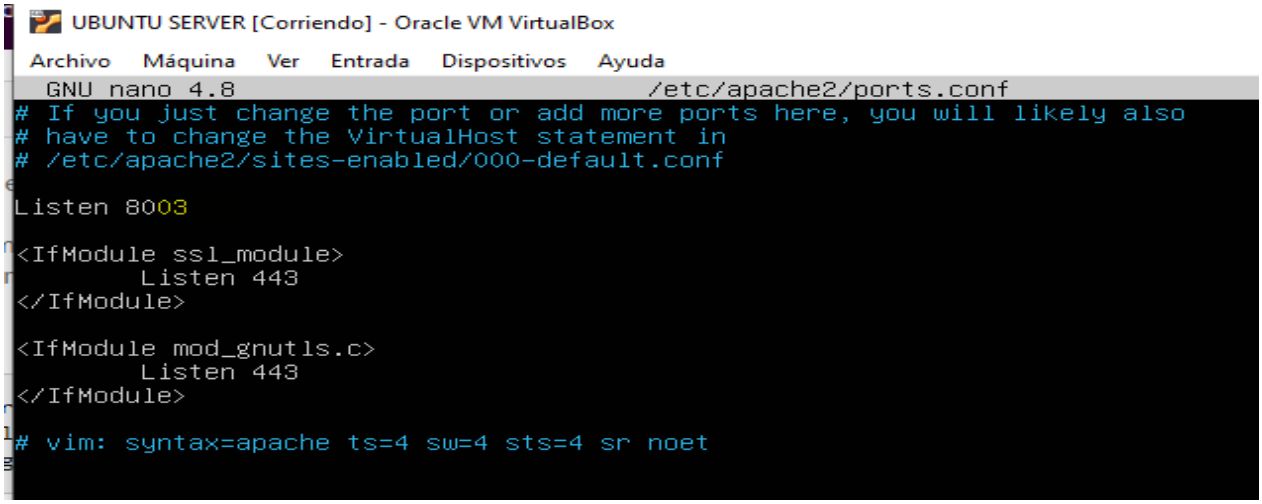
Figura 57 Ventana de información servicios



Fuente 61 elaboración propia

Se accede desde la terminal del servidor, al archivo de configuración de apache2, a través de la instrucción: *nano /etc/apache2/ports.conf*, la cual muestra la imagen representada en la Figura 39, donde posteriormente se ubica en la línea listen 80 y se procede a realizar la actualización, finalizando con las teclas Ctrl + X y luego enter, como se presenta en la Figura 58.

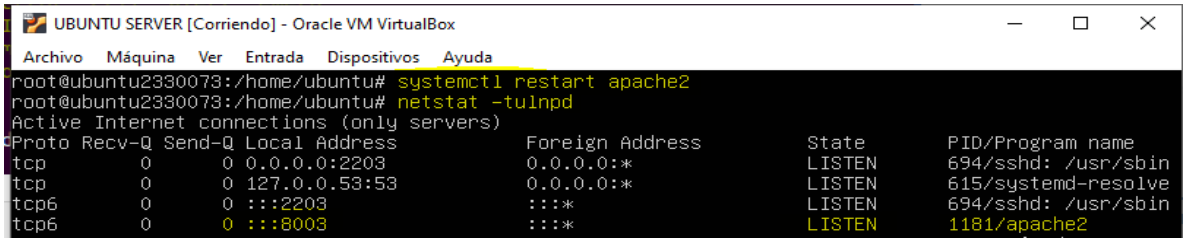
Figura 58 Ventana de Configuración servicio web



Fuente 62 elaboración propia

Para que surtan efecto los cambios realizados, se procede a reiniciar el servicio web apache, a través de la instrucción: *systemctl restart* apache2, confirmando que se ha configurado un nuevo puerto, donde es asignado el puerto 8003, como se presenta en la Figura 59.

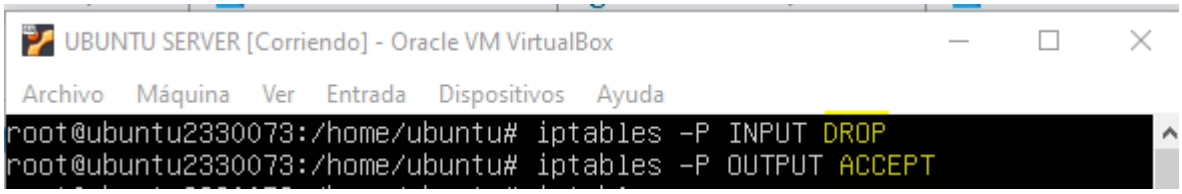
Figura 59 Ventana de reinicio servicio



Fuente 63 elaboración propia

Se realiza ingreso de regla por IPTABLES, para que todas las conexiones entrantes al servidor sean rechazadas y las conexiones salientes aceptadas, mediante la instrucción: *iptables -P INPUT DROP* y *iptables -P OUTPUT ACCEPT,* como se observa en la Figura 60.

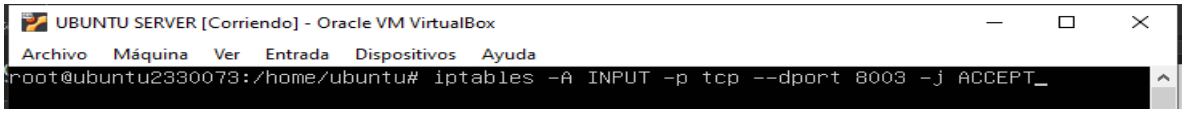
Figura 60 Implementación de regla DROP y ACCEPT



Fuente 64 elaboración propia

Como se han bloqueado todas las conexiones entrantes, es necesario crear una excepción a esta regla, para que el servidor web pueda mostrar la información del sitio, este procedimiento se logra a través de la creación de una regla de aceptación de conexiones al pueto 8003 del servidor web por *Iptables,* mediante la instrucción: iptables -A INPUT -p tcp—dport 8003 -j ACCEPT, como se aprecia en la Figura 60.

Figura 61 Excepción regla servicio web



Fuente 65 Elaboración propia

6.4 FASE IV EVALUACIÓN DEL DISEÑO TÉCNICO DEL CSIRT

Para esta fase es importante determinar la evaluación de la operación del centro de respuesta del CSIRT, para el cual, se propone que existan indicadores que permitan evaluar el desempeño del equipo de respuesta, así como generar los reportes o informes de los ataques que más se estén presentando, todo esto ayudara al análisis situacional de la seguridad informática, que, de forma articulada, permite elevar una alerta a las organizaciones para combatir el cibercrimen.

Con el fin de medir la gestión y operación del CSIRT, se propone la implementación y seguimiento de los indicadores de la Tabla 5.

Tabla 5 Indicadores de Medición S.I.

Formula	Indicador
Número de incidentes de S.I. gestionados X 100 Total, de Incidentes	% Porcentaje gestión de incidentes
Número de eventos de S.I solucionados x 100 Total, de eventos de S.I	% Porcentaje de solución de eventos de S.I

Fuente 66 elaboración propia

De otra parte, es necesario incorporar dentro de la fase de evaluación, la percepción de las partes interesadas, en ese sentido, cada gestión debe ir acompañada por una encuesta de percepción de los usuarios, con el fin de determinar el grado de satisfacción sobre los casos solucionados, estableciendo una muestra representativa para garantizar la objetividad de la evaluación. Para estas mediciones, se puede utilizar las siguientes preguntas para evaluar la gestión:

¿Cómo califica la oportunidad en la gestión del incidente?

Excelente
Buena
Regular
Mala

¿El incidente reportado fue solucionado?

Sí
No

¿Como califica la calidad en la atención del servicio?

Excelente
Buena
Regular
Mala

Para el caso de los informes es importante medir las tendencias de los ataques para alertar a las organizaciones , empleados , aliados y ciudadanía en general sobre las cantidades y tipos de ataques que se están atendiendo y sí se considera adecuado explicar los delitos y el modo con el que el cibercrimen está operando, es importante para este tipo de informes usar gráficas estadísticas que presenten los datos de tal manera que sean fácil de comprender y conocer los ataques más representativos a la seguridad de la organización, con el fin de analizar su comportamiento e implementar las medidas pertinentes, tal como se expone en el Anexo A Informe de Seguridad.

7 CONCLUSIONES

Existen diversas herramientas de software que permiten abordar los aspectos necesarios para prestar los servicios de un CSIRT, entre ellos la identificación y análisis de vulnerabilidades, algunas herramientas en software libre y otras más especializadas de pago, sin embargo, todas ellas se complementan aportando características individuales e indispensables en la seguridad informática, que permiten atender y dar respuesta los incidentes informáticos.

El modelo de operación del CSIRT, es la base del diseño técnico estructurado, allí se obtiene como aprendizaje significativo, que a partir de la planificación de los recursos y las actividades que serán implementadas en dicha estructura, tendremos como resultado la capacidad operativa y de respuesta, por lo cual, la eficiencia del CSIRT, dependerá de la profundidad del análisis con la que se planifique.

La implementación de las herramientas de gestión de incidentes y análisis de vulnerabilidades, permitirán operar al CSIRT de forma organizada, los reportes de vulnerabilidades, así como los de incidentes, serán necesarios para el soporte de la gestión, trazabilidad y análisis del desempeño.

La medición del desempeño del CSIRT, debe realizarse de forma periódica, para esto, serán indispensables los indicadores y auditorias, que permiten conocer los resultados positivos y negativos del equipo de respuesta, permitiendo corregir aquellas falencias en las que se deba fortalecer su estructura.

El diseño técnico estructurado de un CSIRT, es la mejor forma para prepararse ante cualquier evento e incidente de seguridad informática, su conformación, permite la prevención y mitigación del riesgo informático y el retorno de la inversión, es razonable con relación a las consecuencias económicas y reputacionales que ocasionarían la materialización de un riesgo de este tipo.

8 RECOMENDACIONES

Es necesario establecer los procedimientos de mitigación y documentarlos, con el fin de que sirvan de guía y solución eficaz para la operación.

El CSIRT, debe ser implementado de acuerdo a los recursos disponibles, aunque cada rol planteado en el diseño estructurado es importante para la operación, puede irse implementado de manera evolutiva por servicios.

Los informes de evaluación del diseño del CSIRT, pueden variar de acuerdo a las expectativas y los resultados, que en materia de seguridad y desempeño, generen el equipo de respuesta, sin embargo, se deben profundizar los aspectos de mayor impacto y orientarlos a la efectividad con la que está operando.

Las herramientas de seguridad que provee el software libre, son indispensables para toda la etapa de la gestión de incidentes del CSIRT, sin embargo, debe considerarse los riesgos de no contar con un soporte y actualizaciones oportunas de algunas vulnerabilidades.

Ningún diseño es totalmente seguro, así logre la implementación propuesta, el equipo humano, las herramientas y técnicas, deberán ser renovadas y actualizadas, conforme vaya evolucionando la tecnología. capacitar al equipo de respuesta, es fundamental para no restarle efectividad a la operación.

Implemente en la organización un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, esto apalancará la gestión y prevendrá brechas de seguridad.

BIBLIOGRAFÍA

AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN [Sitio Web] Attiki ENISA Cómo crear un CSIRT paso a paso , P. 6 [Consulta : 31 de julio]. ,Disponible en: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

COLOMBIA. EL CONGRESO DE COLOMBIA, Ley 1273(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”.

COLOMBIA. EL CONGRESO DE COLOMBIA, Ley 1581 (17 de octubre de 2012) "Por la cual se dictan disposiciones generales para la protección de datos personales"

CENTRO DE RESPUESTAS A INCIDENTES CIBERNÉTICOS [Sitio Web] Paraguay CERT CIS Controls Spanish Translation , P. 5 [Consulta : 28 de mayo 2021]. ,Disponible en: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA [Sitio Web] Bogotá DAFP 15 de mayo ,Disponible en: https://www.funcionpublica.gov.co/eva/es/racionalizacion2018

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG [Sitio Web] Bogotá DAFP 24 de julio 2018 ,Disponible en: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34268003

DEPARTAMENTO NACIONAL DE PLANEACIÓN [Sitio Web] Bogotá DNP CONPES 3854 Política Nacional de Seguridad Digital, P. 44-45 [Consulta : 28 de mayo 2021]. ,Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

DEPARTAMENTO NACIONAL DE PLANEACIÓN [Sitio Web] Bogotá DNP, CONPES 3995 Política Nacional de Confianza y Seguridad Digital, 01 de julio 2020 ,Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

ESCRIVÁ GASCÓ G. Seguridad informática [En Línea]. Madrid: Macmillan Iberia, S.A. 2013 [consultado 26 Jul 2021]. P.175 - 216 Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43260?page=1

EL TIEMPO [Sitio Web] Bogotá Anonymous revela correos y contraseñas de miembros del Ejército , P. [Consulta : 30 de mayo 2021]. ,Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/anonymous-revela-correos-y-contrasenas-de-miembros-del-ejercito-de-colombia-585874

EL TIEMPO [Sitio Web] Bogotá 30 de mayo 2021 ,Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/anonymous-revela-correos-y-contrasenas-de-miembros-del-ejercito-de-colombia-585874

GREENBONE , OpenVAS - Escáner de evaluación de vulnerabilidad abierta [Sitio Web] Osnabrück 19 de mayo 2021 ,Disponible en: https://www.openvas.org/

ICONTEC (2012), GUIA TECNICA COLOMBIANA ISO /IEC 27035:2012

INSTITUTO NACIONAL DE CIBER SEGURIDAD [Sitio Web] Madrid INCIBE Glosario de términos de ciberseguridad , P. 24 [Consulta : 28 de mayo 2021]. , Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

INSTITUTO DE SEGURIDAD Y METODOLOGIAS ABIERTAS [Sitio Web] Barcelona ISSECOM Manual de metodología de pruebas de seguridad de código abierto , [Consulta : 19 de junio 2021]. ,Disponible en: https://www.isecom.org/research.html#content5-9d

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGIAS [Sitio Web] NIST Cibersecurity Framework CSF , P. 4-6 [Consulta : 19 de junio 2021]. ,Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES [Sitio Web] Bogotá MINTIC Glosario , P. [Consulta : 28 de mayo 2021]. ,Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES [Sitio Web] Bogotá MINTIC , Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. , P. 9 [Consulta : 18 de julio 2021]. ,Disponible en:

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150509_G21_Gestion_Incidentes.pdf

ORGANIZACIÓN DE ESTADOS AMERICANOS [Sitio Web] Washington DC. OEA abril 2016 ,Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

POLICIA NACIONAL DE COLOMBIA [Sitio Web] Bogotá PONAL Balance cibercrimen 2020 , P. [Consulta : 30 de mayo 2021]. ,Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

POLICIA NACIONAL DE COLOMBIA [Sitio Web] Bogotá PONAL Tendencias cibercrimen en Colombia , P. [Consulta : 30 de mayo 2021]. ,Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

ZAPATA PUERTA ,Luis Norberto y RECAMAN CHAUX, Hernando Investigación en ingeniería de sistemas e informática [En línea]. Investigación Universidad Pedagógica y Tecnológica de Colombia 2011 [Consultado el 30 de mayo 2021]Disponible en https://www.researchgate.net/profile/Jair-Otero/publication/220017085_Excalibur_Software_para_la_Administracion_de_Mecanimos_de_Seguridad_y_Servicios_de_Red_en_Sistemas_Operativos_Linux/links/0deec528bc07062c7c000000/Excalibur-Software-para-la-Administracion-de-Mecanimos-de-Seguridad-y-Servicios-de-Red-en-Sistemas-Operativos-Linux.pdf#page=117

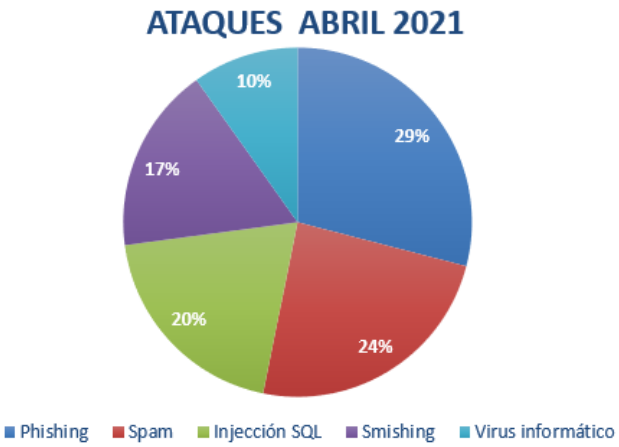
OWASP, Top 10 - 2017 [Sitio Web] Leinstraat OWASP [Consulta: 19 de mayo 2021] ,Disponible en: https://owasp.org/www-pdf-archive/OWASP-Top-10-2017-es.pdf

ZAPATA PUERTA, Luis Norberto y RECAMAN CHAUX, Hernando, Investigación en ingeniería de sistemas e informática [En línea].Investigación Universidad Pedagógica y Tecnológica de Colombia 2011 [Consultado el 30 de mayo 2021] Disponible en: https://www.researchgate.net/profile/Jair-Otero/publication/220017085_Excalibur_Software_para_la_Administracion_de_Mecanimos_de_Seguridad_y_Servicios_de_Red_en_Sistemas_Operativos_Linux/links/0deec528bc07062c7c000000/Excalibur-Software-para-la-Administracion-de-Mecanimos-de-Seguridad-y-Servicios-de-Red-en-Sistemas-Operativos-Linux.pdf#page=117

ANEXO A. INFORME DE SEGURIDAD

Informe de seguridad

TIPO DE ATAQUES	No.	%
Phishing	5895	29%
Spam	4896	24%
Inyección SQL	4000	20%
Smishing	3500	17%
Virus informático	2000	10%
TOTAL	**20291**	**100%**



INDICADOR	% DESEMPEÑO
% Gestión de Incidentes	98%
% Solución de eventos	75%