PROPUESTA TÉCNICA DE UNA INFRAESTRUCTURA LÓGICA PARA LAS OPERACIONES PROPIAS DE UN CSIRT ENFOCADO A LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN COLOMBIA.

LEIDY VANESSA GIRALDO MARTINEZ

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

PROPUESTA TÉCNICA DE UNA INFRAESTRUCTURA LÓGICA PARA LAS OPERACIONES PROPIAS DE UN CSIRT ENFOCADO A LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN COLOMBIA.

LEIDY VANESSA GIRALDO MARTINEZ

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Yenny Stella Nuñez Alvarez
Director

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

NOTA DE ACEPTACIÒN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente de Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Manizales.

DEDICATORIA

En primer lugar, quiero dedicarles todo a mis papas y a mi hermano, sin lugar a dudas son mi motor y mi mayor motivación para salir adelante. También para ti para quien sino… y por supuesto a Don Ferigo, porque alguien que tiene como frase de cabecera el “Never Give Up” debe de tener un ángel que la guía y que le muestra el camino que se debe de seguir sin nunca rendirse.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

GLOSARIO

AMENAZA INFORMATICA: El término amenaza visto desde el punto de vista informático hace referencia principalmente a un incidente bien sea nuevo o recién descubierto que puede llegar a dañar un sistema de información e incluso la organización como tal. Es un proceso que puede llegar a violar la seguridad de una empresa a través de vulnerabilidades.

ARPANET: ARPANET es la abreviación del término Advanced research projects agency network, es decir la Red de Agencias de Proyectos de investigación avanzada. Se trataba principalmente de una red de computadores que permitía enviar información de tipo militar a través de conexiones de diferentes tipos de grupos investigadores en estados unidos.

ATAQUE INFORMATICO: El ataque informático se define como un intento que busca acceder a los equipos tecnológicos de una organización, bien sea computadores o servidores, entre otros. Esto lo realiza a través de técnicas como introducción de virus o malware mediante el uso de diferentes técnicas que insertan el código malicioso en el equipo.

AUTENTICACION: La autenticación es el proceso por el cual se comprueba que una persona es quien dice ser en el momento en que busque acceder a un equipo o aun servicio virtual de un lugar determinado.

CERT: El CERT es un equipo de respuestas ante las emergencias de nivel informático. Es decir, este es un centro que se dedica a dar respuesta a todo tipo de incidentes que sean dirigidos a sistemas de información y sus tecnologías adyacentes. Adicional a esto, estos equipos a través de la investigación pueden generar alertas de amenazas nuevas de tal manera que los usuarios puedan prevenir antes de que ocurran.

CIBERSEGURIDAD: El término CIBERSEGURIDAD hace referencia al proceso que se encarga de defender los computadores, servidores e incluso dispositivos móviles y cualquier otro recurso tecnológico de ataques maliciosos.

CONFIDENCIALIDAD: La confidencialidad dentro de las Tecnologías de la Información hace referencia a la protección de los datos y la información que se transmite entre emisores y diferentes destinatarios si así se requiere.

CONPES 3854: Política Nacional de Seguridad Digital.

CSIRT: Equipo de respuesta ante emergencias informáticas. Es un grupo de profesionales que se encargan principalmente de desarrollar medidas que puedan

prevenir o reaccionar ante incidentes como tal de la seguridad de los sistemas de información.

DISPONIBILIDAD: La Disponibilidad hace referencia al proceso por el cual la información se encuentra siempre disponible para las personas que necesitan acceder a ella y que lógicamente cuenten con la autorización requerida.

GUSANO: Un gusano informático es un programa de software que contiene código malicioso y que puede ser fácilmente replicado a través de computadores e incluso a través de redes informáticas por donde se conectan dichos equipos.

HACKER: Un hacker es aquella persona que dedica sus esfuerzos a realizar códigos y pruebas a Sistemas de Información con el objetivo de transmitir esa información a las empresas para que estas tomen acciones correctivas.

INCIDENTE DE SEGURIDAD DE LA INFORMACION: Este tipo de incidentes hace referencia principalmente a toda aquella violación de las diferentes políticas de Seguridad Informática con las que cuenta una organización.

INTEGRIDAD: La integridad de la información tiene que ver principalmente con la información que no ha sido modificada y que se encuentra correcta dentro de sus parámetros originales en que fue entregada o puesta a disposición de un Sistema de Información.

MALWARE: Un malware es un programa que tiene código malicioso y que busca principalmente generar daños a un sistema informático sin que el usuario final del ataque tenga conocimiento de este.

PHISHING: Más conocido como suplantación de identidad, este término hace referencia al proceso delictivo mediante técnicas de ingeniería social los delincuentes adquieren información confidencial mediamente técnicas fraudulentas.

RAMSOMWARE: Se considera un ataque que busca el secuestro de información o datos a través de la restricción de acceso y buscando en su mayoría beneficios económicos a cambio de claves de desencriptación.

SI: Sistema de Información: Se considera un sistema de información al conjunto de datos que pueden tener una interacción entre sí mismos con un objetivo en común.

SOC: Centro de operaciones de Seguridad, son los encargados de realizar los respectivos seguimientos y análisis a los procedimientos que se presentan bien sea en las redes, servidores, sitios web, entre otros; de tal manera que puedan detectar anomalías que puedan comprometer como tal la estabilidad de un Sistema de Información.

TI: Tecnologías de información. Hace referencia principalmente a el uso de diferentes tipos de equipos bien sea de telecomunicaciones u ordenadores que puedan ser encaminados a transmitir, procesar y almacenar datos.

WANACRY: este es un ataque de tipo Ransomware que buscaba el secuestro de la información a cambio de una recompensa económica.

RESUMEN

En este proyecto aplicado se realizará la propuesta del diseño de la infraestructura lógica de un CSIRT, de tal manera que permita la ejecución de las actividades propias de este tanto en servicios proactivos como reactivos para el sector de las pequeñas y medianas empresas.

Dentro de esta propuesta se realizará una búsqueda bibliográfica acerca de cómo se encuentra el panorama de las pequeñas y medianas empresas en cuanto a temas de ciberseguridad, también se establecerán cuáles son los requerimientos tanto de software como de hardware para poner en práctica este tipo de equipos enfocado principalmente para el sector de las pequeñas y medianas empresas.

Por último, dentro de este documento que corresponde a un proyecto aplicado se realizara un laboratorio contralado que comprende las pruebas del software detectado previamente con el fin de realizar una demostración de estas herramientas en cuanto a temas de solución de incidentes informáticos.

PALABRAS CLAVE: Amenaza, Ataque, Autenticacion, Cert, Csirt, Ciberseguridad, Confidencialidad, Disponibilidad, Gusano, Hacker, Incidente De Seguridad, Integridad, Malware, Ransomware, Riesgo, Sgsi, Soc, Software, Vulnerabilidad.

ABSTRACT

In this applied project, the proposal for the design of the logical infrastructure of a CSIRT will be executed, in such a way that it allows the execution of its own activities both in proactive and reactive services for the sector of small and medium companies.

Within this proposal, a bibliographic search will be carried out on how the panorama of small and medium companies is in terms of cybersecurity issues, options will also be established are the requirements of both software and hardware to implement this type of equipment mainly focused on the small and medium-sized business sector.

Finally, within this document that corresponds to an applied project, a controlled laboratory will be carried out that includes the tests of the previously detected software in order to carry out a demonstration of these tools in terms of computer incident resolution issues.

KEYWORDS: Attack, Authentication, Availability, CERT, CSIRT, Cybersecurity, Confidentiality, Hacker, Integrity, Malware, Ramsomware, Security Incident, SOC, Software, Trojan, Vulnerability.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE ILUSTRACIONES

LISTA DE ANEXOS

INTRODUCCIÓN

En la actualidad han incrementado en gran número los ataques informáticos a los diferentes sistemas de información que se encuentran en la web, algunos de estos han sido tan catastróficos como el “Wanacry”, el cual según el portal BBC NEWS[1], se estima que afecto aproximadamente a 200.000 personas en todo el mundo generando el secuestro de la información a cambio de un pago por lo general en bitcoins. Actividades tan graves como esta ha dejado en evidencia las prácticas tan incipientes que se tienen en cuanto a ciberseguridad.

Es inminente el crecimiento exponencial que está teniendo los ciberataques, razón por la cual no puede ser menor el esfuerzo de la ciudadanía para repeler este tipo de irrupciones y de paralelamente retroalimentar a otras personas en cuanto a procesos ya documentados para evitar y mitigar vulnerabilidades.

Por tal razón es que ha surgido los CSIRT, como respuesta a el crecimiento de ciberdelincuentes y actividades delictivas dentro de la web, estos equipos se crean con el principal objetivo que mitigar y reaccionar en tiempo real ante ciberataques que afectan por lo general a organizaciones que cuentan con poca o nula preparación para actuar ante esta actividad.

Sin embargo, estas actividades delictivas no son solo cuestión de grandes empresas, las pequeñas y medianas empresas a lo largo del mundo también han sido flanco de ataques importantes, generando así una necesidad más amplia de infraestructuras lógicas y tecnologías que faciliten la creación de protocolos y políticas que les permita protegerse y mitigar la gran cantidad de vulnerabilidades que tienen para que en caso de sufrir una irrupción informática pueda este ser tratado a tiempo disminuyendo así su impacto en la organización.

Es allí donde los CSIRT deben plantear una alternativa para este tipo de empresas a través de constituciones de equipos más pequeños, pero más dinámicos en cuanto a temas de software que permitan dar respuesta mucho más inmediata a incidentes de Seguridad Informática y que a su vez plantee alternativas para evitarlas en el futuro a la organización flanco de este tipo de actividades.

[1] MILLAN, Alejandro V.BBC NEWS. [Sitio web].Qué tiene que ver Perú con el virus WannaCry, protagonista del ciberataque a nivel mundial. [Consulta: 4 de mayo de 2021]. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-39938098

.1 DEFINICIÓN DEL PROBLEMA

.1.1 ANTECEDENTES DEL PROBLEMA

Según la Revista Portafolio [2] la pandemia no solo ha traído grandes desafíos en cuanto a temas de Salud y Economía; el sector tecnológico también se ha visto altamente afectado debido al incremento considerable de delitos informáticos. Según el Centro cibernético de la Policía Nacional, para el primer semestre del año 2020 los ciberdelitos tuvieron un crecimiento del 59%. Es decir, en ese periodo de tiempo se llegaron a registrar en esta plataforma 17.211 denuncias de carácter informático.

De igual manera se dio para el segundo semestre del año 2020 como lo indica el portal Asuntos: Legales [3] en donde se habla que para el mes de noviembre el incremento paso a ser del 83% respecto a la fecha del año anterior, es decir se pasaron a tener 21.107 delitos informáticos a registrar 36.834 ciberdelitos. Según el portal, el delito que más suele presentarse es el de Suplantación de sitios web, se pasó de 892 casos registrados a 4.776 casos registrados teniendo prácticamente un incrementito del 435%; le siguen delitos como la Extracción de datos personales, las suplantaciones de identidad, entre otros.

Cifras que suelen generar una gran preocupación para todos los sectores de la economía en Colombia, principalmente porque la resolución de este tipo de ciberdelitos trae consigo una inversión de recursos económicos, recursos humanos y tiempo necesario para dejar los sistemas en una versión estable.

[2] Portafolio, Economía. [Sitio web]. Delitos informáticos, la otra pandemia del coronavirus [Consulta: 2 de mayo de 2021]. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

[3] Asuntos: Legales. [Sitio web]. Judicial Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis. [Consulta: 2 de mayo de 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

.1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son los requerimientos de software y hardware necesarios para diseñar una propuesta de infraestructura lógica para las operaciones propias del centro de respuesta a incidentes de Seguridad Informática?

.1.3 DEFINICION PROBLEMA

Entre abril y julio del 2019, según lo informó la compañía Fortinet [4] en su área de Inteligencia y amenazas, Colombia sufrió algo más de 40 billones de ciberataques. Esta es sin lugar a dudas una cifra altamente preocupante y más si adicionalmente Colombia se encuentra en el puesto 39 dentro del ranking de índices de seguridad, de 60 países estudiados por la compañía Fortinet en su informe.

Todo esto permite evidenciar que Colombia es un flanco de alta importancia para los ciberdelincuentes en la actualidad, muestra de esto es el informe que presentó la compañía ESET (ENJOY SAFE TECNOLOGY)[5], en donde da a conocer que el país fue el que más ataques de tipo malware en cuanto a países de la región como tal.

Las cifras del ranking apuntan a que en Colombia el 12.52% de todos los dispositivos móviles están infectados con algún tipo de virus que busca sustraer información o en el peor de los casos destruir el sistema.

En cuanto a los ordenadores, la cifra que ofrece el ranking es que el 16.4 % de todos los computadores en Colombia se encuentran infectados.

Comparando con los primeros y últimos puestos de este ranking se podría decir que el país se encuentra en la media de estas valoraciones, lo que da a entender que si bien es cierto no están tan expuestos y tan vulnerables a los ataques si falta mucho en materia de educación, infraestructura y equipos de respuesta en cuanto a incidentes de seguridad de la información.

Es por esta razón que se plantea la necesidad de tener un CSIRT para las pequeñas y medianas empresas que sirva como apoyo a las compañías en el momento en que presenten un incidente.

---

[4] FORTINET. [Sitio web]. América Latina sufrió más de 41 billones de intentos de ciberataques en 2020. [Consulta: 2 de mayo de 2021]. Disponible en: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020

[5] GIUSTO, Denise B. WeliveSecurity. [Sitio web]. Países más afectados por el Ransomware en Latinoamérica durante 2018. [Consulta: 4 de mayo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/

De esta forma, es fundamental que este equipo sirva de portal de información en cuanto a nuevos delitos y que presente una guía que les facilite a los usuarios comprender como actuar ante un ataque informático.

Sin embargo no es suficiente esfuerzo la conformación de este tipo de equipos, si bien es cierto la sola estructuración de estas organizaciones ya es un avance en temas de Seguridad Informática para las pequeñas y medianas empresas; estos deben de tener una fuerte estructura tecnológica de tal manera que a través de su puesta en marcha puedan dar respuesta a los incidentes informáticos, a prevenir futuros ataque e incluso a capacitar a estas organizaciones para que a través de la practicidad puedan implementar estructuras de nivel tecnológico tan robustas como les sea posible para prevenir incidentes a futuro.

.2 JUSTIFICACIÓN

La información se ha convertido día tras día en uno de los principales activos de cualquier tipo de organización, razón por la cual la necesidad de protegerla ha pasado de ser una actividad exclusiva de un área de Tecnología a ser una actividad que en su mayoría está articulada con los objetivos organizacionales de las empresas ya que preservar dicho activo de una manera óptima le permitirá a la empresa garantizar un correcto manejo de la información lo que sin lugar a dudas mejorara la reputación en un mercado determinado.

Tal es el caso de las Pequeñas y medianas empresas (PYMES), las cuales han empezado a afrontar grandes retos en cuanto a temas de Seguridad Informática puesto que el desarrollo tecnológico no ha sido ajeno a ellos y por ende los temas de preservación de la información abarcan en gran medida diferentes procesos que le permiten estar al día en cuanto a técnicas de Seguridad Digital acorde al tipo y tamaño de organización en el que se desenvuelve.

Como se indica en la Ley 590 de 2000[6], el gobierno ha visto la necesidad de impulsar el desarrollo integral de este tipo de empresas a través de temas tan importantes como la generación de empleo, desarrollos regionales e incluso la integración de diferentes sectores de la economía para de esta forma apuntar a la evolución y al posicionamiento de dichas empresas en la economía de un país.
Razón por la cual se inician una serie de estrategias y demás procesos que buscan principalmente la evolución de este tipo de empresas para de esta forma aumentar el crecimiento económico de estas y por ende aumentar el mercado en el que dichas empresas pueden desenvolverse.

Dentro de estas estrategias surgen temas importantes como la inversión en infraestructura tecnológica, esto principalmente porque la tecnológica en ocasiones automatiza procesos que suelen ser desarrollados por seres humanos y a través de esta automatización los procesos pasan a ser mucho más eficientes y mucho más eficaces. Esta evolución tecnológica de las Pequeñas y medianas empresas ha traído consigo todo un mundo de desconocimiento y malas interpretaciones de la tecnología.

Según Keith Farlinger, CEO de América BDO International [7] para el 2015, el 43% de las empresas en Colombia no cuentan con preparación alguna para responder ante un ataque informático. Dentro de este porcentaje lastimosamente las Pequeñas y medianas

---

[6] COLOMBIA.CONGRESO DE LA REPUBLICA DE COLOMBIA. [En línea]. Bogotá, D.C. Ley 590 de 2000. (10 de Julio.). Por lo cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresas. [Consulta: 17 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0590_2000.html

[7] REVISTA SEMANA. [En Línea]. Bogotá. El 43% de las empresas colombianas no están preparadas contra los ciberataques.7 de junio 2016. [Consulta: 16 de Mayo de 2021].Disponible en: https://www.semana.com/pais/articulo/colombia-tuvo-perdidas-de-1-billon-por-ciberataques/224404/

empresas son las que suelen estar más vulnerables ante este tipo de actividades por poca capacidad instalada o por pocos recursos tecnológicos en sus organizaciones.

Lo anterior no hace más que acervar la necesidad que tienen este tipo de organizaciones de contar con espacios en donde pueda ser mucho más fácil solucionar los diferentes tipos de ataques y amenazas a través de equipos de profesionales que se dedican a este tipo de soluciones; si bien es cierto este tipo de espacios y equipos ya existen en el país a través de organizaciones llamadas CSIRT, es importante establecer un equipo de estos para sectores de la economía mucho más pequeños con poco acceso a conocimientos tecnológicos y con pocos recursos para hacer grandes inversiones de Seguridad de la Información Dentro de la organización. A través de un CSIRT para pequeñas y medianas empresas las organizaciones podrán tener un equipo aliado que no solo los ayude a solucionar sus diferentes ataques de Seguridad informática, sino que a su vez pueda capacitarlos y pueda darle unas pautas a nivel lógico de cómo mejorar las infraestructuras tecnológicas para ser cada vez más seguras.

.3 OBJETIVOS

.3.1 OBJETIVOS GENERAL

Proponer un diseño de una infraestructura lógica que permita desarrollar las actividades propias de un CSIRT de acuerdo con los servicios reactivos y proactivos del mismo, enfocado a las pequeñas y medianas empresas en Colombia.

.3.2 OBJETIVOS ESPECÍFICOS

.3.3 Examinar el panorama actual de la Ciberseguridad en pequeñas y medianas empresas en Colombia y los ataques que han causado más impacto en la operatividad de las mismas.

.3.4 Estructurar la información relacionada con herramientas de hardware y software que permitan desarrollar las actividades del CSIRT teniendo presente el catálogo de servicios.

.3.5 Establecer los requerimientos necesarios en relación a la tecnología de hardware y software para el diseño de la infraestructura lógica que permitan desarrollar las actividades del CSIRT.

.3.6 Desarrollar a partir de laboratorios controlados y realización de pruebas de software, la demostración de las herramientas que pueden utilizarse para ejecución de las tareas propias de un CSIRT.

.4 MARCO REFERENCIAL

.4.1 MARCO TEÓRICO

En la actualidad el crecimiento del uso de las Tecnologías de la Información y las telecomunicaciones ha empezado a estar presente en prácticamente todos los ámbitos de la sociedad; lo que ha desencadenado un uso masivo del ciberespacio en donde al día de hoy es que se realizan la mayoría de los procesos de la internet, Incluyendo los conflictos y ataques que empiezan a vulnerar no solo la seguridad de las organizaciones sino que incluso se han presentado ataques que han puesto en jaque la seguridad nacional de un país.

Según la firma Deloitte[8], en Colombia las organizaciones no se están poniendo al frente de la situación, sus estructuras no están preparadas para ataques de seguridad informática.

Según esta firma, tan solo el 10% de las empresas tienen un área encargada de la prevención y mitigación de ciberataques, incluso, el resultado arrojo que aproximadamente el 40% de las organizaciones en el 2019, no tienen personal capacitado para adelantar las actividades necesarias para la implementación de la seguridad de la información dentro de la compañía.

Esto deja entrever las empresas no se están tomando en serio todo el tema de seguridad informática, tampoco están centrando recursos económicos para empezar a abordar ese tema, Deloitte estimo que el 50% de todas las organizaciones solo destinan entre 1% y el 5% del presupuesto del área de TI para proteger todo el tema de Seguridad de la Información.

Si se compara esto con Europa sin lugar a dudas se tendría un resultado de retraso en cuanto a avances en todos los aspectos, ya que no solo falta aunar en esfuerzos de Hardware, Software, sino que también falta implementar y educar a los profesionales de TI para que puedan empezar a incursionar en el tema de Ciberseguridad y puedan contrarrestar todas las amenazas que se tienen en el ciberespacio.

Todo esto ha propiciado que se generen equipos que puedan repeler este tipo de incidentes y ataques y que también puedan educar a los funcionarios de todas las organizaciones para que puedan ayudar en caso de un incidente a mitigar el daño ocasionado.

[8] Deloitte. [Sitio web]. Ciber Riesgos y Seguridad de la Información en América latina & Caribe. Países más afectados por el Ransomware en Latinoamérica durante 2018. [Consulta: 6 de mayo de 2021]. Disponible en: https://www2.deloitte.com/co/es/pages/risk/articles/ciber-riesgos-y-seguridad-de-la-info-en-america-latina-y-caribe.html

La primera vez que se implementó un equipo para responder a un ataque informático fue en el año 1988 debido a que se detectó un ataque llamado el Gusano “Morris” [9], este fue creado por un estudiante de la universidad de Harvard llamado Robert Tapan Morris, su impacto fue tal que se determinó que pudo haber afectado al 10% de todos los usuarios en ese momento de la red de computadoras creada por el Departamento de Defensa de los Estados Unidas denominada (ARPANET) Este ataque se dio a través de una vulnerabilidad del sistema operativo Unix, lo que le permitió propagarse rápidamente e ir bloqueando computador tras computador hasta que fue detectado y combatido.

El equipo encargado de combatir este ataque se centró principalmente en no solo corregir las vulnerabilidades del sistema operativo, sino que también realizo acciones que permitieron parchar los computadores que ya las presentaban bien sea que se encontraran en ARPANET o que se encontraran fuera de esta red.

Este ataque dio pie a lo que hoy en día se conoce como los CSIRT o CERT (Equipos de respuesta a incidentes de seguridad), que en la actualidad toma cada vez más relevancia ya que son los que se están encargando no solo de repeler todas las irrupciones presentadas sino de preparar a las organizaciones a que aprendan cómo reaccionar ante un incidente y como pueden minimizar el daño ocasionado. Este tipo de organizaciones cuenta con un equipo multidisciplinar de expertos quienes realizan las funciones en base a unos procesos y unas funciones previamente establecidas dentro de la estructura del CSIRT para de esta forma optimizar el recurso humano y generar el mayor impacto positivo posible. Su evolución ha permitido que ya no solo se enfoquen en gestionar como tal los incidentes de una organización, sino que también permite ejecutar servicios tales como el análisis forense que hoy en día es fundamental al momento de poder judicializar a alguno de estos atacantes preservando la cadena de evidencia intacta para que las pruebas puedan ser aprobadas por las autoridades judiciales.

Recordando que la seguridad de la información se basa principalmente en proteger la información registrada, bien sea de manera impresa, en Discos Duros e incluso en la memoria de los seres humanos; lo que conlleva a que los CSIRT trabajen en pro de este principio ya que el objetivo final es el de preservar la información tal y como estaba antes del incidente.

Estos equipos están preparados para actuar de manera inmediata, puesto que, un incidente dentro de una organización es por así decirlo una acción critica para la entidad y por ende cada minuto toma vital importancia para evitar que se generen más daños. Es por esto que este tipo de procesos debe de estar correctamente documentado no solo con las funciones sino con el personal a cargo de cada función para que todos trabajen similar al funcionamiento de un reloj en donde la sincronización permite un adecuado manejo del incidente.

[9] WeliveSecurity. [Sitio web]. Martes de retrospectiva: el gusano Morris. [Consulta: 6 de mayo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/

En cuanto al panorama Mundial de estos equipos de respuesta a incidentes informáticos se podrían listar los siguientes:

- **Kaspersky ICS CERT:** Este es un proyecto ruso conjunto con la compañía Kaspersky que busca principalmente ofrecer una gran cantidad de servicios que busquen la solución de incidentes informáticos propiamente en los sistemas industriales. Centran sus labores en ofrecer soluciones de inteligencia artificial, consultoría sobre Seguridad de la Información e incluso ofrecen equipos de investigación que permitan realizar análisis a las empresas que tengan acceso a este equipo.

- **InfoSSecurity Inciden Response Team:** Este es otro equipo de Respuesta a incidentes informáticos para Rusia. Su función principal no es la de desarrollar procesos que permitan dar respuesta a incidentes, su principal actuar es el de realizar una búsqueda a través de los diferentes equipos que se encuentran vinculados al Centro Nacional de Coordinación de Incidentes Informáticos (NCCCI)[10] para de esta forma darle una visión mucho más completa al usuario y que este tenga un consolidado de los diferentes tipos de respuestas que pueda tener.

- **RU-CERT:** Este es un centro ruso dedicado a la respuesta de incidentes informáticos. Su principal objetivo es el de disminuir las amenazas de cualquier nivel que se encuentren en los diferentes Sistemas de Información. Su actuar se da a través del segmento ruso de Internet y abarca a diferentes tipos de usuarios desde grandes empresas hasta pequeñas empresas e incluso usuarios independientes.

- **FIRST:** El First es el Foro Global de Equipos de Seguridad y Respuesta a Incidentes[11]. Es sin lugar a dudas la organización principal a nivel mundial en cuanto a respuesta a incidentes informáticos. La principal ventaja que tiene esta organización sobre otras es el acceso que puede tener a diferentes equipos de seguridad informática de todo tipo lo que le permitirá encontrar una solución mucho más efectiva y optima a cualquier tipo de incidente. El FIRST busca también crear una cooperación a través de diferentes equipos para de esta forma trabajar mancomunadamente no solo en resolver incidentes sino también en prevenirlos a través de diferentes tipos de investigaciones.

- **CN-CERT:** Centro Criptológico Nacional.[12] Este es un equipo de Respuesta a Incidentes informáticos ubicado en España y que hace parte del Centro Nacional de Inteligencia de este país. Su principal objetivo es el de mejorar todos los aspectos de

[10] INFOSECYRITY a Softline Company. SOC. [Sitio web]. Brindamos servicios de un centro de respuesta y monitoreo de incidentes utilizando tecnologías Big Data. [Consulta: 17 de mayo de 2021]. Disponible en: https://in4security.com/

[11] FIRST. Improving Security Together. [Sitio web]. FIRST is the global Forum of Incident Response and Security [Consulta: 17 de mayo de 2021]. Disponible en: https://www.first.org/

[12] CN-CERT. [Sitio web]. Centro Criptológico Nacional. [Consulta: 17 de mayo de 2021]. Disponible en: https://www.ccn-cert.cni.es/

la Ciberseguridad en España a través de la cooperación y la ayuda en cuanto a temas de incidentes informáticos.

.4.2 MARCO CONCEPTUAL

Dentro de un Incidente de Seguridad Informática, un CSIRT de lo que se encarga a grandes rasgos es de controlar y disminuir el daño causado, conservar intacta la cadena de evidencia, proporcionar todo lo necesario para la recuperación eficaz y rápida, evitar futuros ataques y dimensionar el daño causado.
Algunos de estos ataques son:

- Accesos no autorizados al sistema.
- Denegación del servicio.
- Uso no autorizado de un sistema para el manejo de los datos
- Cambios de las plataformas del SI sin consentimiento del propietario del sistema.

Existen algunos tipos de CSIRT dependiendo el lugar donde será implementado

.4.3 TIPOS CSIRT

.4.3.1 Centros de coordinación

En este caso se presentan acciones similares a la de los CSIRT, la diferencia es que existe una relación entre varios de estos equipos que generan una comunidad que está coordinada en pro de ayudarse mutuamente.

.4.3.2 CSIRTs Nacionales

En este caso el CSIRT presta servicios como tal en función del país. En la actualidad la mayoría de los países ya tienen implementados estos equipos debido al incremento exponencial de ataques a la información.

.4.3.3 CSIRTs Interno

Este equipo se enfoca principalmente en prestar sus servicios dentro de una organización. Bien podría ser un CSIRT de una entidad bancaria o una multinacional cuyos objetivos estratégicos se basan en la seguridad de su información.

.4.3.4 Equipos de Proveedores.

Este tipo de CSIRT lo que hace principalmente es vender un paquete de informes acerca de las vulnerabilidades de Software y Hardware.

.4.4 FUNCIONES PRINCIPALES CSIRT

De igual manera un CSIRT centra su principal actividad en todo lo que tiene que ver con el manejo de los incidentes. Dentro de las funciones principales de este tema se encuentran:

.4.4.1 Reporte de Incidente

Para el caso del CSIRT, este paso es de vital importancia ya que permite que todos los reportes de cualquier incidente sean recopilados y posteriormente revisados buscando relación entre un ataque y otro, de esta forma el equipo podrá encontrar comportamientos similares, patrones o cualquier tipo de información de un incidente que permita contrarrestar otro.

.4.4.2 Análisis del Incidente

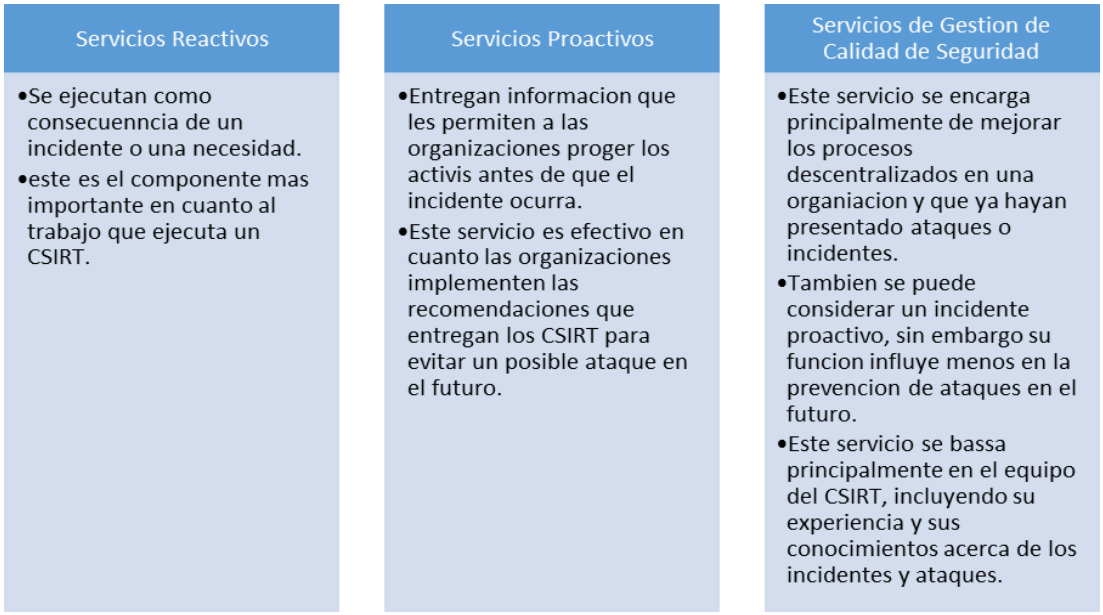
En este paso el CSIRT lo que hace es analizar de manera exhaustiva un ataque o un reporte con el fin de determinar la mayor cantidad de datos que sea posible de este. Es decir, en este paso se define cuál es la prioridad, el ámbito en el que se desenvuelve y la amenaza que este representa; de igual manera al tiempo se van viendo los procesos que se ejecutaran para la mitigación y respuesta al incidente.

.4.4.3 Respuesta al Incidente

En este proceso un CSIRT puede realizar dos acciones, en primer lugar, puede indicarle todas las recomendaciones concernientes del caso a la compañía atacada para que sea esta junto con su propio equipo la que se encargue de la prevención y contención del incidente. En el otro caso es el CSIRT propio quien ejecuta todo el proceso desde aplicar las recomendaciones detectadas y realizar su respectiva prevención y contención del ataque.

En el proceso de creación de un CSIRT se debe de tener muy claro aspectos tales como: Misión, Metas, Objetivos, ubicación dentro de la organización, público al que se le prestara el servicio, como funcionara y por último que servicios va a prestar. Como se evidencia en la Ilustración, es importante tener presente que servicios va a prestar propiamente el CSIRT; si estos servicios van a ser reactivos, proactivos o apuntaran como tal a la gestión y calidad de la Seguridad de la Información.

Ilustración 1.Servicios de un CSIRT



Fuente: LANFRANCO, Einar.CSIRTs ¿De qué SE TRATA? Modelos posibles, servicios y herramientas. [Imagen]. p. 12. [Consulta: 10 de mayo de 2021]. Disponible en: https://studylib.es/doc/6142341/csirts

El éxito de implementar un CSIRT está básicamente en que la comunidad objetivo sepa de su presencia y que tengan claro que son los servicios que el equipo puede ofrecer en pro de solucionar incidentes de seguridad de la información.

Es fundamental que el público este correctamente educado en cuanto al alcance del CSIRT y de esta forma pueda dimensionar toda la ayuda posible y recurrir a ellos en caso de un ataque.

En todo el proceso el CSIRT de lo que se encarga a grandes rasgos es de controlar y disminuir el daño causado, conservar intacta la cadena de evidencia, proporcionar todo lo necesario para la recuperación eficaz y rápida, evitar futuros ataques y dimensionar el daño causado.

.4.5 MARCO LEGAL

En Colombia La Ley 1273 de 2009 [13] incursiono penalizando todo tipo de vulneración de la Información y Datos personales de la siguiente manera:

[13] COLOMBIA.CONGRESO DE LA REPUBLICA. [En línea]. Bogotá, D.C. Ley 1273 del 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [Consulta: 17 de Mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- **Artículo 269A:** Acceso abusivo a un sistema informático.
  En este caso este articulo busca a grandes rasgos penalizar a toda persona que sin tener la respectiva autorización ingrese de manera parcial o total a un Sistema de información bien sea que tenga un acceso previo o no. La pena que se tiene estimada para este delito es prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B:** Obstaculización ilegítima de sistema informático o red de telecomunicación. Básicamente lo que busca penalizar este artículo es a aquellas personas que sin autorización impidan u obstaculicen el funcionamiento de manera continua de un Sistema de Información y a los respectivos datos que allí se encuentran; este delito también aplica a quien no permita el ingreso a una red de telecomunicaciones. La pena contemplada para este artículo es de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C:** Interceptación de datos informáticos.
  Lo que penaliza este artículo es a aquellas personas que, sin tener una orden judicial previamente generada por las autoridades competentes, intercepte cualquier tipo de datos informáticos bien sea desde su lugar de origen o destino. Las penas contempladas son prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269D:** Daño Informático.
  El artículo apunta a judicializar a cualquier persona que destruya, altere, borre o elimine cualquier tipo de dato informático o Sistemas de información. La pena contemplada es de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E:** Uso de software malicioso.
  Se penalizará a los ciudadanos que sin tener la facultad adecuada desarrollen, trafiquen, adquieran o cualquier, etc. a todo tipo de Software malicioso o programas tecnológicos que tengan fines nocivos. La pena que contempla este artículo es de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F:** Violación de datos personales.
  La ley contempla que cualquier persona que no cuente con la facultad correspondiente y que incurra en compilar, sustraer, vender, intercambiar, comprar, entre otros datos personales, bodegas de información o bases de datos podrá incurrir en una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269G:** Suplantación de sitios web para capturar datos personales.

El artículo hace referencia a penalizar a las personas que con un objetivo delictivo y sin facultades diseñe, desarrollo, replique o envié páginas web, enlaces o ventanas emergentes. La pena podría llegar a ser prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

- **Artículo 269I:** Hurto por medios informáticos y semejantes.
  Apunta a cuyas personas que, superando medidas de seguridad informáticas, ejecute la conducta señalada en el artículo 239 manipulando un sistema de Información, una red de sistema electrónico u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, podrá incurrir en las penas señaladas en el artículo 240 de este Código.

- **Artículo 269J:** Transferencia no consentida de activos.
  Quien con ánimo de lucro y valiéndose de alguna manipulación o artimaña informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre y cuando la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes.

De esta forma se esperaba regular en el ordenamiento la temática y que los ciberdelitos disminuyeran considerablemente, sin embargo, no ha sido el caso ya que Colombia sigue estando expuesta a un sinfín de ataques informáticos, tales como: Ransomware, Phishing, entre otros.

Razón por la cual la corte constitucional expidió una sentencia en el año 2012 denominada la T-260. Allí a lo que hace referencia principalmente es la garantía que el estado debe de tener respecto a toda la información en razón de no vulnerar los derechos que puedan tener los ciudadanos en cuanto a la protección de información.

Dentro del Documento CONPES 3854 de 2016 [14] en donde lo que se busca es crear una Política Nacional de Seguridad Digital que se plantea fortalecer todas las acciones necesarias para mejorar la capacidad de respuesta de las partes afectadas en temas de poder identificar, gestionar, tratar y disminuir los riesgos que pueden desencadenar todos los procesos de seguridad digital en los diferentes sectores económicos del país.

[14] COLOMBIA.CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. [En línea].Bogotá, D.C. CONPES 3854. (11 de abril de 2016). Política Nacional de Seguridad Digital. [Consulta: 17 de Mayo de 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Ley 1928 del 24 de Julio de 2018.[15] En donde se aprueba el convenio realizado sobre la Ciberdelincuencia adoptado el 23 de Noviembre de 2001 en Budapest.

Esta ley se centra principalmente en adoptar todas las medidas aprobadas en el convenio anteriormente mencionado en donde se busca prevenir todos aquellos actos que vayan encaminados a afectar y alterar la confidencialidad, integridad y disponibilidad de los sistemas de información, las redes y todos aquellos datos que se manejen en las diferentes herramientas tecnológicas que se tienen en la actualidad. De igual forma se espera atacar el abuso de todos estos sistemas tipificando cada uno de los actos delictivos para posteriormente generar los poderes suficientes a través de la detección, investigación y sanciones correspondientes que permitan atacar de forma certera y definitiva estas acciones.

Esta ley cuenta con 47 artículos de los cuales los más relevantes en cuanto a tipificación de delitos son:

- **Artículo 2-Acceso Ilícito:** En este artículo se tipifica como delito el acceso deliberado y de manera ilegítima a un sistema de información o a parte de el con el objetivo de obtener los datos que se encuentran alojados en estos lugares con una intención propiamente ilícita.

- **Artículo 3- Interceptación ilícita:** en este artículo se tipifica que cada parte dentro del convenio adoptara en su legislación como delito el acto que intercepta de forma premeditada y deliberada a través de diferentes técnicas los datos e información que se encuentran dentro de una comunicación o transmisión privada realizada a través de un sistema de información.

- **Artículo 4-Interferencia de Datos:** En este caso el convenio tipifica como un delito la comisión de manera premeditada y deliberada todo aquel acto que genere un daño, una pérdida o un deterioro a un activo informático.

- **Artículo 5-Interferencia del sistema:** desde este artículo se busca legislar tanto la producción, venta y obtención de funcionalidades de programas informáticos que faciliten la ejecución de los delitos mencionados en los artículos anteriores. De igual forma también se establece como delito la difusión y obtención de contraseñas que permitan tener acceso a diferentes sistemas de información sin autorización.

[15] COLOMBIA.CONGRESO DE LA REPUBLICA. [En línea].Bogotá, D.C. Ley 1928 24 de Julio de 2018. Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, Adoptado el 23 de noviembre de 2001 en BUDAPEST. [Consulta: 23 de Mayo de 2021].Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

- **Artículo 9-Delitos relacionados con la pornografía infantil:** En este artículo se busca adoptar las medidas necesarias para tipificar como un delito los siguientes hechos.

    - La producción de pornografía infantil a través de las visualizaciones y técnicas de difusión mediante un sistema de información.
    - La publicación y puesta de contenido de pornografía infantil en un sistema de información.
    - La difusión de pornografía infantil mediante un sistema de información.
    - La posesión de material de pornografía infantil almacenado en un sistema de información.

.5 DISEÑO METODOLÓGICO

.5.1 TIPO DE INVESTIGACIÓN

El tipo de investigación utilizado en este proyecto aplicado es el descriptivo, esto principalmente porque se especificarán aspectos fundamentales de la estructura lógica de un CSIRT para las pequeñas y medianas empresas.

Se detallarán las herramientas a nivel de software y de hardware necesarias para el funcionamiento de un equipo de respuesta de incidentes informáticos, así mismo mediante una investigación de diferentes referentes bibliográficos se generará un panorama actual de los tipos de ataques y herramientas más utilizadas en las Pequeñas y medianas empresas en cuanto a la seguridad de la información. Se hace uso de datos reales y cifras publicadas en informes de ciberseguridad de compañías especializadas en seguridad informática como INCIBE, KASPERSKY, Efiscalia, entre otras.

De igual manera se detalla y describe cada una de las áreas que pertenecen a la propuesta de la infraestructura tecnológica del CSIRT.

.5.2 ENFOQUE DE LA INVESTIGACIÓN

El enfoque de investigación utilizado en este proyecto aplicado será cualitativo, principalmente porque la investigación está orientada a realizar una revisión bibliográfica de todo el fenómeno de los ataques informáticos e incidentes de seguridad de la información en las pequeñas y medianas empresas, lo que permitirá estudiar como tal el fenómeno de este tipo de incidentes en esta población objetivo a través de documentación y exploración de herramientas que mitiguen este tipo de acciones.

Posterior a estudiar y establecer la visión inicial de la seguridad de la información en las pequeñas y medianas empresas, se procede a interpretar esta información a través de laboratorios que permiten explicar como tal la cualidad en concreto de la importancia de la infraestructura lógica en un CSIRT para las pequeñas y medianas empresas.

.5.3 FUENTES PRIMARIAS

Las fuentes primarias utilizadas en esta investigación serán principalmente revistas científicas, Tesis, Informes de seguridad de la información y diarios o revistas que indiquen información importante para el desarrollo del proyecto aplicado.

De igual forma se hará uso del repositorio de la biblioteca de la Universidad Nacional Abierta y a Distancia, así como los documentos detectados y relevantes en google academics.

.5.4 TÉCNICAS DE RECOLECCIÓN Y ANÁLISIS DE INFORMACIÓN

Las técnicas de recolección y análisis de la información estarán fundamentadas principalmente en la observación ya que a partir de la documentación adquirida mediante las fuentes primarias se permite dar una idea inicial de la Seguridad Informática en las pequeñas y medianas empresas. De esta forma se procede a generar la propuesta de la estructura lógica de un CSIRT el cual se fundamenta en una recolección bibliográfica a través de documentos que citan e indican las herramientas tanto de software como hardware necesarios para poner en marcha este tipo de equipos.

.6 DESARROLLO DE LOS OBJETIVOS

.6.1 EXAMINAR EL PANORAMA ACTUAL DE LA CIBERSEGURIDAD EN PEQUEÑAS Y MEDIANAS EMPRESAS EN COLOMBIA Y LOS ATAQUES QUE HAN CAUSADO MAS IMPACTO EN LA OPERATIVIDAD DE LAS MISMAS

En la actualidad se ha venido incrementando los delitos informáticos en cada uno de los sectores de la economía no solo de Colombia sino a nivel mundial. Este tipo de prácticas generan un gran impacto y afectación para aquellos que son víctimas de estos procesos.

En Colombia según el estudio de tendencias del cibercrimen generado por el programa Seguridad aplicada al Fortalecimiento Empresarial del Tanque de Análisis y creatividad de las TIC (TicTac).[16] Se presentan las diferentes cifras y técnicas de los ciberdelitos efectuados en el año 2019 y a su vez planea las posibles técnicas a las cuales se enfrentarían las empresas colombianas para el año 2020.

En cuanto a cifras el estudio indica que para el año de estudio se registraron 30.410 delitos canalizados a través de los diferentes medios que dispone la Policía Nacional para el registro del mismo. De la totalidad de los casos, a través de la plataforma implementada por la fiscalía para reportar delitos de manera virtual, se denunciaron 17.531 casos relacionados con ciberdelitos. Ante este panorama, el programa de Seguridad Aplicada al fortalecimiento empresarial mediante su estudio indica que, en comparación con el año inmediatamente anterior, en el 2019 se presentó un incremento del 54% en cuanto a incidentes de seguridad de la información.

[16] Cámara Colombiana de Informática y Telecomunicaciones (CCIT), Tanque de Análisis y creatividad de las TIC(TicTac), Centro De Capacidades para la Ciberseguridad en Colombia (c4). [En línea].Informe de las tendencias Cibercrimen en Colombia 2019-2020. Programa seguridad aplicada al fortalecimiento empresarial (SAFE). Octubre 29 de 2019.[Consulta el 26 de Mayo de 2021].Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Ilustración 2.Consolidado delitos informáticos Colombia.

Fuente: Cámara Colombiana de Informática y Telecomunicaciones (CCIT), Tanque de Análisis y creatividad de las TIC(TicTac), Centro De Capacidades para la Ciberseguridad en Colombia (c4). [En línea].Informe de las tendencias Cibercrimen en Colombia 2019-2020. Programa seguridad aplicada al fortalecimiento empresarial (SAFE). Octubre 29 de 2019. [Consulta el 26 de Mayo de 2021].Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

En cuanto a los delitos más comunes según el estudio se plantean los siguientes:

- **Hurto por medio Informático**, en este caso los delincuentes son conscientes que el dinero se encuentra en las cuentas bancarias, razón por la cual buscan comprometer todos los dispositivos usados para hacer las diferentes transacciones virtuales que permiten las entidades bancarias. Si bien es cierto que este delito suele presentarse mayormente en personas naturales, los ciberdelincuentes han empezado a ver una oportunidad de ataques efectivos en las pequeñas y medianas empresas ya que estas no cuentan con grandes estándares de seguridad informática y por ende se convierten en blancos fáciles.

- **Violación de datos personales.** Según el estudio de tendencias de cibercrimen, para el año 2019 se reportaron aproximadamente 8.037 ciberdelitos.

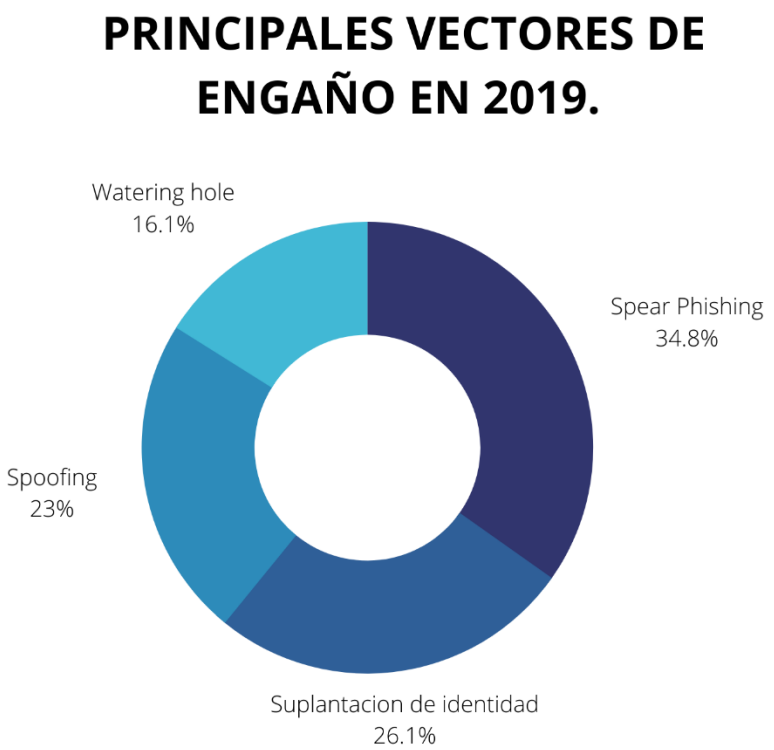
- **Acceso Abusivo a Sistemas de información.** Se reportaron 7.994 casos de delincuentes que buscan acceder a los sistemas de información a través de diferentes técnicas que comprometen la seguridad del dispositivo.

Ahora bien, en cuanto a ubicación geográfica de los ataques según (SAFE), los principales ataques se presentan en Bogotá, Cali, Medellín, Barranquilla y Bucaramanga; de esta forma del total de los delitos para el 2019, en estas 5 ciudades se concentra el 55% de los casos denunciados.

Si bien es cierto que los ataques suelen estar dirigidos y agruparse en las grandes ciudades, los delincuentes ven un objetivo de mayor lucro y mayor incidencia en las entidades financieras y en las Pequeñas y medianas empresas ya que es en las últimas donde se pueden llegar a presentar ciberdelitos de manera accesible por el poco control y la poca implementación de políticas de Seguridad de la Información; esto sumado a las restricciones con las que cuentan estas organizaciones en cuanto a inversiones tecnológicas ya que suelen contar con presupuestos muy ajustados a cumplir sus objetivos organizacionales y por ende no dedican recursos ni físicos ni humanos a mejorar la infraestructura tecnológica para disminuir los ciberataques los cuales se han aumentado de manera exponencial generando daños críticos para las organizaciones.

En cuanto a los principales vectores de engaño que se ocupan para cometer los diferentes delitos informáticos, los correos fraudulentos personalizados mejor conocidos como Spear Phishing ocupan el primer lugar con el 34.8% para el año 2019.

Ilustración 3.Principales vectores de engaño delitos informáticos 2019.



Fuente: Cámara Colombiana de Informática y Telecomunicaciones (CCIT), Tanque de Análisis y creatividad de las TIC(TicTac), Centro De Capacidades para la Ciberseguridad en Colombia (c4). [En línea].Informe de las tendencias Cibercrimen en Colombia 2019-2020. Programa seguridad aplicada al fortalecimiento empresarial (SAFE). Octubre 29 de 2019. [Consulta el 26 de Mayo de 2021].Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Según el estudio, para las Pequeñas y Medianas empresas que sufren ataques informáticos, el 60% de estas posterior a los 6 meses de recibir una vulneración a sus activos informáticos no pueden mantenerse en el mercado y no logran superar las afectaciones de estos delitos razón por la cual se ven obligados a finalizar su empresa.

Según Kaspersky [17] a través de un estudio realizado concluye que si bien es cierto que las empresas son conscientes de la protección de sus datos y por ende la necesidad de contar con una infraestructura tecnológica lo suficientemente robusta para asegurar esta protección, no es fácil para este tipo de organizaciones ya que en muchas ocasiones cuentan con una minoría de empleados y oficinas muy pequeñas que imposibilitan estos procesos. Razón por la cual según Kaspersky, el 29% de las PYMES en el año 2019 prefieren subcontratar los procesos de Ciberseguridad con entidades externas ya que representan procesos mucho más efectivos e inmediatos. Esta cifra sin lugar a dudas

[17] Kaspersky Team. KASPERSKY Daily. [Sitio web]Cuidado con las brechas: la protección de los datos en las pequeñas empresas.20 de Septiembre de 2018.[Consulta el 25 de Mayo de 2021].Disponible en:https://www.kaspersky.es/blog/data-protection-for-smb/19280/#methodolgy

puede representar un incremento considerable en el mercado de soluciones de Seguridad Informática en Colombia, principalmente porque el 90% de las empresas en el país pertenece al sector de las Pequeñas y Medianas empresas, la cifra asciende a 2.540.953 PYMES registradas para el año 2019.

Ante estas cifras altamente relevantes para las empresas de todo tipo en la actualidad, diferentes compañías han empezado a compilar una serie de recomendaciones, estándares y herramientas útiles para disminuir no solo los ataques informáticos sino el impacto de estos sobre la operatividad de las Pequeñas y medianas empresas.

Kaspersky Latinoamérica [18] indica principalmente que en el panorama actual, las PyMes se encuentran ante el reto de la migración al mundo digital para transformar sus operaciones y poder adaptarlos a las necesidades de la época, razón por la cual no solo tienen como reto la migración tecnología sino también todo aspecto que comprenda temas de Seguridad de la Información. Esta misma compañía plantea unos puntos fundamentales de ciberseguridad que permitan desligar preocupaciones de las diferentes empresas en este tipo de temas. Los puntos más importantes de la guía son:

- **Identificación de los riesgos:** Este aspecto si bien es cierto aplica para cualquier tipo de empresa, en el caso de las PyMES es fundamental ya que deben de conocer a detalle debido a la cantidad limitada de recursos tecnológicos lo correspondiente las características de dichos equipos, las redes con las que cuenta la compañía y todo activo informático que implique algún proceso como tal en la empresa. A partir de este análisis se podrá realizar una estimación del riesgo para cada uno de estos equipos.

- **Mantener actualizados todos los equipos:** Si bien es cierto que muchas PyMES cuentan con un presupuesto reducido, lo ideal es que cada licencia que se utilizará en la compañía cuente con la licencia correspondiente con el fin de evitar un mayor riesgo.

- **Realizar Copias de seguridad:** Aspecto fundamental para las PyMES ya que, en caso de un ataque informático, a través de las copias de seguridad el impacto ocasionado por dicho ataque será menor.

- **Utilizar Soluciones de seguridad informática:** Kaspersky dentro de sus herramientas cuenta con una solución llamada *Kaspersky Endpoint Security Cloud.E*sta herramienta permite proteger todos los activos informáticos de la compañía a través de soluciones que se encuentran alojadas en los propios servidores de Kaspersky lo que hará que la administración sea mucho más intuitiva y fácil para los encargados del área de tecnología de la empresa. Funciona principalmente a través de las herramientas de bloqueo que posee la compañía en

[18] Kaspersky Latam.[Sitio web].Ciberseguridad: la aliada de las PyMES durante la realidad actual.25 de Junio de 2020 Consulta: el 29 de Mayo de 2021].Disponible: https://latam.kaspersky.com/about/press-releases/2020_ciberseguridad-la-aliada-de-las-pymes-durante-la-realidad-actual

cuanto a Ransomware, malware y demás ataques informáticos. De esta forma Kaspersky no solo bloquea este tipo de procesos delictivos, sino que también puede crear terminales remotas para de esta forma proteger los activos informáticos generados e implementados por medio del teletrabajo el cual también representa un riesgo adicional para la compañía. Por último, la herramienta le permite al administrador tener un control total de las soluciones y detecciones realizadas a través de la nube en un tablero de indicadores que facilita la toma de decisiones.

La compañía iBiS Computer [19] complementa las recomendaciones realizadas por Kaspersky con recomendaciones indispensables para mejorar la seguridad informática en la compañía.

- **Políticas de Contraseñas Seguras:** En este caso se recomienda que ninguna contraseña utilizada para los procesos de la compañía sea la que arroja el mismo sistema por defecto. Lo ideal es contener una contraseña con símbolos alfanuméricos, mayúscula, minúscula y demás para lograr una robustez elevada en dicha contraseña que haga difícil la detección de la misma.

- **Aumentar conciencia de actividades sospechosas**: Aspecto fundamental ya que es a través de la intuición que se pueden prevenir la mayoría de ataques informáticos. La mejor herramienta es el sentido común, si algo parece peligroso lo mejor es no darle clic.

Según el documento de la Tesis de Master de Ángela María Parra Giraldo, publicado por la Universidad Internacional de la Rioja Unir [20] la implementación de la Norma ISO 27001 sería una excelente alternativa para las Pequeñas y medianas empresas en cuanto a estándares de seguridad de la información. Esto principalmente porque según el documento en Colombia existen una serie de regulaciones y normativas que le exigen a las empresas a partir del número de empleados diferentes implementaciones de herramientas que aseguren la información y garanticen el correcto funcionar de la organización.

Para las PyMES la ISO 27001 sería una excelente alternativa para garantizar todo su proceso de seguridad de la información, si bien es cierto que esta norma es transversal a cada organización, es decir cada empresa determina que controles desea implementar de acuerdo a sus capacidades y a sus necesidades.

---

[19] IBis Computer. Blog Ibis Computer. [Sitio web]. 5 prácticas de ciberseguridad para pymes en 2021. [Consulta el 29 de Mayo de 2021].Disponible:https://www.ibiscomputer.com/blog/128-5-practicas-de-ciberseguridad-para-pymes-en-2021

[20] PARRA GIRALDO, Ángela María. [En Línea]. ISO 27001 PARA PYMES. Universidad Internacional de la Rioja Master Universitario en Seguridad Informática. Trabajo Fin de Master. 18 de octubre de 2014. [Consulta: el 29 de mayo de 2021.]. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/3128/AngelaMaria_Parra_Giraldo.pdf?sequence=1&isAllowed=y

Esta norma centra su actuar en 4 pasos. Planificar, Hacer, Verificar y actuar.

Otro de los Marcos que las Pequeñas y medianas empresas están empezando a implementar en las organizaciones para disminuir los incidentes de seguridad informática es el Marco CSF (Cybersecurity Framework). Este fue creado por el Instituto Nacional de Estándares y Tecnología. Dentro de los sectores de infraestructura crítica que identifica este marco se encuentran las pequeñas y medianas empresas en diferentes sectores de la economía. Razón por la cual se crea para identificar aquellas normas y diferentes directrices de seguridad aplicadas en los diferentes sectores críticos de infraestructura de tal manera que mediante enfoques adaptables y continuos facilita la priorización de las actividades que se requieren para mejorar el rendimiento de dichas organizaciones y de esta forma mantener una economía estable en los diferentes mercados.

Este marco fue creado en EEUU en el año 2013[21] buscando principalmente implementar una serie de enfoques que permitieran disminuir de manera exponencial los diferentes riesgos generados en los sectores de la economía desde el punto de incidentes de seguridad informática. De igual forma busca aumentar tanto el rendimiento como la rentabilidad de una organización basado principalmente en el tratamiento del riesgo generado del posicionamiento de una organización en el mercado determinado. Los principales componentes de este marco son:

- **Framework Core:** Este componente consta principalmente de una serie de actividades y resultados de seguridad informática basados principalmente en diferentes categorías que suelen estar alineadas con las normativas que corresponden al tipo de organización donde se implementara. Su difusión se facilita ya que utiliza un lenguaje basado en lo simple más que en lo técnico, razón por la cual es mucho más aplicable a todas las áreas de la organización.

- **Niveles de implementación del CSF:** Este componente se basa en definir el grado de los riesgos aplicados a la organización. Este grado puede llegar a ser dese nivel 1 que corresponde a riesgo parcial, nivel 2 que hace referencia a el riesgo informado, nivel 3 que se refiere al nivel repetible y el nivel 4 que indica el riesgo adaptado.

[21] OEA.AWS. [En Línea].CIBERSEGURIDAD MARCO NIST.Un abordaje integral de la Ciberseguridad. [Consulta el 15 de junio de 2021.] Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Ilustración 4. Niveles Marco CSF

Fuente: OEA.AWS. [En Línea].CIBERSEGURIDAD MARCO NIST.Un abordaje integral de la Ciberseguridad. [Consulta: el 15 de junio de 2021.] Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

- **Perfiles:** En este componente se incluye la alineación que se da entre los requisitos del marco y los objetivos organizacionales de la empresa. De esta forma se determina la tolerancia que pueda llegar a tener una organización a los diferentes tipos de riesgos.

Otro de los Marcos que las Pequeñas y medianas empresas han empezado a adaptar y a sincronizar con sus objetivos organizacionales es el Marco Cobit (Control Objetives for Information and related Technology). Este marco principalmente le facilita a una organización la construcción de políticas de seguridad de la información claras y puntuales, de igual forma apoya la generación de buenas prácticas de control de herramientas tecnológicas en las empresas. Permite la comprensión, la administración y la evaluación correcta de los riesgos asociados a la organización generando así una serie de beneficios para la organización.

Este marco dentro de su desarrollo hace especial énfasis en la información, ya que considera que es el recurso clave por el cual un Pyme puede crecer e incluso ser destruida en un mercado determinado. Razón por la cual este tipo de empresas no son ajenas a este reto de proteger la información y se ven en la necesidad de adoptar marcos y estrategias que permitan no solo proteger el principal activo como lo es la información sino también alcanzar los objetivos organizacionales a través de la optimización de procesos de seguridad informática.

Si bien es cierto que una empresa que pertenezca al sector de las Pymes suele contar con recursos limitados, el marco COBIT no se limita ni se construye en base a grandes infraestructuras, por el contrario se adapta a cualquier tipo de organización, de tal manera que si la organización en concreto cuenta con una infraestructura muy limitada, basara con contar con pocas políticas concisas y claras para cubrir toda la naturaleza de la empresa y protegerla ante incidentes de seguridad informática.

Por ultimo las pequeñas y medianas empresas dentro de sus objetivos organizacionales están incluyendo análisis o procesos menos robustos y por ende requieren menos recursos, generando así un beneficio en aspectos de la seguridad informática. Tal es el caso del Análisis DOFA**,** En este caso el análisis lo que busca es evaluar las debilidades, fortalezas, amenazas y algunas oportunidades de un proyecto que se tenga estructurado. De esta forma se estructura una matriz en donde se ubican bien sea las fortalezas, oportunidades, amenazas y debilidades para de esta forma ponderar los aspectos más relevantes.

En cuanto al Análisis PEST**,** éste tipo de herramienta o análisis sirve para estudiar a fondo el público objetivo para de esta forma comprender las circunstancias que rodean como tal a este grupo de clientes en donde se piensa ofrecer o implementar el CSIRT.

.6.2 ESTRUCTURAR LA INFORMACION RELACIONADA CON HERRAMIENTAS DE HARDWARE Y SOFTWARE QUE PERMITAN DESARROLLAR LAS ACTIVIDADES DEL CSIRT TENIENDO PRESENTE EL CATALOGO DE SERVICIOS.

SERVICIOS OFERTADOS POR EL CSIRT PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

Dentro de la creación de un CSIRT, que para este caso se implementara y centrara sus funciones en el sector de las pequeñas y medianas empresas es fundamental determinar cuáles serán los servicios que prestara y que herramientas apoyaran la ejecución de dichos servicios en función de apoyar a las Pequeñas y Medianas empresas a resolver incidentes de seguridad informática.
Los servicios que se prestaran serán tanto reactivos como proactivos, es decir el Equipo de respuesta a incidentes informáticos no solo se centrara en ofrecer su portafolio de servicios basados en solucionar los problemas que presentan las organizaciones en un momento determinado, también prestara dentro de su portafolio procesos que permitan generar alertas, capacitaciones y demás ítems que sirvan como base en una organización para solucionar incidentes que no requieren ser escalados hasta este tipo de Equipos especializados.

.6.2.1 SERVICIOS PROACTIVOS

Como se mencionó actualmente, el CSIRT prestara servicios que permitan prevenir y anticiparse a los posibles ataques que puedan llegar a recibir las organizaciones. De esta forma se pueden llegar a disminuir futuros incidentes puesto que las empresas tendrán el conocimiento necesario para discernir entre riesgos potenciales para su empresa y cómo abordarlos.

.6.2.1.1 Análisis y monitoreo infraestructura tecnológica

Este equipo cuenta dentro de su estructura organizacional con funcionarios que realizan un monitoreo remoto de las organizaciones para de esta forma determinar malas prácticas o maquinas potencialmente riesgosas para una empresa. Ellos serán los encargados de realizar un análisis de vulnerabilidades web de los diferentes Aplicativos y portales web que posee la organización para determinar posibles vulnerabilidades y proceder a subsanarlas para disminuir los riesgos.

- **Software:**

Process Explorer: Este es un software que permite monitorear todos los procesos, las aplicaciones y las tareas que se están ejecutando en el ordenador que está siendo vigilado. El programa listara de una manera detallada las librerías y la cantidad de

recursos que pueda llegar a consumir un determinado proceso, adicional a esto permite en caso de encontrar procesos sospechosos se puede finalizar el proceso o modificar su ejecución hasta que se pueda revisar a detalle que función está realizando el proceso en el ordenador.
En este caso el profesional encargado de realizar la vigilancia se conectará remotamente a los diferentes equipos de la organización y realizará una inspección utilizando esta herramienta para determinar maquinas potencialmente infectadas o en riesgo.

Nexpose: Esta es una herramienta que permite realizar un escaneo de vulnerabilidades tanto de una red como de un activo web. Funciona básicamente identificando cuáles son los servicios que se tienen activos, que puertos tienen abiertos y que aplicaciones se están ejecutando en la máquina. Estos resultados suelen ser mostrados en un informe generado por el mismo software en donde hace una priorización de las vulnerabilidades detectadas y el impacto de estas para de esta forma tener la información necesaria para iniciar a mitigar las vulnerabilidades más críticas para la organización.

CIRCL AIL Analysis of Information Leaks: Marco para el análisis de fugas de información.
Esta herramienta permite el análisis y detección de posibles filtraciones de la información o de fuentes de datos que no estén estructuradas dentro de un sistema. Es una herramienta muy útil para un CSIRT ya que permite:

- Detección de la URL, de igual forma permite ubicar geográficamente la dirección IP correspondiente.
- Permite detectar posibles intromisiones a bases de datos bancarias.
- Cuenta con un apartado que permite extraer direcciones de navegadores anónimos como Tor. onion, entre otros.
- Facilita la creación y la consulta de estadísticas sobre módulos y aplicaciones web.
- Cuenta con diferentes módulos que permiten extraer una gran cantidad de información.
- Permite desencriptar archivos que contengan codificaciones tales como Base64, Codificación hexadecimal e incluso codificaciones personalizadas.
- Permite rastrear intervalos regulares URL o aquellos servicios que se encuentren ocultos en Tor.

- **Hardware:**

En este servicio prestado será necesario contar con computadores portátiles que permitan no solo realizar monitoreo, sino que también puedan continuar con el resto del proceso establecido ante el hallazgo de un incidente de seguridad informática.
Para el CSIRT se utilizarán portátiles Lenovo ThinkPad T14 2da Generación de 14 pulgadas.

Estos equipos cuentan con un procesador Intel Core i7 DE 11va generación, dentro de sus componentes cuenta con una tarjeta gráfica NVIDIA GeForce Mx450 que facilitara

la ejecución de diferentes herramientas de software necesarias para prestar los servicios requeridos.

IPS: Este es un sistema de prevención de intrusos, puede considerarse desde el punto de vista o hardware depende la elección de la herramienta. Su principal función es la de revisar y verificar el tráfico que pasa por la red con el fin de poder lograr la detección de posibles delincuentes que se encuentren escuchando la información que allí se transmite para programar futuros ataques. Su funcionamiento se puede considerar como una herramienta para los servicios proactivos de un CSIRT ya que son reacciones que se dan en el momento en que se detecte el ataque.

.6.2.1.2 Auditorias de Seguridad Informática.

Este equipo cuenta con un profesional Auditor en sistemas informáticos idóneo que podrá realizar este tipo de procesos dentro de las organizaciones que harán parte de las empresas beneficiadas por el CSIRT. El objetivo de brindar este servicio a las pequeñas y medianas empresas es poder realizar una auditoria completa de toda la infraestructura tecnológica determinando no solo los equipos con un riesgo superior sino estableciendo planes de mejora que le permitan a la organización mitigar el impacto y la probabilidad de que un riesgo detectado pueda generarse.

- **Software:**

Para prestar este servicio se utilizará una plantilla diseñada propiamente por el equipo técnico del CSIRT en donde se establezcan los criterios más importantes de la infraestructura tecnológica, todos los procesos, responsables, equipos y demás ítems que pueden dar una visión de la empresa a nivel informático como tal.

También se utilizará la Matriz de análisis y gestión de riesgos publicada en la Metodología Magerit. Esta busca principalmente hacer un análisis de riesgos en los activos identificados en la empresa, posteriormente se ponderan estos riesgos generando así los riesgos que pueden llegar a generar mayor daño o que pueden ser más críticos para la organización.

Esto será de utilidad principalmente para determinar ante un incidente de Seguridad Informática dentro de una organización, cuál sería el impacto de este sobre los activos que se cuentan.

- **Hardware:**

En cuanto al Hardware, se utilizará el mismo equipo portátil Lenovo ThinkPad T14 2da Generación de 14 pulgadas, principalmente porque el profesional que realiza la vigilancia de infraestructura también será el que realice las auditorias de manera presencial o remota.

Se contará con un disco duro Toshiba de 2 Tb que le permitirán al profesional almacenar toda la información relevante de la Auditoria para posteriormente ser analizada por el resto del equipo.

.6.2.1.3 Desarrollo de herramientas de Seguridad.

Este servicio es fundamental para el CSIRT ya que dentro de su estructura organizacional cuenta con un área para la investigación y el desarrollo, así como para realizar laboratorios que les permitan determinar y crear herramientas que puedan solucionar incidentes de seguridad informática que no requieren un proceso tan exhausto en cuanto a su solución.

- **Software:**

VirtualBox: Este es un software que permite crear máquinas virtuales bien sea con Windows o con cualquier otro sistema operativo que sea seleccionado. Es fundamental para este servicio del CSIRT ya que permitirá generar diferentes máquinas virtuales con múltiples sistemas operativos para proceder a generar ataques controlados y posterior a esto iniciar con el desarrollo de herramientas que den respuesta a este tipo de ataques.

VisualStudio: Es un entorno de desarrollo integrado para sistemas operativos Windows y MacOS. Permite generar aplicativos con una gran cantidad de lenguajes como lo son_ C++, C#, Visual Basic, Java, entre otros. Es multiplataforma y es fácilmente adaptable a cualquier necesidad que pueda llegar a tener un desarrollador.

Para el caso del CSIRT, esta herramienta será fundamental ya que permitirá crear aplicaciones de Seguridad Informática a través de los diferentes lenguajes de programación que decidan los profesionales implementar.

- **Hardware**

Equipos Computo: Se utilizarán equipos portátil Lenovo ThinkPad T14 2da Generación de 14 pulgadas.

Se hará uso de una Workstation P310 que cuenta con un procesador Intel XEON E3-1280 V5. Este equipo será de gran ayuda para ejecutar este tipo de servicios principalmente porque se necesitan tener instaladas diferentes tipos de máquinas virtuales todas con características múltiples lo que puede generar una disminución de los recursos del equipo en el que se ejecuta, lo que puede llegar a generar una baja de rendimiento del CSIRT como tal.

.6.2.1.4 Educación, entrenamiento y concienciación sobre Seguridad Informática.

Este servicio que será ofertado en el CSIRT para las pequeñas y medianas empresas consiste principalmente en la creación de planes educativos y de formación en aspectos esenciales de la Seguridad Informática.

Estos entrenamientos se dividirán en niveles empezando desde el más básico hasta el más avanzado que sea posible dictar a través de los profesionales con los que cuenta el CSIRT para esta labor.

Dentro de este servicio, se plantea dictar charlas a las diferentes empresas del sector de las PYMES para que puedan aumentar su identidad y su apropiación en cuanto a los activos informáticos de la organización, esto se busca principalmente porque al lograr obtener una serie de profesionales con alta conciencia por proteger los activos a cargo, se disminuirá el riesgo que puede generar las malas prácticas al momento de hacer uso de los equipos.

Puede ser dictado de forma virtual o presencial dependiendo la necesidad del cliente, para esto el CSIRT cuenta con una sala de capacitaciones en caso de que las actividades sean presenciales, caso contrario se pueden dictar desde la sala de juntas la cual contara con un equipamiento necesario para transmitir el conocimiento de la mejor manera posible.

- **Software y Hardware**

Cisco Webex Room: Esta es una herramienta diseñada por la compañía Cisco, la cual consiste principalmente en un sistema integrado que permite crear un escenario de video avanzado y especializado. Cisco Webex Room permite habilitar cualquier espacio en un centro colaborativo ideal para capacitaciones y reuniones con clientes potenciales.

Cuenta con 2 pantallas LED de 70 pulgadas que pueden estar sincronizadas o en su defecto proyectando datos diferentes en cada una.

Este dispositivo cuenta con cámara, altavoces y micrófonos integrados, lo que facilita la difusión del contenido de manera tanto presencial como virtual.

Por ultimo cuenta con un software especializado que permite conectarse con cualquier empresa en cualquier parte del mundo de manera sencilla y rápida, es multiplataforma y puede integrarse con un sinfín de dispositivos electrónicos que pueden ayudar a mejorar la experiencia del servicio.

Cisco Webex Share: Sumado a la plataforma Webex Room, el CSIRT cuenta también con un dispositivo que permite compartir pantalla en cualquier pantalla sin necesidad de tener cables o adaptadores. Su diseño minimalista les facilita los procesos a los

funcionarios del CSIRT que prestan este servicio de manera presencial en las diferentes empresas que lo soliciten.

Adicional a los servicios anteriores, también se contará con profesionales que apoyen la parte de las comunicaciones generando informes de gestión, noticias y demás información que permita captar más clientes. Así como asistiendo a eventos que sean de interés general para el CSIRT y que permitan generar nuevos procesos como tal en la organización.

Se hará uso de una herramienta de software indispensable para las comunicaciones el cual es la página web o sitio web publico explicada a continuación.

Sitio Web público: Sí bien es cierto, esta no se considera una herramienta como tal, aunque contar con ella es parte fundamental para el desarrollo de un CSIRT. Esto debido a que en su mayoría el primer contacto que pueda llegar a tener las personas con estos equipos se da a través de un sitio web. Desde allí estos equipos pueden compilar y publicar la información más relevante de la organización como tal. De igual forma desde un sitio web el equipo de respuesta puede publicar constantemente informes de vulnerabilidades y ataques solventados para que de esta forma el usuario pueda reconocer algunos de los comportamientos similares de estos ataques y los relacione con la organización en donde se encuentra. Por último, tener un sitio web con una interfaz llamativa hará que el usuario pueda sentir confianza de estar en este sitio y seguramente dará el paso hacia contactarlos y contratar los servicios respectivos.

.6.2.2 SERVICIOS REACTIVOS

.6.2.2.1 Alertas y Avisos

Dentro de este servicio se tiene como tal las publicaciones de alertas y avisos que corresponden a incidentes de Seguridad Informática presentes y detectados por las grandes compañías de Ciberseguridad en el mundo.

El CSIRT hará la difusión de esta información a través de la página web, así como el correo electrónico para permitir obtener una mejor difusión y llegar a la mayor cantidad de clientes y empresas posibles.

- **Software:**

OWASP Top Ten: Esta herramienta online es fundamental a la hora de generar un informe de amenazas actuales, de vulnerabilidades o de diferentes ataques conocidos dentro del ciberespacio.

Básicamente es un documento estándar que presenta los riesgos de Seguridad de la Información más críticos para las aplicaciones web.

CSIRTs by Country-Interactive Map: Dentro del proceso de generar alertas y avisos, conocer la información publicada por otros equipos de Respuesta a Incidentes Informáticos es muy importante, razón por la cual este mapa interactivo donde listan los CSIRT más importantes del mundo junto con el enlace para visitar el sitio web permitirá conocer las amenazas y ataques publicados por ellos para posteriormente analizar si este tipo de delitos informáticos aplican para el sector de las Pequeñas y Medianas empresas y si dentro de los reportes de incidentes actuales se está presentando con frecuencia.

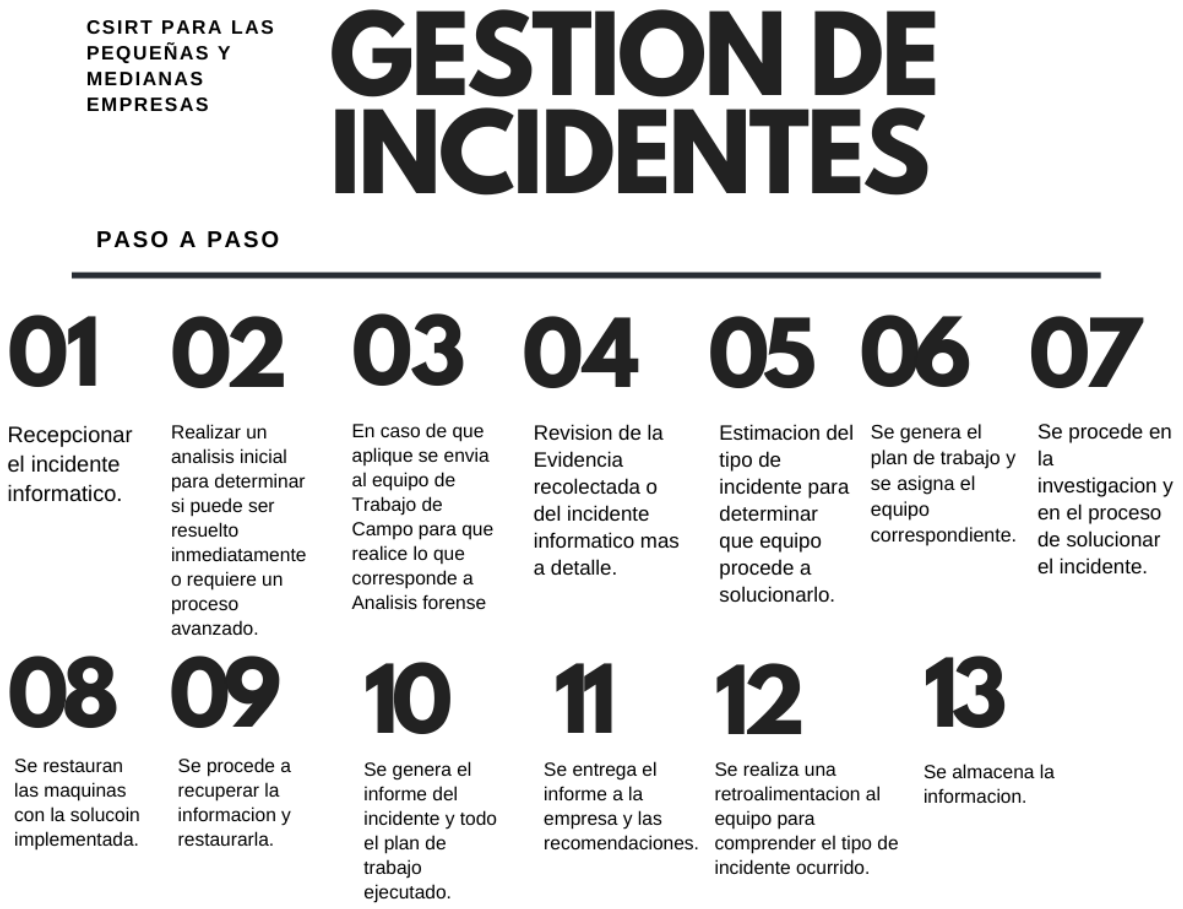
Cisco Secure Email: Debido a que la información si bien es cierto será publicada a través de la página web, también existirán documentos, amenazas y avisos que serán enviados por correo electrónico. Es por esta razón que es fundamental asegurar el correo con el fin de que no sea suplantado y termine siendo objeto de un ataque informático a las empresas que reciben la información.

Esta herramienta permite proteger el correo electrónico de las amenazas más frecuentes y dañinas en la red; cuenta con una estructura de defensa en varias capas lo cual aumenta sus niveles de seguridad a tal punto que va a ser un blanco difícil para los atacantes.

.6.2.2.2 Gestión de Incidentes

Este es sin lugar a dudas el servicio más importante dentro de un CSIRT, de hecho, es un servicio indispensable para este tipo de organizaciones. Dentro de este se contempla ejecutar todo lo que corresponde a la gestión y manejo de un Incidente de Seguridad Informática, desde la recepción del incidente hasta la entrega del informe final a la organización atacada y las recomendaciones finales.
Como se puede ver en la figura a continuación, cuenta con 14 pasos que evidencian el flujo que puede llegar a tener un incidente al momento de ingresar al CSIRT.

Ilustración 5.Paso a paso para la Gestión de Incidentes CSIRT



Fuente Propia.

- **Software:**

Clasificación BGP Gnup:
Esta es una variación del estándar OpenPGP. La herramienta facilita el cifrado y la firma de los datos y las respectivas comunicaciones por donde pasan estos. Funciona a través de comandos lo que facilita la integración con otras implementaciones.

Sin lugar a dudas contar con una alternativa que permita proteger la privacidad es un paso inicial para salvaguardar la información puesto que las contraseñas serán de más difícil acceso y no es fácil para un atacante encontrar el tipo de cifrado con el que cuenta nuestro sistema de información.

Para un CSIRT tener una aplicación como esta permite manejar una serie de datos cifrados, encriptar los correos y los paquetes enviados por la red para de esta forma evitar que atacantes ingresen a nuestro sistema y puedan detectar los datos que circulan en ella.

Request Tracker for incident Response:
RTIR es una herramienta que suelen usar muchos de los CSIRT en el mundo, permite encontrar patrones comunes entre los diferentes informes de los incidentes. De esta forma mediante datos claves podrá vincular diferentes incidentes y de esta forma conocer comportamientos comunes y aplicarlos en la solución del incidente presentado.

Esta solución permite crear una red de CSIRT de esta forma cada uno retroalimenta a los otros lo que permite sin lugar a dudas la optimización de tiempo y la ejecución de respuesta a ataques ya presentados casi que inmediata.

CVE Search:
Esta es una herramienta de código abierto mayormente usada por aquellos investigadores en seguridad de la información. Lo que hace útil la herramienta es la facilidad para descargar todas las vulnerabilidades registradas en CVE (Common Vulnerabilities and Exposures) y también en CPE (Common Platform Enumeration); posterior a la descarga de dichas vulnerabilidades la herramienta optimiza considerablemente la búsqueda de los dichos hallazgos.

El principal objetivo de CVE es ahorrarse el tiempo que conlleva ingresar directamente a estas bases de datos y buscar, puesto que debido a la cantidad de recursos este proceso llevaría mucho tiempo. De esta manera, al instalar estas descargas en una base de datos MongoDB, las búsquedas se podrían hacer sin necesidad de conectarse a internet.

Para hacer uso de esta solución se necesitaría una instalación de Python en su versión más reciente, adicional a esto lógicamente se deberá tener instalado un gestor de base de datos MongoDB en su última versión. También se necesitan una serie de extensiones y packs que requiere Python para funcionar correctamente.

IntelMQ:
Esta es una de las herramientas más usadas por todos los equipos de seguridad en todo el mundo. Consiste principalmente en recopilar y procesar a través de algoritmos de búsqueda inteligente las amenazas y los procesos que se llevan a cabo para solucionarlas para de esta forma optimizar el tiempo y la recopilación de los procesos dentro de estos equipos.

Sus bondades pueden ser aplicadas para la gestión de manejo de los incidentes, reconocimiento del escenario, notificaciones automáticas y lógicamente como recopilador de información y otras herramientas útiles para el CSIRT.
Las principales funciones que presenta IntelMQ son:

- Disminuir el tiempo que conlleva administrar un Sistema de un Equipo de Respuesta de Incidentes Informáticos.
- Disminuir la dificultad para escribir bots para diferente información.
- Disminuir la perdida de eventos en el procesamiento del CSIRT.
- Implementar Json para la gestión de los mensajes.

- Crear Fácilmente listas negras.

N6 (Network Security Incident eXchange):
Esta herramienta fue creada principalmente para recopilar, procesar y posteriormente distribuir información sobre amenazas de seguridad de la información. Se podría decir que hace las veces de centro de procesamiento de información, optimizando de esta forma todos los datos que son más relevantes, sus respectivos dueños y las redes en las que opera.

Las fuentes de datos que soporta esta aplicación son: CSIRT, CERT, Proveedores de herramientas de seguridad de la información, Organizaciones sin fines de lucro, Investigadores de Seguridad de la información.

TheHive:
Esta herramienta de código abierto está especialmente diseñada para favorecer a los SOC, CSIRT, CERT respecto a los análisis de código gratuito en cuanto a incidentes de seguridad informática.

Sus principales funciones son:

- Colaborar: en este caso los profesionales que hacen parte de estos equipos de respuesta pueden retroalimentarse entre sí incluso con transmisiones en vivo acerca del procesamiento y el manejo que se le da a un caso real. Permite asignar tareas y notificarles a los encargados los tiempos de esta.
- Elaborar: Permite lógicamente el desarrollo de estas tareas y la posterior documentación, también optimiza el tiempo de los profesionales usando plantillas para de esta forma automatizar la documentación de incidentes.
- Monitorear: De esta forma los profesionales pueden indagar IPs, Direcciones de correo electrónico y demás portales para de esta forma analizar y detectar vulnerabilidades que puedan generar un riesgo latente.

GcNotify:
Esta más que una herramienta es una extensión que puede hacerse con Outlook, en donde su funcionalidad consiste en reenviar aquellos correos electrónicos de procedencia sospechosa a el equipo de Seguridad de la Información dentro de una Organización.

El archivo se envía automáticamente a las direcciones electrónicas previamente establecidas por el equipo de Seguridad de la Información con toda la información necesaria para hacer el análisis correspondiente y detectar un posible ataque o por qué se considera un correo malicioso.

Es altamente personalizable, sencilla de usar y permite enviar uno o muchos correos electrónicos como archivos adjuntos.

CimSweep:
Más allá de ser una herramienta, esta es un conjunto de diferentes aplicaciones que permiten realizar y ejecutar procesos de búsqueda y respuesta de incidentes de seguridad de la información en el sistema operativo Windows.

Es bastante potente, sin embargo, su implementación puede ser algo compleja lo mismo que su uso ya que requiere reglas de validación. Ahora bien, estas implementaciones disminuyen el tiempo que pueda invertir un agente para personalizar los procesos, estos complementos lo hacen todo de forma automática. Permite obtener información sensible como:

- Claves de registro, tipos de valor y contenidos con alto valor para el equipo de respuesta a incidentes.
- Directorio de recursos.
- Entradas de registros a los eventos.
- Servicios
- Procesos.

Virus Total:
Esta es una herramienta online gratuita para los usuarios finales. Se encuentra publicada en https://www.virustotal.com/gui/. Funciona principalmente inspeccionando a través de diferentes escáneres de antivirus y listas de bloqueos de URL un archivo subido a la plataforma. Luego de realizar este análisis, se muestran los resultados básicos o más completos dependiendo el paquete seleccionado, en donde indica la información del archivo escaneado y si se encuentra dentro de las diferentes librerías y ha sido detectado como un archivo malicioso, esta herramienta informa en caso de detectar código malicioso, la etiqueta de detección como tal del archivo.

Sirve tanto para los servicios reactivos como proactivos de un CSIRT, ya que si bien es cierto que este permite detectar un archivo sospechoso y comprobar que es un virus en el momento de un incidente de Seguridad Informática, también cuenta con una comunidad en donde se retroalimentan conocimientos acerca de los archivos ingresados e incluso existen votaciones para determinar el riesgo de diferentes tipos de contenido malicioso.

No More Ransom
Esta es una herramienta en línea que se encuentra publicada en https://www.nomoreransom.org/ generada a través de una iniciativa de los países bajos, el Centro Europeo de Delitos Cibernéticos de Europa, Kaspersky y McAfee, su principal función es ayudar a todos los usuarios que son víctimas de ransomware a recuperar sus archivos sin acceder a las pretensiones del atacante que en su mayoría son económicas.

Esta herramienta se considera apta para los servicios reactivos y proactivos de un CSIRT ya que a través de un ataque de Ransomware se puede ingresar a esta URL y diligenciar la información solicitada para detectar el tipo de ataque presentado y posteriormente proceder a desencriptar los archivos secuestrados para ser restaurados en un equipo sin código malicioso. De igual forma también es apta para prestar un servicio proactivo ya que la iniciativa busca también educar a los diferentes usuarios sobre la funcionalidad de un ataque a través de un ransomware, lo que permitirá tomar medidas de prevención ante este tipo de infecciones.

ESET SysInspector:
Esta es una herramienta gratuita publicada por la compañía ESET que permite realizar diagnósticos de los equipos. Está integrada con las diferentes herramientas de la compañía como lo son: ESET NOD32 Antivirus, ESET Internet Security y ESET Smart Security Premium.

Busca principalmente detectar códigos maliciosos en el equipo, sin embargo también tiene funcionalidades que permiten revisar los procesos y los servicios que se encuentran activos, detección de archivos sospechosos o que no contienen firma, controladores sin actualizar que por su obsolescencia están generando una disminución de rendimiento en el equipo, entradas de registro erróneas, problemas de software y hardware y conexiones de red que generen alguna sospecha por no tener información clara y concisa.

FTK Imager
Esta es una herramienta que permite obtener imágenes y realizar una vista previa de los datos. Es usada principalmente en la recopilación de evidencia para análisis forense. Se considera una herramienta para los servicios reactivos de un CSIRT principalmente porque permite hacer una copia de datos conservando la evidencia original de una unidad para su posterior análisis.

Dentro de sus principales funciones se encuentra:

- Crear imágenes forenses: Permite la creación de una imagen bien sea de un disco local como también de discos extraíbles. También permite la creación de una cantidad de carpetas determinadas dentro de un disco duro.
- Visualizar archivos y carpetas: Cuenta con panel que permite observar todos los archivos y carpetas de la unidad seleccionada.
- Visualizar imágenes forenses: Cuenta con una opción que permite montar una imagen forense en el dispositivo para de esta forma revisar la información.
- Recuperar archivos de la papelera de reciclaje que aún no se han sobrescrito.
- Crear hash de archivos: Permite encriptar los archivos a través de funciones hash MD5 y SHA-1.

PESTUDIO:

Esta es una herramienta gratuita portable para Windows que sirve principalmente para analizar diferentes archivos ejecutables .exe buscando principalmente si este ejecutable contiene archivo malicioso o por si el contrario es seguro de instalar. Por lo general funciona a través del análisis de patrones, indicadores y anomalías que pueden generar una sospecha y que a través del reporte le permitirá al usuario discernir entre una buena aplicación y una aplicación con posible malware.

Es bastante sencilla de utilizar ya que no requiere instalación y si se desea modificar su análisis, solo se debe modificar el archivo de configuración que se encuentra en la carpeta donde se aloja el archivo.

- **Hardware**:

Firewall CISCO ASA 5500 Series Data Sheet: Este dispositivo de la compañía CISCO está enfocado principalmente en proteger los centros de datos y entornos de trabajo pesado que principalmente tienen necesidades en donde la baja latencia es fundamental, sin embargo, también se tienen capacidades de procesamiento elevadas.

Es multiplataforma, por tal razón permite integrar diferentes servicios de CISCO, así como de compañías aliadas para de esta forma eliminar cualquier tipo de brecha de seguridad que se tenga en la organización.

Cuenta con servicios como:

- Application Visibility and Control.
- Sistema de prevención de intrusiones de próxima generación.
- Protección anti malware.
- Filtrado de URL
- Mitigación de ataques DDos

Copias de Seguridad:
Para el caso del CSIRT se debe contar con un servidor que permita realizar copias de seguridad a diferentes sistemas y almacenarlos de manera segura. Debe ser una herramienta lo suficientemente robusta para guardar información de una gran cantidad de usuarios. Una alternativa ideal sería utilizar un servidor NAS. Este es un tipo de servidor que facilita el almacenamiento adjunto a la red, de ahí su nombre NAS. Su principal función es la de facilitar los archivos guardados a través de la red a la que se encuentra conectado el servidor.

Este dispositivo parte de una configuración de software previamente configurado, posterior a esto se instala todos sus componentes a la caja que haría las veces de Hardware y permitiría configurar las respectivas puertas de enlaces para acceder a él.

Servidor CISCO UCS B200 M5 Blade Server Data Sheet.
El servidor para el funcionamiento y procesamiento de las aplicaciones y demás herramientas necesarias para la gestión de incidentes de Seguridad Informática será el CISCO UCS B200 M5. Este es un servidor que ofrece una gran cantidad de recursos que permiten no comprometer el rendimiento ante la implementación de diferentes herramientas de trabajo pesado.

En cuanto a las características de rendimiento, es flexible al momento de implementarse y puede ser optimizado con configuraciones adicionales de seguridad. Puede ser adaptado a los otros servidores de la organización, así como al almacenamiento en la nube y accesos de los equipos que realizan sus funciones en el trabajo de campo.

Resumiendo y consolidando de un manera clara y concisa, los servicios del CSIRT para las Pequeñas y Medianas empresas, puede ser observado en la siguiente tabla en donde se asignan tanto el software como el hardware a cada uno de los servicios del equipo bien sea de tipo Reactivo o Proactivo.

Tabla 1.Consolidado Servicios CSIRT.

TIPO DE SERVICIOS	SERVICIOS	SOFTWARE	HARDWARE
Servicios Proactivos	Análisis y Monitoreo infraestructura Tecnológica	❖ Process Explorer. ❖ Nexpose ❖ CIRC AIL Analysis of Information Leaks.	❖ Portátiles Lenovo ThinkPad T14 2DA Generación. ❖ IPS
	Auditorias de Seguridad Informática.	❖ Matriz Metodología Magerit. ❖ Plantilla diseñada por el equipo técnico del CSIRT	❖ Portátiles Lenovo ThinkPad T14 2DA Generación. ❖ Disco duro Toshiba de 2TB
	Desarrollo de herramientas de Seguridad.	❖ VirtualBox ❖ VisualStudio	❖ Portátiles Lenovo ThinkPad T14 2DA Generación. ❖ Workstation P310. ❖
	Educación, entrenamiento y concienciación	❖ Cisco Webex Room. ❖ Cisco Webex Share. ❖ Sitio Web Público.	

	sobre Seguridad Informática.		
Servicios Reactivos	Alertas y Avisos	❖ OWASP Top Ten. ❖ CSIRTs by Country-Interactive Map. ❖ Cisco Secure Email.	
	Gestation de Incidentes.	❖ Clasificación BGP Gnup ❖ Request Tracker for incident Response. ❖ CVE Search. ❖ IntelMQ. ❖ N6 (Network Security Incident Exchange.) ❖ TheHive ❖ GcNotify ❖ CIMSweep ❖ Virus Total ❖ No More Ransom. ❖ ESET SysInspector. ❖ FTK Imager. ❖ PESTUDIO	❖ Firewall CISCO ASA 5500 Series Data Sheet. ❖ Copias de Seguridad. ❖ Servidor CISCO UCS B200 M5 Blade Server Data Sheet. ❖

Fuente: Creación Propia

.6.3 ESTABLECER LOS REQUERIMIENTOS NECESARIOS EN RELACION A LA TECNOLOGIA DE HARDWARE Y SOFTWARE PARA EL DISEÑO DE LA INFRAESTRUCTURA LOGICA QUE PERMITAN DESARROLLAR LAS ACTIVIDADES DEL CSIRT

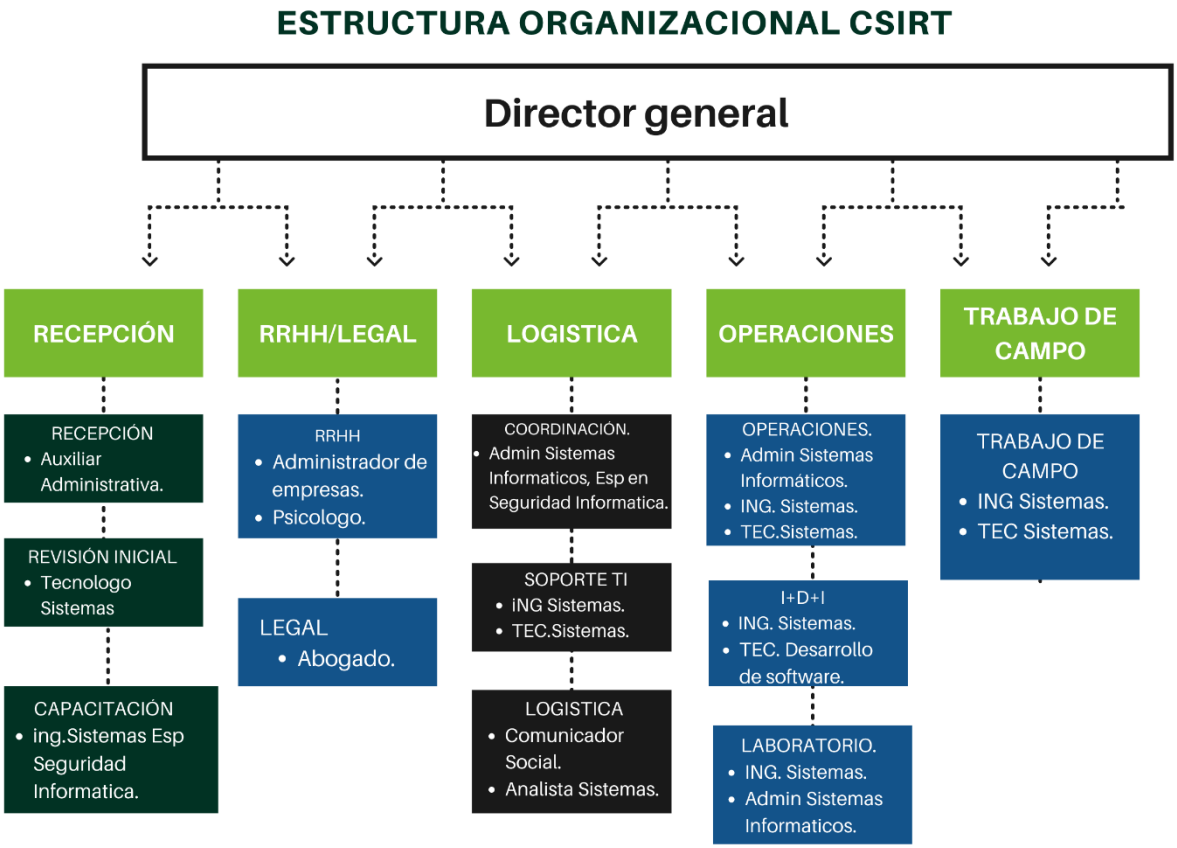
.6.3.1 Estructura Organizacional CSIRT

En la ilustración 4 se podrá observar la estructura a nivel organizacional de un CSIRT en cuanto a los servicios que presta que para este caso serían proactivos y reactivos.

Ilustración 6. Estructura organizacional CSIRT

Fuente: Creación propia.

Ilustración 7. Estructura Organizacional –Talento Humano CSIRT



Fuente Creación Propia.

.6.3.1.1 Director General.

El CSIRT contara con un director general que será el encargado de engranar toda el área administrativa como el área operativa.
Este director será quien tome las decisiones finales relevantes en la compañía, cuenta con un subalterno que será el director operativo, de esta forma recibirá las sugerencias de este y tomara las decisiones que considera son las indicadas no solo para mejorar su efectividad como CSIRT sino también para lograr los objetivos organizacionales de la empresa.

.6.3.1.2 Recepción CSIRT

En esta sección se encontrará la recepción del centro de respuesta a incidentes informáticos y también se contará con la sala de capacitaciones para generar planes educativos a los diferentes usuarios que hagan parte del CSIRT.

En esta área se cuenta con un profesional que dará una revisión inicial al incidente y podrá generar un plan de acción para posteriormente pasarlo al equipo de operaciones quienes serán los encargados de dar respuesta a la problemática.

Otras de las funciones de esta área son:

- Revisar inicialmente el incidente para poder dar un bosquejo inicial de qué tipo de inocente se presenta. En este caso será un Tecnólogo en sistemas el encargado de este proceso.
- Recepcionar todas las solicitudes, correos y peticiones de los clientes y direccionarlos a los profesionales encargados. Quien se encargará de la recepción del CSIRT será una auxiliar administrativa con diferentes cursos en Sistemas de información.
- Desde allí el equipo podrá constantemente estar formando y actualizando a su personal y a clientes específicos todo lo que corresponde a nuevas tecnologías, nuevas amenazas detectadas y nuevas herramientas y técnicas aplicadas por los Ciberdelincuentes. El profesional que se encargará de capacitar tanto al equipo del CSIRT como a los clientes externos será un Ingeniero de Sistemas Especialista en Seguridad Informática.
- Dictar planes de capacitación, formación y concienciación de Seguridad de la Información para las pequeñas y medianas empresas que soliciten este tipo de servicio.

.6.3.1.3 RRHH/Legal

En esta sección se cuenta con el área de Recursos Humanos en donde se realizaran las siguientes funciones:

- Realizar la selección del personal idóneo y competente que cumpla a cabalidad con los requisitos establecidos en cada uno de los cargos que se tienen en el CSIRT.
- Realizar actividades que mejoren el clima laboral de toda la organización para de esta forma aumentar las buenas relaciones y el trabajo en equipo dentro del CSIRT.
- Asumir procesos disciplinarios en caso de que existan con el fin de darle el manejo adecuado y poder llegar al fondo de cada investigación para determinar que comportamiento o que regla fue vulnerada en la organización.

- ❖ Desarrollar los planes y estrategias laborales recomendadas por el director general para de esta forma mejorar la productividad de todo el CSIRT.

De igual manera se encuentra en esta sección un área jurídica que se encarga de:

- ❖ Realizar y verificar cada uno de los contratos de trabajo en pro de beneficios tanto para los empleados como para la organización; de igual forma desde allí se implementan las políticas y reglas necesarias para evitar acciones legales al momento de finiquitar un contrato laboral.
- ❖ Representar a la organización en caso de un litigio por cualquier tipo de inconsistencia o requerimientos por parte de los empleados.
- ❖ Responder cualquier solicitud jurídica como derechos de petición, tutelas y demandas que lleguen al CSIRT por incumplimiento en alguno de sus compromisos con los clientes.

.6.3.1.4 Logística

Dentro de esta sección se encuentran aspectos fundamentales para el funcionamiento del CSIRT. Esto principalmente porque es donde se encuentra la información almacenada de todo el equipo y de los clientes que alojan la información allí. También se tienen profesionales que apoyaran todo el tema de soporte y todo el tema logístico de tal manera que puedan generar un puente y puedan dar un manejo adecuado a los clientes de las pequeñas y medianas empresas.

Las áreas que se encuentran en esta sección son:

.6.3.1.5 Coordinación CSIRT

La coordinación operativa del CSIRT estará a cargo de un Administrador de Sistemas Informáticos Especialista en Seguridad Informática.

Dentro de esta se encuentran aquellos que lideran todo el grupo del Equipo de Respuesta, son quienes dan los lineamientos iniciales y dirigen el equipo.

De igual forma también se dedica a realizar acuerdos con otras organizaciones en temas operativos y técnicos, en donde se retroalimentan entre sí y llegan a cooperaciones mutuas que permiten crear una comunidad que vela por todo lo que comprende la Ciberseguridad.

Dentro de las principales funciones de este equipo se encuentra:

- ❖ Dirigir o coordinar estratégicamente todos los miembros del CSIRT.
- ❖ Supervisar las actividades realizadas por el equipo

- Buscar aliados estratégicos de CSIRT, organizaciones y demás entidades que puedan aportar al crecimiento de la organización.
- Coordinar eficazmente a través de gestiones la respuesta ante los incidentes y los procesos realizados.

Los coordinadores de un CSIRT deben de ser profesionales con amplia formación en temas de seguridad Informática y manejo de crisis y recuperación de negocios.

.6.3.1.6 Soporte de TI

Para el área de Soporte se contará con 2 profesionales, uno de estos será un Ingeniero de Sistemas quien se encargará de realizar toda la gestión del soporte como tal que se requiere, a su vez se contará con un Técnico en sistemas quien apoyará la parte operacional del proceso.

Dentro de este equipo el equipo de soporte de TI es quien adopta la tarea de gestionar, analizar y dar respuesta a todo lo concerniente a amenazas que afectan como tal la infraestructura de TI.

Dentro de esta área se deben de encargar de todo lo concerniente a la búsqueda de herramientas tecnológicas de alto impacto que puedan aumentar el rendimiento y optimizar el tiempo del CSIRT.

De igual forma también se encargan de todo lo correspondiente al análisis de las estadísticas y las tendencias globales en cuanto a ataques.

.6.3.1.7 Comunicaciones y Logística

En esta sección se contará con un Comunicador Social quien será el encargado de las comunicaciones del CSIRT, de buscar estrategias de difusión y demás; a su vez se tendrá un Analista de Sistemas que estará haciendo las conexiones y buscando alternativas de mejora desde la parte tecnológica.

En esta área podría ubicarse un equipo que haga las veces de comunicadores y encargados de las relaciones públicas. En este caso es fundamental ya que un CSIRT debe de generar constantemente comunicaciones y promoción de sus servicios en la comunidad donde se encuentran ubicadas y establecidas sus operaciones. Este equipo es fundamental ya que de una buena área de comunicación podría desprenderse un aumento de la confianza y reconocimiento del equipo dentro del mercado y por ende podrían aumentar los suscriptores o clientes potenciales.

Sus funciones son básicamente:

- Identificar los medios de comunicación disponibles y que podrían ser de acceso adecuado para el equipo.
- Crear mecanismos oficiales para de esta forma generar estrategias de divulgación de información correspondiente a las funciones y procesos del el CSIRT.
- Participación en eventos y foros que tengan que ver con la temática como tal del equipo.

.6.3.1.8 Centro de Datos.

Acá se encuentran los servidores de la organización los cuales almacenan no solo las aplicaciones desarrolladas e implementadas por el CSIRT, sino que también se cuentan con copias de seguridad de los clientes de Pequeñas y medianas empresas que optaron por almacenar sus copias de seguridad en la organización como tal.

.6.3.1.9 Operaciones

- **I+D+I:**

Los profesionales que operarán este proceso serán principalmente un Ingeniero de Sistemas y un Técnico en Desarrollo de Software.

Dentro de este grupo se encuentran los encargados de implementar y desarrollar herramientas que permitan mejorar todo el funcionamiento del CSIRT. De igual forma también se encargarán de la formación y la investigación correspondiente en cuanto a tendencias de incidentes de seguridad informática y nuevas amenazas detectadas.

- **Centro de Operaciones:**

Debido a que el Centro de Operaciones es la parte principal del CSIRT, será la que tenga más personas encargadas del proceso. En este caso se contará con un Administrador de Sistemas Informáticos, Ingeniero de Sistemas y Técnico en sistemas; todos 3 contaran con diferentes capacitaciones y planes de entrenamiento en temas referentes a la Seguridad Informática.

Desde el centro de operaciones se realizan los procesos más críticos del CSIRT. Es allí donde se realiza todo lo que corresponde a temas de gestión, seguimiento y análisis de los incidentes reportados. Dentro de este equipo pueden encontrarse roles como el Encargado de Gestión de incidentes o el Encargado de Monitoreo de incidentes.

Es muy probable que mientras un CSIRT se consolida, este equipo no reciba retroalimentaciones, sin embargo, a medida que el Equipo se va dando a conocer pueden empezar a llegar incidentes de diferente tipo.
Algunas de las funciones de esta área son:

- Alertar y advertir acerca de posibles ataques.
- Apoyar a todas las áreas alternas del CSIRT con el fin de facilitarles el procedimiento dentro de las funciones desarrolladas.
- Coordinar todas las labores ejecutadas en la organización de tal manera que estas estén correctamente engranadas con las políticas del equipo previamente establecidas.
- Realizar toda la gestión del incidente informático que sea direccionado a esta área porque su impacto así lo requiere.

❖ **Laboratorios:**

Para el Laboratorio se contará con un Ingeniero de Sistemas y un Administrador de Sistemas informáticos, los cuales están altamente capacitados en Seguridad Informática, cuentan con certificaciones de Ethical Hacker de diferentes compañías de Ciberseguridad.

El CSIRT contara con un área exclusiva para realizar laboratorios controlados. Es decir, se contará con una infraestructura tecnológica lo suficientemente segura para ejecutar ataques y replicar amenazas con el fin de poder encontrar soluciones más prácticas y más seguras.

.6.3.1.10 Trabajo de Campo

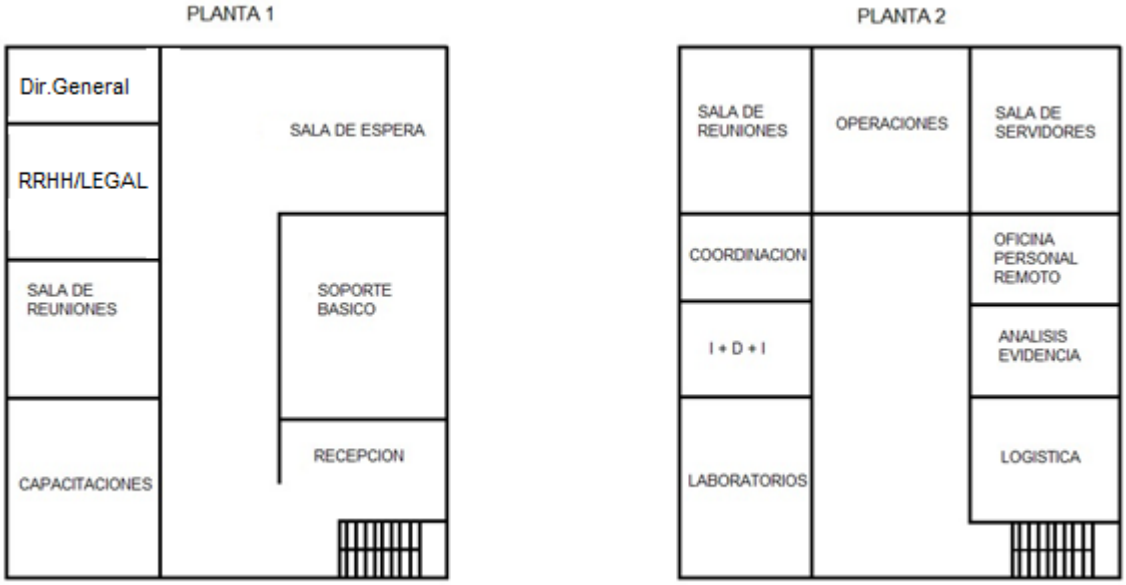
Quienes desempeñen esta función serán principalmente un Ingeniero de Sistemas y un Técnico en Sistemas que siempre estarán en las empresas de los clientes capturando toda la información necesaria para realizar la Gestión del Incidente Informático correctamente.

El CSIRT para las pequeñas y medianas empresas contara con una sección que se ubicara siempre en las empresas donde se presentó el incidente. Desde allí los profesionales se encargarán principalmente de recolectar la evidencia digital y de preservar esta lo más original posible para de esta forma no solo dar respuesta al incidente informático sino también determinar la forma de ataque y posibles responsables detrás del mismo.

Los profesionales tendrán acceso remotamente a los servidores de la organización para dirigir las copias de seguridad de las imágenes previamente creadas de las unidades afectadas por el ataque informático.

.6.3.2 Estructura Física CSIRT

Ilustración 8. Estructura Física CSIRT



Fuente Creación Propia.

El CSIRT tendrá su infraestructura física en un espacio que contará con 2 plantas.

.6.3.2.1 Planta 1

En esta planta se encontrará todo lo que tiene que ver con la dirección general, recursos humanos, área jurídica, la recepción, revisión inicial y capacitaciones:

- **Dirección General:** Esta será la oficina donde se ubicara el Director general de la organización. Sera una oficina que cuenta con un proyector y una pantalla inteligente que le permitirá al profesional como tal observar y visualizar los procesos del CSIRT de una manera más interactiva.
- **RRHH/Legal:** En este espacio se ubicara el área de Recursos Humanos y el área jurídica, desde donde se centrara todo lo que tiene que ver con contratación, planes de mejoramiento y manejo de procesos y requerimientos jurídicos.
- **Recepción**: Sera un espacio en donde se encontrará una persona que se encargara de atender a las personas que llegan o que llaman como tal a las oficinas y les brindara la atención necesaria para direccionarlos hacia el área a la que desean dirigirse.
- **Soporte Básico:** Desde esta oficina se contará con un profesional que realizara la revisión del incidente recibido, aplicará técnicas para determinar la situación y la magnitud como tal del ataque; en caso de que este no represente mayor dificultad

para dar solución, se procederá a realizar el proceso básico de análisis del incidente para dar una respuesta al cliente y una solución satisfactoria.

- **Capacitaciones:** El CSIRT contara con una sala de capacitaciones presenciales que tendrá capacidad para 20 personas, contara con diferentes equipos electrónicos que le permita al profesional encargado de capacitar, entregar la información apropiada a los clientes que se estarán formando.
- **Sala de Reuniones:** En esta área aparte de servir para hacer reuniones con diferentes clientes y demás de nivel básico, también se tendrá una herramienta de CISCO robusta que permitirá capacitar virtualmente a cualquier empresa que solicite este servicio.
- **Sala de espera:** Se contará con una sala de espera para que los clientes puedan estar allí mientras se les está dando una respuesta a su solicitud.

.6.3.2.2 Planta 2

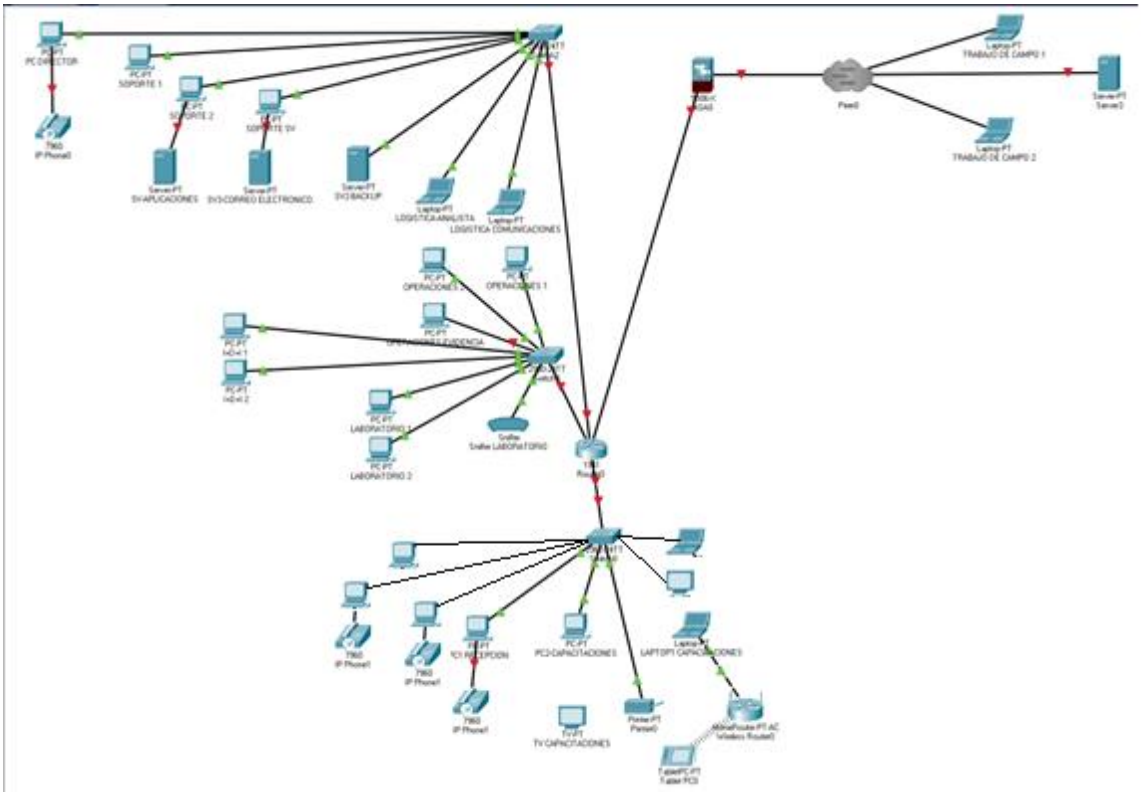
- **Sala de Reuniones 2:** Esta sala de reuniones será estrictamente para la coordinación del CSIRT con clientes potenciales o Coordinadores de otros CSIRT de la industria con el fin de generar alianzas estratégicas que permitan aumentar la cantidad de clientes.
- **Logística:** En la oficina de logística se ubicarán los profesionales encargados de las comunicaciones desde el CSIRT hacia los clientes, así mismo se encargarán de buscar aliados estratégicos y detectar información fundamental para mejorar la reputación del Equipo.
- **Análisis de evidencia:** En la oficina de análisis de evidencia se ubicará un profesional que se encarga de capturar toda la información proveniente del ataque.
  Sin embargo, en algunas ocasiones la evidencia es traída por el equipo de Trabajo de campo; en esta situación el profesional toma las imágenes forenses correspondientes y las revisa con el fin de detectar información relevante que pueda ser recopilada y haga parte del proceso de análisis de incidente.
- **Laboratorios:** En esta oficina se contará con 2 profesionales encargados de probar diferentes herramientas con el fin de encontrar las más idóneas para dar respuesta a los tipos de clientes con los que cuenta el CSIRT; también se realizaran ataques controlados para evidenciar la forma de actuar de algunos malware y poder prevenir ataques a futuro en las organizaciones que hacen parte del público del CSIRT.
- **I+D+I:** En esta se desarrollarán herramientas que no solo apoyen el análisis de Incidentes informáticos sino también herramientas que optimicen todas las funciones como tal del CSIRT.
- **Coordinación:** En esta área se encontrar el Coordinador del CSIRT, encargado de tomar las decisiones de todo el equipo y realizar conexiones estratégicas con los altos mandos de otros CSIRT para de esta forma establecer alianzas y captar más clientes potenciales.
- **Oficina personal Remoto:** Este será el espacio físico para los profesionales que estarán realizando el trabajo de campo. Desde acá pueden depurar la información

recolectada en las empresas para posteriormente direccionarla al área de Análisis de evidencia.

- **Sala de Servidores:** En esta oficina se ubicarán los servidores de la organización, así mismo se encontrarán tanto el Router como los 2 switchs que corresponden a la planta dependiendo la Topología de Red seleccionada para el CSIRT.
  Esta oficina cuenta con Aire acondicionado, Red eléctrica de respaldo y dispositivos de UPS para asegurar el funcionamiento del Centro a pesar de las fallas eléctricas que puedan presentarse.
- **Operaciones:** En esta oficina se encuentran los profesionales que harán toda la gestión y la respuesta al incidente informático. Reciben la evidencia analizada por parte del respectivo profesional y proceden a realizar el procedo dependiendo del tipo de ataque presentado. Luego de esto se encargan de restaurar la información y finalizar el informe para entrega a la empresa que presento el inconveniente de seguridad.

.6.3.3 Estructura Tecnológica CSIRT

Ilustración 9. Estructura tecnológica CSIRT



Fuente: Creación propia.

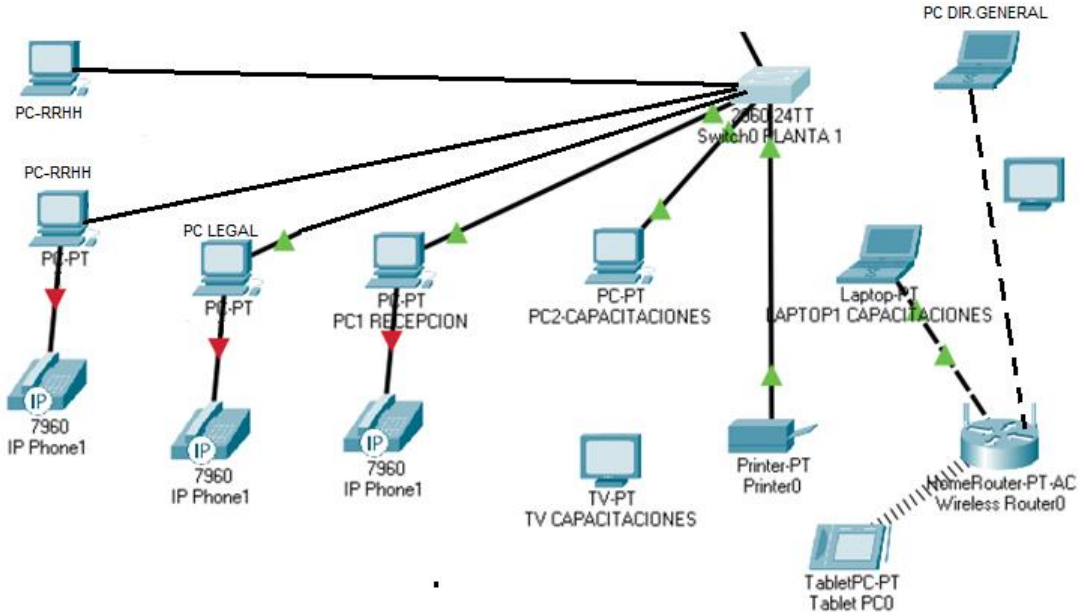
La estructura tecnológica del CSIRT constara principalmente de 2 plantas en donde se ubicarán las diferentes secciones establecidas anteriormente para el funcionamiento como tal del lugar.

Esta estructura cuenta con un apartado especial para las conexiones remotas que incluyen principalmente los computadores de los profesionales que realizan el trabajo de campo, el servidor en la nube de respaldo con el que cuenta la organización y el firewall y pagina web que se encuentran conectados a la red de la organización.

Las dos plantas estarán divididas mediante redes independientes para de esta forma asegurar cada una en caso de una fuga o un incidente informático presentado en el mismo CSIRT.

.6.3.3.1 Planta 1

Ilustración 10.Planta 1-Estructura Tecnológica CSIRT.



Fuente Creación Propia.

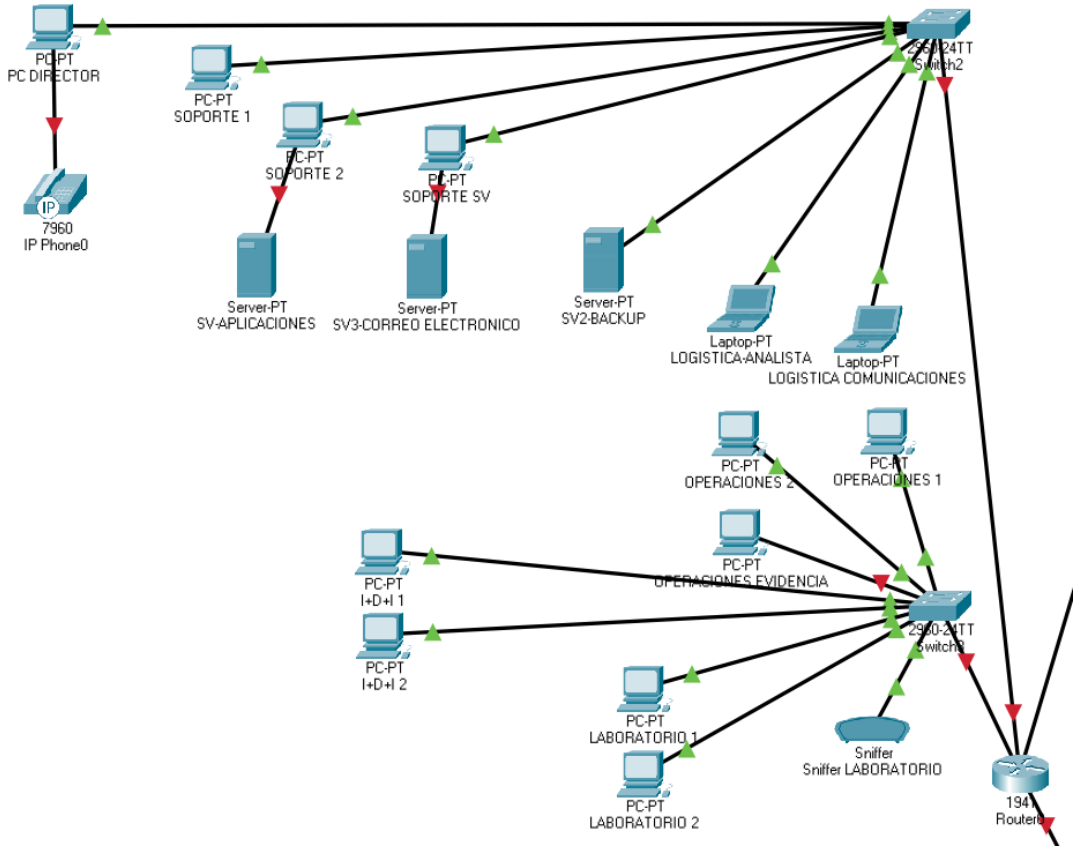
En la planta 1 se contar con un switch que permitirá crear la VLAN1, esta será la de recepción y todo lo de la primer planta. Esta planta contara con 5 computadores de escritorio, 2 computadores portátiles, una Tablet, 3 teléfonos y una impresora, todos conectados a la VLAN. Adicional a esto se tiene instalado un Router Wifi que permitirá no solo acceder mediante wifi a diferentes sitios web sino que también a través de esta red se configurara una red de visitante para los clientes que lleguen y deban esperar una respuesta determinada de su solicitud.

En esta planta se encuentra ubicada la sala de capacitaciones y reuniones, en las cuales se tendrá instalada la herramienta CISCO Webex room, el cual tendrá acceso wifi a la red para poder conectarse con los clientes remotamente si es el caso necesario.

De igual forma, el acceso a la red mediante cableado o wifi se hará a través de diferentes protocolos seguros y reglas de validación que se tienen implementados en la misma con el fin de evitar posibles suplantaciones de identidad y alteración de los mensajes que se trasmiten como tal por la red.

.6.3.3.2 Planta 2

Ilustración 11.Planta 2.Estructura Tecnológica CSIRT



Fuente Creación Propia.

Toda la planta se divide en 2 VLAN, esto principalmente porque las funciones que se realizan en las áreas de I+D+I, laboratorios y operaciones son actividades que pueden representar un riesgo para las demás secciones de la organización, es por esto que seccionando la planta en dos VLAN se puede prevenir que un incidente se propague por toda la red y ocasione daños y perdida de información que puede alterar los servicios de los clientes.

- **VLAN 1**

En el área de operaciones se cuenta con 3 computadores que se encargaran de realizar todo el procesamiento del incidente informático, desde el análisis de la evidencia hasta el procesamiento y recuperación de las máquinas y activos afectados.

Para los laboratorios se contara con 2 computadores y un sniffer que permitirán implementar y realizar ataques controlados con el fin de comprender el funcionamiento y aprender cómo actúan diferentes malware en los activos que atacan.

En el área de I+D+I se tendrán 2 computadores conectados que permitirán a los profesionales que realizan su labor en este lugar, desarrollar diferentes herramientas y aplicaciones que optimicen los servicios del CSIRT y permitan aumentar la seguridad en las empresas que están suscritas al equipo.

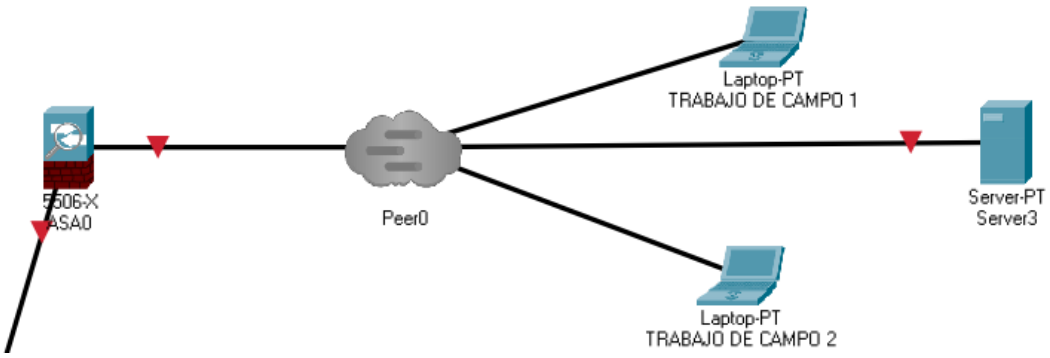
- **VLAN 2:**

En esta VLAN se encuentra el área de dirección en donde se contará con un computador y un teléfono a cargo del director del CSIRT.

En la sección de Soporte se tienen 3 computadores los cuales están conectados y prestan soporte no solo a los clientes del Centro sino también se hacen cargo de los Servidores de la organización, en este caso se tienen 3; uno especializado para las aplicaciones, otro para las copias de seguridad tanto del CSIRT como de los clientes y el ultimo encargado del correo electrónico especializado de la empresa.

Por último, se tiene el área de Logística, la cual tendrá 2 computadores que hacen parte de los profesionales que se encargan no solo de realizar las comunicaciones del CSIRT sino también de todo el tema de imagen institucional y captación de nuevos clientes.

Ilustración 12.Area Externa-Estructura Tecnológica CSIRT



Fuente Creación Propia

- **TRABAJO DE CAMPO:**

En esta área se cuenta con 2 dispositivos portátiles que les permitan a los profesionales en campo tomar las capturas y las copias de las imágenes de los diferentes discos atacados y enviarlas al Servidor NAS de manera encriptada para que de esta forma el firewall configurado no lo tome como un virus e impida el almacenamiento.

También se cuenta con un servidor en la nube que permitirá la creación de la página web en donde se ofertaran los servicios del CSIRT para captar clientes y usuarios para no solo resolver incidentes de seguridad informática sino para generar planes de capacitaciones en los empleados que hacen parte del sector de las pequeñas y medianas empresas.

Tabla 2.Herramientas Hardware.

NOMBRE	CANTIDAD	ESPECIFICACIONES
Servidor Blade Cisco UCS B200 M5	1	• Soporta hasta 2 procesadores Intel Xeon Escalable de 2da generación, cada uno con 28 núcleos de CPU. • Cuenta con 24 ranuras para memoria DDR4 de velocidad de 2933 MHz. Cada una de estas soporta hasta 3 TB de memoria. • Tarjeta LAN modular en placa base con una tarjeta interfaz virtual de Cisco. • Adaptador intermedio mLOM de 2 puertos y 40 GB de Ethernet. • Dos unidades de Disco Duro (HDD), unidades de estado sólido (SSD). • Soporta hasta 2 GPU adicionales. • Soporta unidad flash USB interna de 16 GB.
NAS empresarial TS-H686 de 6 bahías de QNAP con Intel XEON d-1602.	1	• Procesador Intel XEON d-1602 Dual-Core 2.5 GHz. • 8 GN UDIMM DDR4 ECC • 4 bahías de disco. • 4 puertos de 2.5 GbE • 3 Puertos USB. • Sistema operativo QuTS Hero.
IdeaCentre 3i AIO Intel	13	• Procesador Intel Core i7 10700T. • Sistema Operativo Windows 10 pro 64.

		• Tarjeta gráfica Intel UHD 610 • Pantalla Led de 27”, 250 nits. • Memoria 16 GB 2666 MHz DDR4 • Disco duro SATA G.0 Gb
CISCO Webex Room Phone At- a –Glance	2	• Permite agregar diferentes participantes a la reunión. • Tiene un orador activo. • Uso compartido inalámbrico. • Ajustable a las aplicaciones de Webex. • Análisis de información de los dispositivos que se encuentran activos mediante la Webex Control Hub. • Pantalla de 6” • Cobertura de audio de 360 grados, cancelación de eco acústico y reducción de ruido. • Puerto adicional HDMI.
ThinkPad T14 2da Gen Intel.	4	• Procesador Intel Core i7-1165G7. • Windows 10 Pro 64. • Pantalla de 14” Anti-Glare. • Memoria de 16 GB DDR4. • Almacenamiento de 512 SSD. • Intel Wi-Fi 6E AX210 2X2
Firewall- CISCO ASA 5508 Series Data Sheet.	1	• Cortafuegos 1Gbps. • NIPS 250 Mbps. • Interfaces 8 x RJ45. • Máximo de sesiones simultaneas. 100 mil • Máximo de conexiones nuevas por segundo con AVC. 7.5 mil • TLS 250 Mbps.
Cisco Catalyst 9130 AX Access Points	2	• Wi-fi 6. (802.11ax). • Cisco RF ASIC. Funciones Cisco CleanAir o sistema de prevención de intrusiones inalámbricas.

		• Acceso OFDMA. • 8 Flujos Multiusuario. • Sw Catalyst 9130 AX • Controladores inalámbricos 3504,5530. • Canales de 20 y 40 MHz. • Soporte CSD • Antena de 5 GHz.

Fuente: Creación Propia.

Ahora bien, en cuanto a la relación que tienen los requerimientos tanto humanos como técnicos con los servicios prestados por el CSIRT, estos se encuentran plasmados en la siguiente tabla en donde se podrá observar mediante que recursos se puede lograr el logro de los objetivos y el cumplimiento de todos los servicios de CSIRT.

Tabla 3.Requerimientos alineados con los servicios del CSIRT.

TIPO DE SERVICIOS	SERVICIOS	SOFTWARE	HARDWARE	RECURSOS HUMANOS
Servicios Proactivos	Análisis y Monitoreo infraestructura Tecnológica	❖ Process Explorer. ❖ Nexpose ❖ CIRC AIL Analysis of Information Leaks.	❖ Portátiles Lenovo ThinkPad T14 2DA Generación. ❖ IPS	❖ Profesionales área trabajo de campo. ❖ Profesionales área de operaciones.
	Auditorias de Seguridad Informática.	❖ Matriz Metodología Magerit. ❖ Plantilla diseñada por el equipo técnico del CSIRT	❖ Portátiles Lenovo ThinkPad T14 2DA Generación. ❖ Disco duro Toshiba de 2TB	❖ Profesionales área trabajo de campo. ❖ Profesionales área de operaciones.
	Desarrollo de herramientas de Seguridad.	❖ VirtualBox ❖ VisualStudio	❖ Portátiles Lenovo ThinkPad T14 2DA Generación. ❖ Workstation P310. ❖	❖ Profesionales área de I+D+I. ❖ Profesionales área de Laboratorio. ❖ Profesionales área de Soporte.

	Educación, entrenamiento y concienciación sobre Seguridad Informática.	❖ Cisco Webex Room. ❖ Cisco Webex Share. ❖ Sitio Web Público.		❖ Profesionales área de Coordinación. ❖ Profesionales área de Soporte de TI. ❖ Profesionales área de I+D+I. ❖ Profesional área de Capacitación.
Servicios Reactivos	Alertas y Avisos	❖ OWASP Top Ten. ❖ CSIRTs by Country-Interactive Map. ❖ Cisco Secure Email.		❖ Profesionales area de Logistica. ❖ Profesionales área de Trabajo de campo.
	Gestation de Incidentes.	❖ Clasificación BGP Gnup ❖ Request Tracker for incident Response. ❖ CVE Search. ❖ IntelMQ. ❖ N6(Network Security Incident Exchange.) ❖ TheHive ❖ GcNotify ❖ CIMSweep ❖ Virus Total ❖ No More Ransom. ❖ ESET SysInspector.	❖ Firewall CISCO ASA 5500 Series Data Sheet. ❖ Copias de Seguridad. ❖ Servidor CISCO UCS B200 M5 Blade Server Data Sheet. ❖	❖ Profesional área de recepción. ❖ Profesional área de revisión inicial. ❖ Profesional área de soporte de TI. ❖ Profesionales área de Operaciones. ❖ Profesionales área de Trabajo de campo.

		❖ FTK Imager. ❖ PESTUDIO		

Fuente: Creación Propia.

.6.4 DESARROLLAR A PARTIR DE LABORATORIOS CONTROLADOS Y A REALIZACION DE PRUEBAS DE SOFTWARE, LA DEMOSTRACION DE LAS HERRAMIENTAS QUE PUEDEN UTILIZARSE PARA EJECUCION DE LAS TAREAS PROPIAS DEL CSIRT.

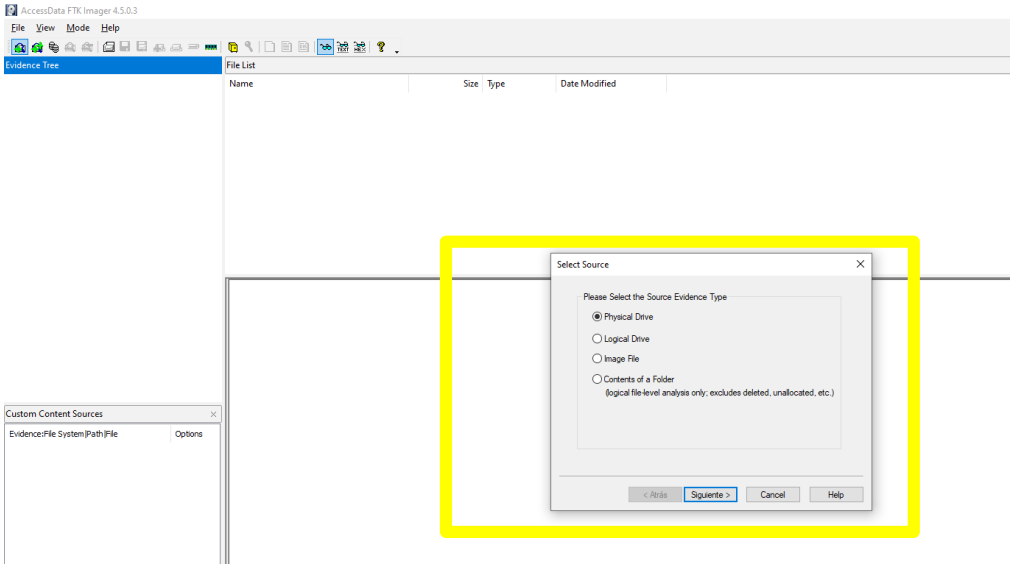
.6.4.1 FTK Imager

Dentro de un CSIRT es fundamental todo el proceso de recolección de evidencia ante un incidente de Seguridad Informática dentro de una pequeña o mediana empresa. Para esto lo ideal es iniciar con una copia completa de la unidad que fue atacada y realizar una revisión de qué fue lo que paso, que tipo de ataque se presentó y encontrar a un posible responsable de este.

Es por este motivo que se hace uso de FTK Imager para generar una imagen de la unidad atacada y posteriormente ser llevada al centro de operaciones para iniciar con todo el proceso de análisis forense y solución de incidentes.

❖ **Paso 1:** Creación Source.

Ilustración 13.Creacion Source FTK Imager



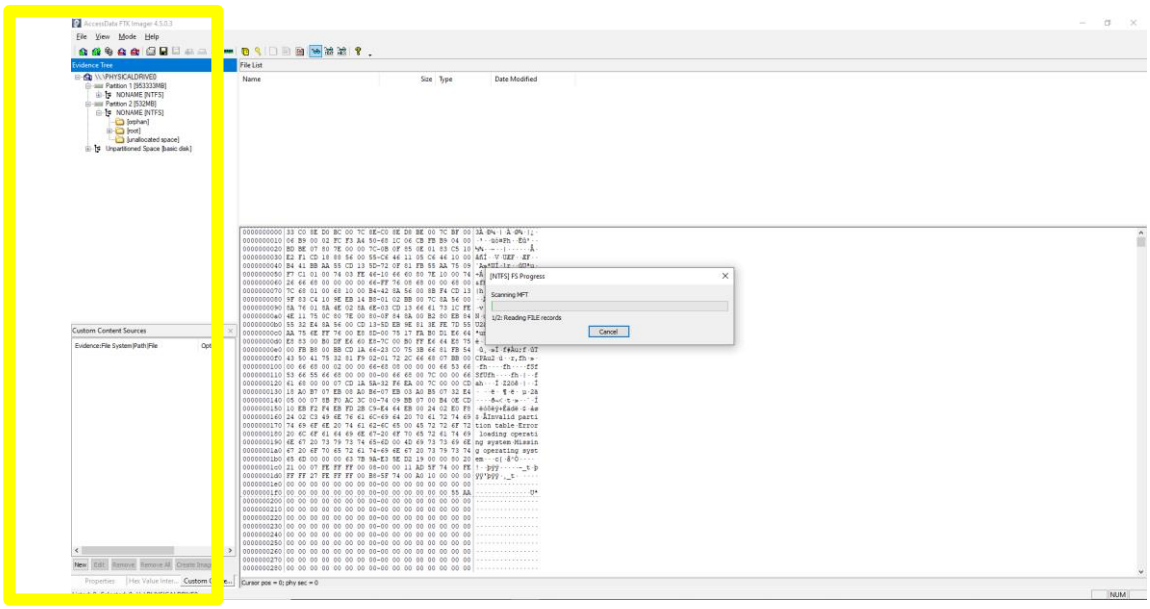
Fuente Creación propia.

Al crear una nueva imagen y seleccionar la opción physical drive la herramienta automáticamente lee la información y detecta las particiones y la estructura del sistema y los archivos contenidos en el sistema.

Estas opciones las muestra en el panel del árbol de evidencia.
Para observar los archivos se le da clic en + para desplegar toda la información.

- **Paso 2:** Se observa el arbol de evidencia con los archivos del source seleccionado.

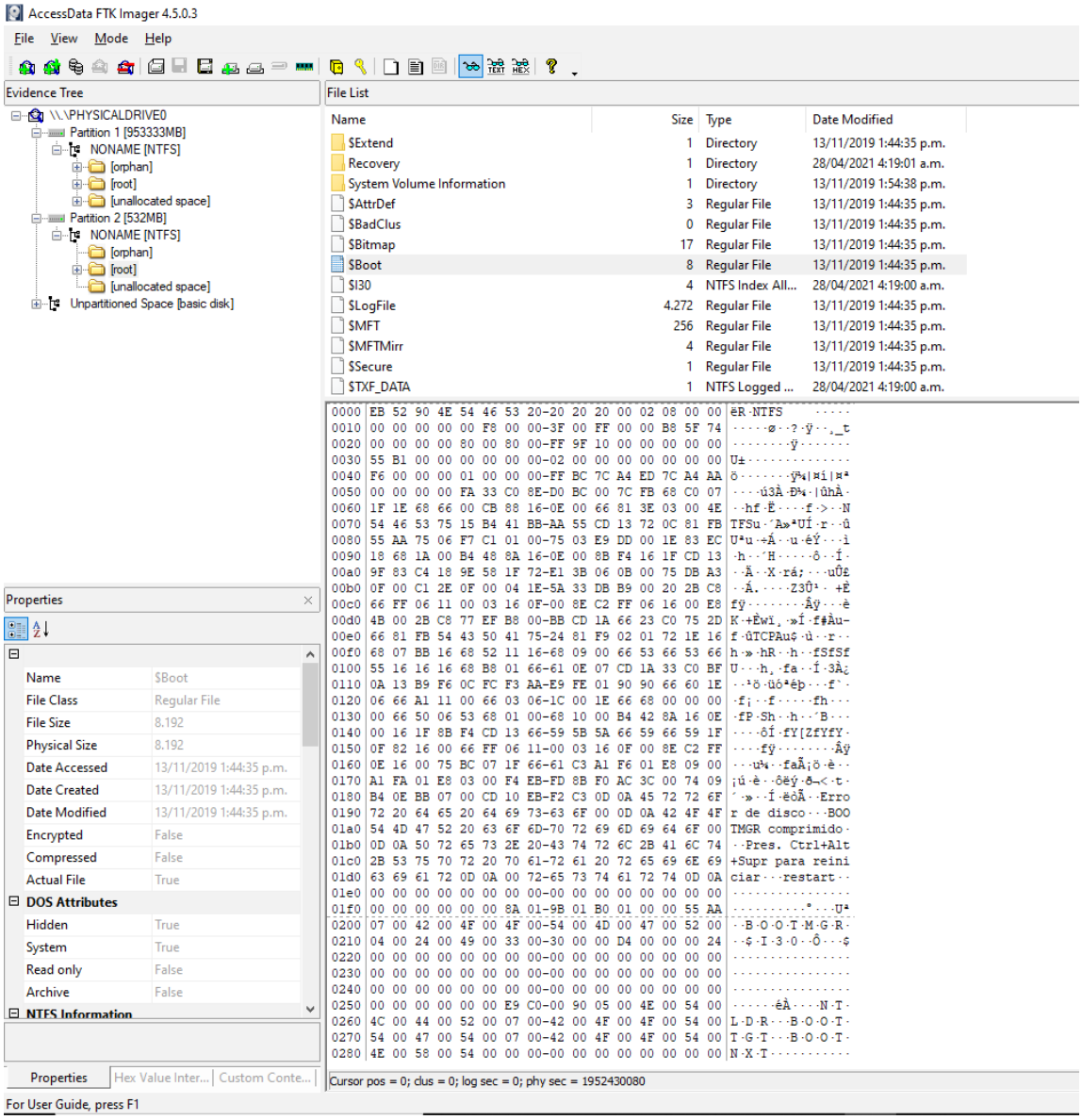
Ilustración 14.Arbol de evidencia FTK Imager.



Fuente Creación Propia.

❖ **Paso 3:** Se observa la información de las carpetas.

Ilustración 15.Informacion Carpetas FTK Imager.



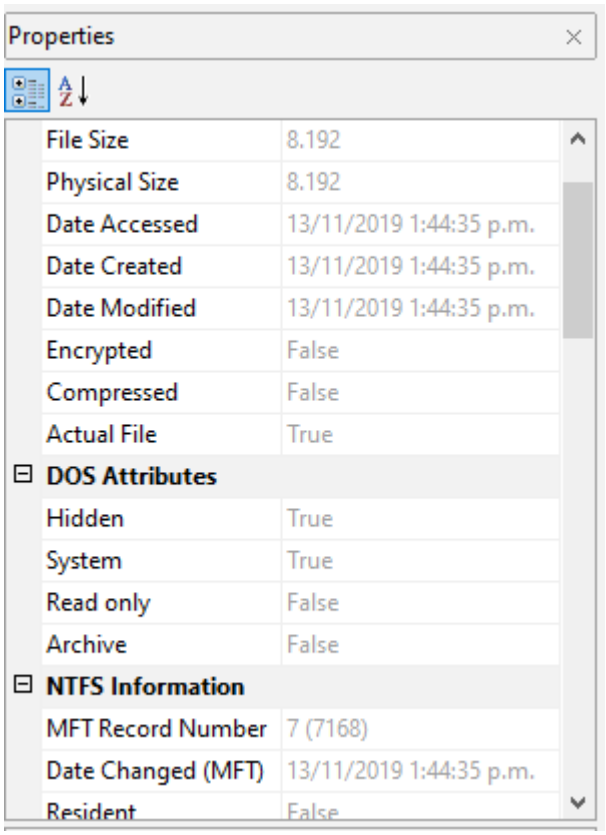
Fuente Creación Propia.

Al seleccionar un archivo si la herramienta no está en capacidad de visualizar este mismo, mostrara la información hexadecimal que le corresponde.

De igual manera en la parte inferior izquierda en las propiedades se pueden observar datos adicionales del archivo como fecha de creación, modificación y si tiene algún tipo de encriptación, entre otros.

❖ **Paso 4:** Se puede observar las marcas de tiempo para el tema forense

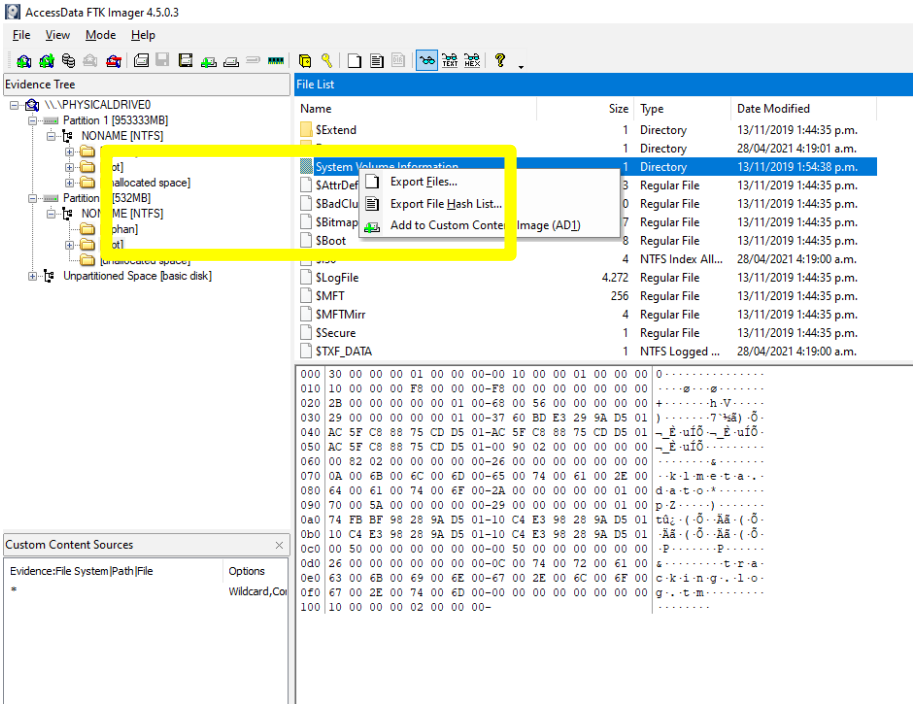
Ilustración 16.Marcas de Tiempo-Análisis Forense.



Fuente Creación Propia.

❖ **Paso 5:** Add to Custom Content Image

Ilustración 17.Agregar una imagen personalizada FTK Imager.

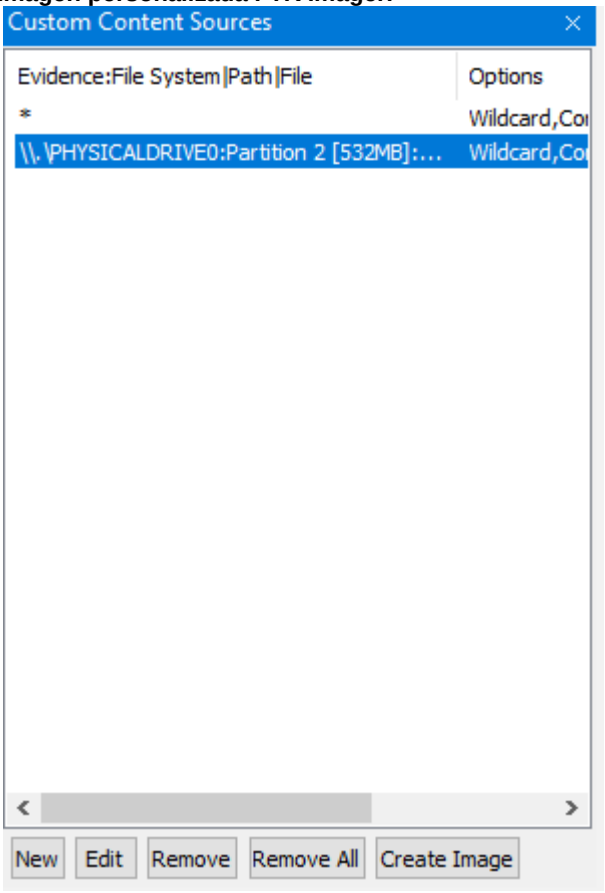


Fuente Creación Propia.

Esta herramienta permite seleccionar los archivos que se desea generar en la imagen de evidencia exportada.

❖ **Paso 6:** Visualización Custom Content Sources.

Ilustración 18.Visualizacion Imagen personalizada FTK Imager.

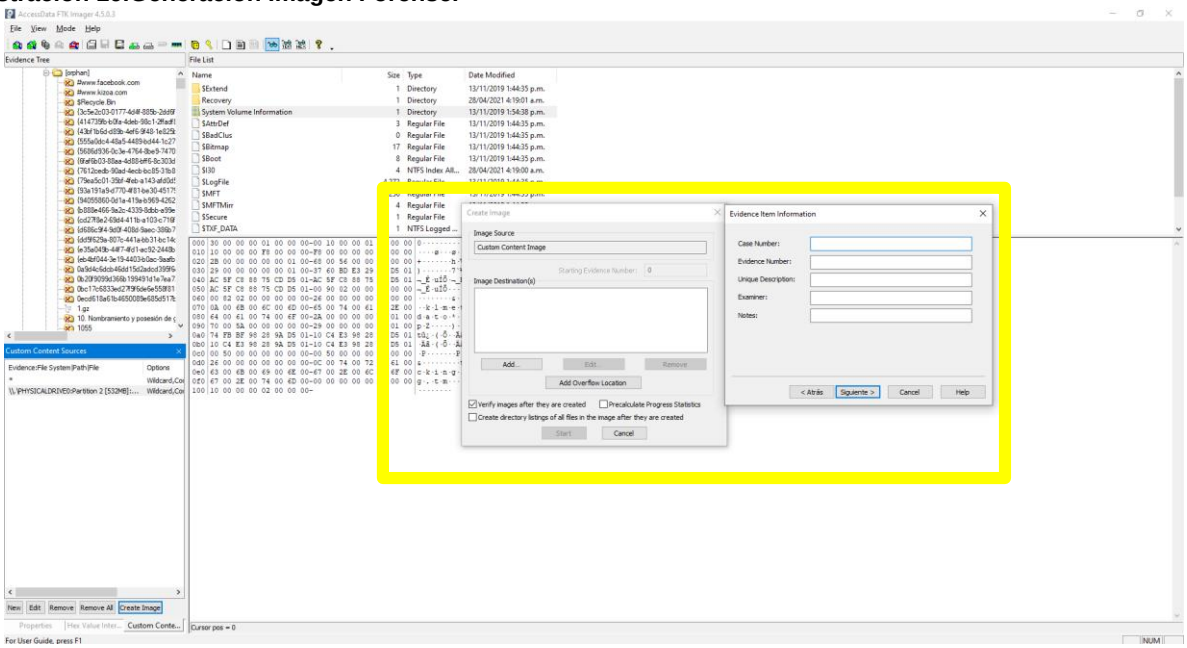


Fuente Creación Propia.

Desde el árbol de archivos personalizados se puede editar la información para agregar, o eliminar particiones.

❖ **Paso 7:** Generar la imagen forense

Ilustración 19.Generacion Imagen Forense.

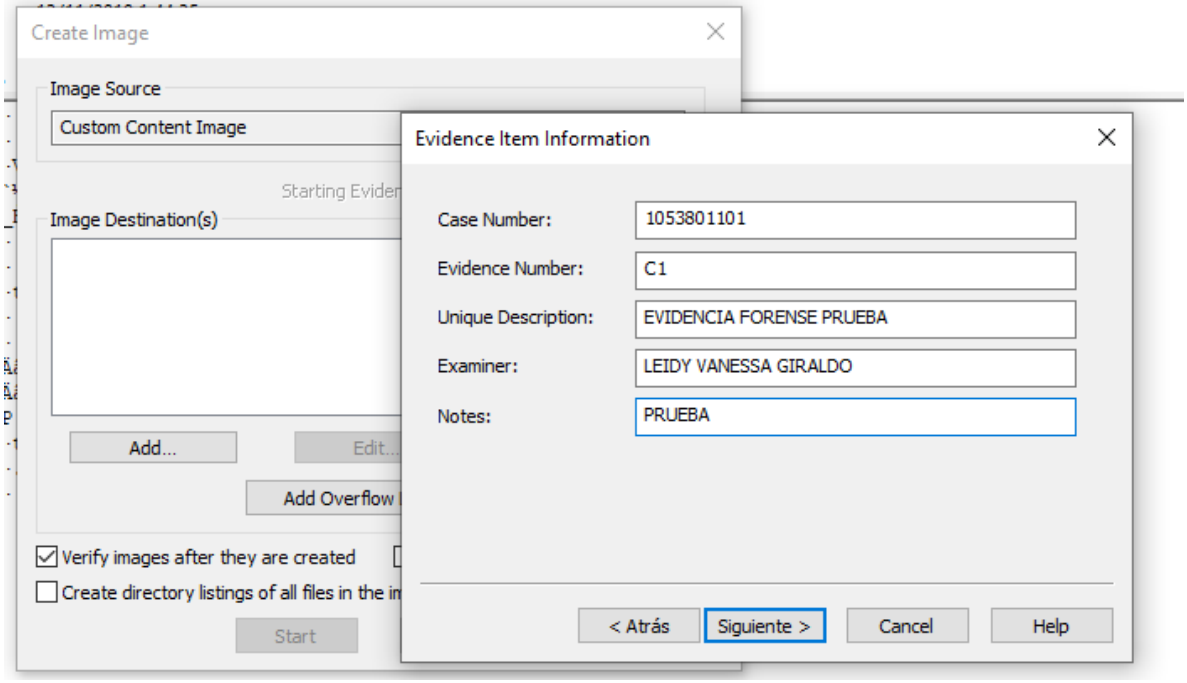


Fuente Creación Propia.

Se procede a generar la imagen forense que para este caso se basara en el contenido personalizado en los pasos anteriores.

❖ **Paso 8:** Ingresar la información para la identificación de la imagen forense.

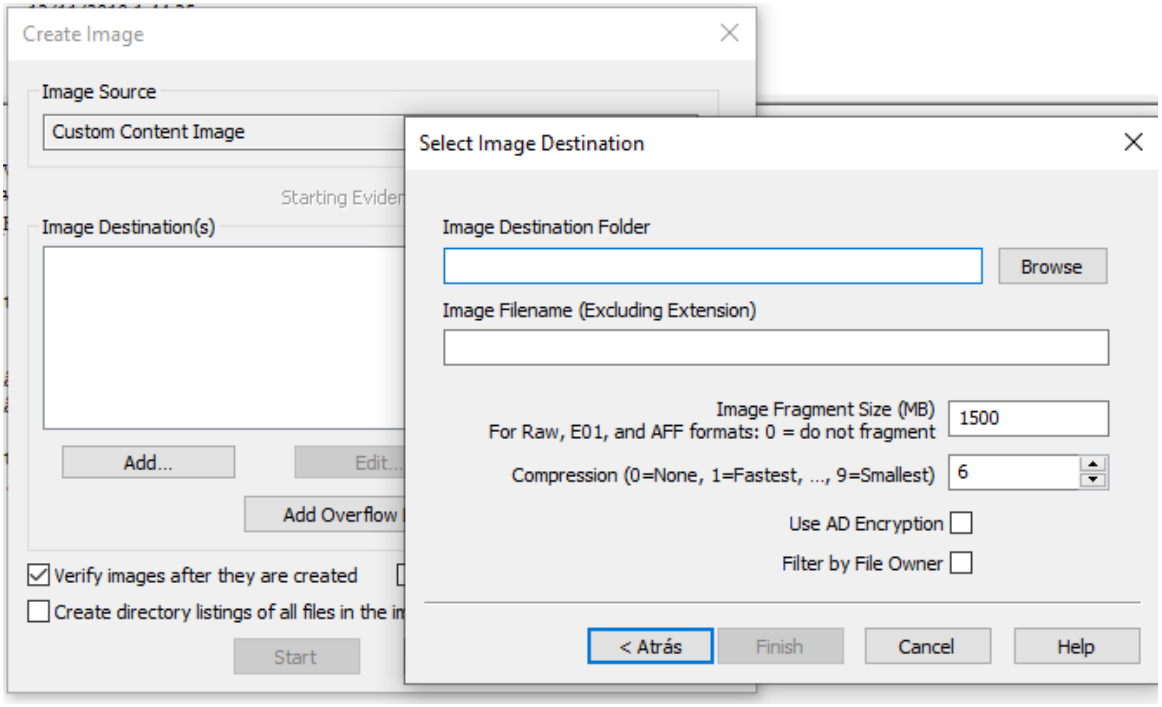
Ilustración 20.Personalizacion Imagen Forense FTK Imager.



Fuente Creación Propia.

❖ **Paso 9:** Se selecciona la carpeta donde se almacenará la imagen forense.

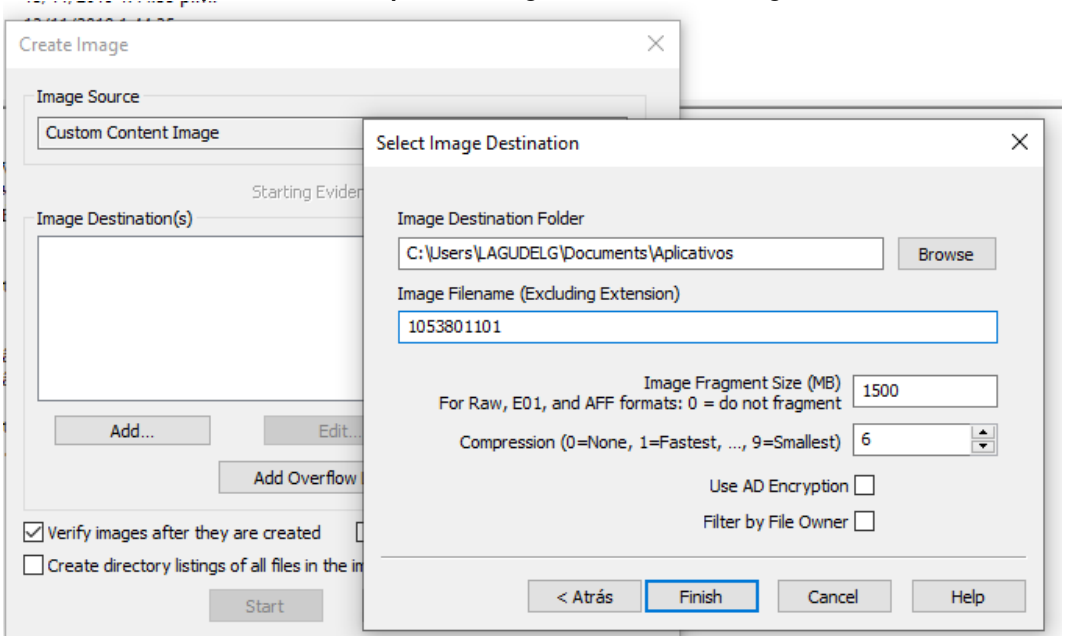
Ilustración 21.Selección Carpeta destino Imagen Forense.



Fuente Creación Propia.

❖ **Paso 10:** Se selecciona el nombre de la imagen, las particiones y el tamaño de cada una de estas.

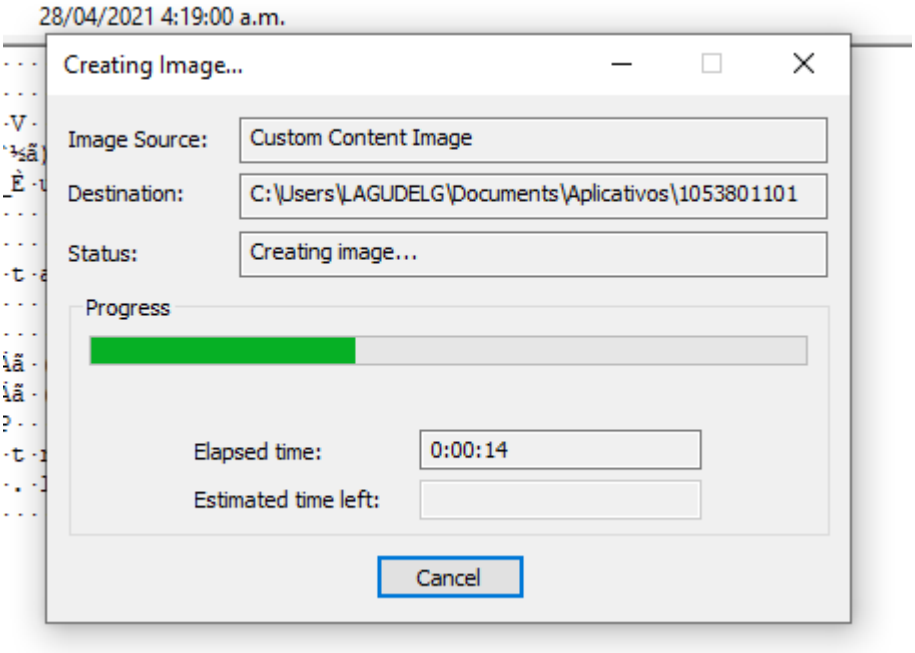
Ilustración 22.Selección opciones de encriptación Imagen Forense FTK Imager.



Fuente Creación Propia.

❖ **Paso 11:** Se inicia con la creación de la imagen forense.

Ilustración 23.Generacion Imagen Forense FTK Imager.



Fuente Creación Propia.

❖ **Paso 12:** Se generan los archivos que corresponden a la imagen forense.

Ilustración 24.Archivos generados imagen Forense. FTK Imager.

Fuente Creación Propia.

❖ **Paso 13:** Se observa el archivo txt con la información de la imagen forense.

Ilustración 25.TXT Reporte imagen Forense. FTK Imager.

```
Created By AccessData® FTK® Imager 4.5.0.3

Case Information:
Acquired using: ADI4.5.0.3
Case Number: 1053801101
Evidence Number: C1
Unique Description: EVIDENCIA FORENSE PRUEBA
Examiner: LEIDY VANESSA GIRALDO
Notes: PRUEBA

------------------------------------------------------------

Information for C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad1:
[Custom Content Sources]
 *(Wildcard,Consider Case,Include Subdirectories)
 \\.\PHYSICALDRIVE0:Partition 2 [532MB]:NONAME [NTFS]|[root]|System Volume Information|*(Wildcard
[Computed Hashes]
 MD5 checksum:    fa5f29ee71c34fa9809e131f2d855ad5
 SHA1 checksum:   d2641b83320eac7914b057f0ed91887578539b6b

Image information:
 Acquisition started:   Thu Jun 10 20:14:00 2021
 Acquisition finished:  Thu Jun 10 20:43:40 2021
 Segment list:
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad1
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad2
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad3
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad4
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad5
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad6
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad7
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad8
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad9
  C:\Users\LAGUDELG\Documents\Aplicativos\1053801101.ad10
```

Fuente Creación Propia.

Tabla 4.Características Técnicas FTK Imager

CARACTERÍSTICAS TÉCNICAS.	
Nombre Herramienta:	FTK Imager.
Tipo de Herramienta:	Software de escritorio.
Licenciamiento:	Cuenta con una versión libre que permite realizar la captura de imágenes forenses y una serie adicional de procesos para la recolección de evidencia.

	De igual manera también hace parte de un paquete herramientas de la compañía mucho más completo que se oferta en el mercado mediante licenciamiento.
Precio licencia.	La licencia de todo el kit de herramientas de FTK tiene un precio de 3.995 USD licencia perpetuidad.
Licencias o usuarios necesarios para el CSIRT.	Para el funcionamiento y la ejecución de los Servicios del CSIRT. Se necesita tener esta herramienta en todos los usuarios del área de: • Soporte de TI • Trabajo de Campo • I+D+I • Laboratorio • Operaciones.
Características Técnicas.	Es una herramienta que permite evaluar de una manera rápida y eficaz la evidencia electrónica mediante la captura de imágenes forenses de todos los datos informáticos de los diferentes equipos afectados.

Fuente: Creación Propia.

.6.4.2 SYSINSPECTOR

El CSIRT diseñado para las pequeñas y medianas empresas contara con un servicio proactivo que consiste principalmente en analizar y monitorear la infraestructura tecnológica de las organizaciones para detectar posibles amenazas o puertas traseras que estén siendo blanco de ciberdelincuentes para planear un ataque informático. Este servicio es fundamental ya que a través de un diagnostico constante de las organizaciones se podrán realizar procesos sencillos y eficaces que disminuyan el riesgo de una organización de recibir cualquier tipo de ataque. Es por esta razón que el CSIRT se basa en una herramienta que permite realizar un diagnóstico del equipo buscando principalmente códigos maliciosos y archivos que puedan llegar a estar corruptos en el sistema.
Las principales funciones de SYSINSPECTOR son:

- Detectar procesos y servicios activos en el sistema señalando con un color determinado el nivel de riesgo que representa para el equipo.
- Detectar archivos sospechosos o que no contengan firma en el sistema.
- Realizar un escaneo del software instalado para posteriormente detectar inconvenientes con este mismo.
- Detecta los controladores que pueden llegar a estar obsoletos o que están generando un problema de incompatibilidad con el sistema.
- Detecta Sistemas operativos sin licencias, sin actualizaciones e incluso sin parches de seguridad instalados.
- Revisa las entradas de registro del sistema y las categoriza dependiendo el riesgo, las que se encuentran rotas las señala con rojo porque representan un riesgo para la organización.

Debido a todas estas funciones es que se hace uso de esta herramienta para realizar el análisis y monitoreo como tal de los equipos pertenecientes a las organizaciones que hacen parte del CSIRT.

Ahora bien, para hacer uso de esta herramienta se debe ingresar al sitio web de la compañía ESET y descargar la herramienta la cual es gratuita.

Posterior a esto se ejecuta el .exe descargado y este empieza con el escaneo del equipo donde se está ejecutando.

❖ **Paso 1:** Ejecución y escaneo del equipo.

Ilustración 26.Ejecucion escaneo SYSINSPECTOR

Fuente Creación Propia.

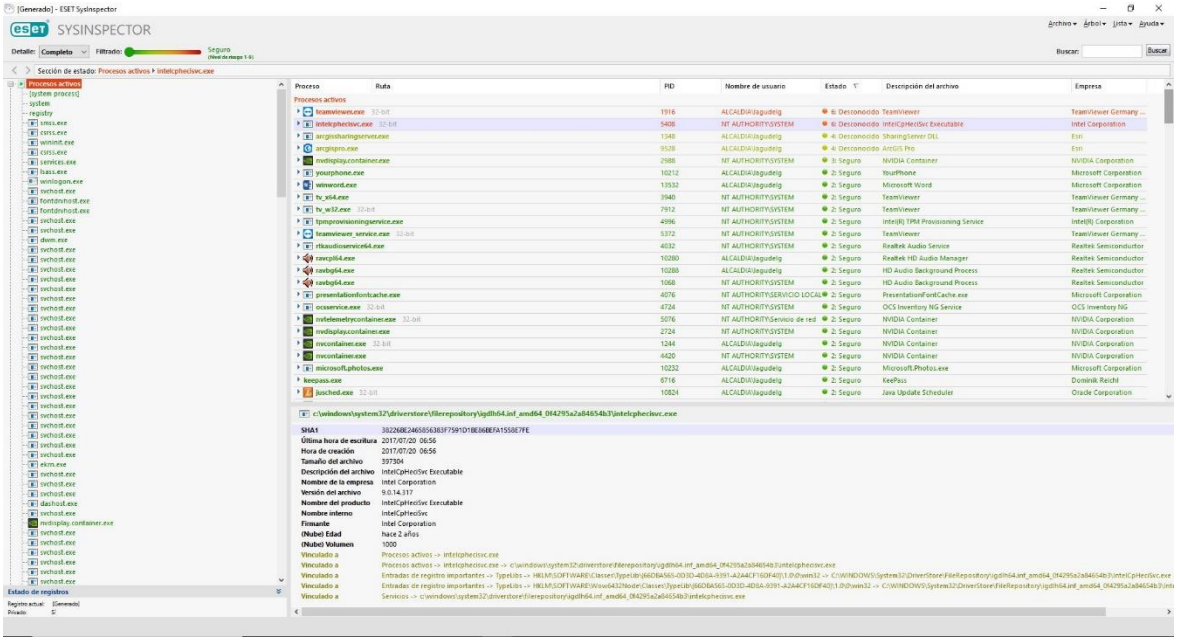
❖ **Paso 2:** Revisión del análisis generado por la herramienta.

Ilustración 27.Resultado Análisis SYSINSPECTOR

Fuente Creación Propia

❖ **Paso 3:** Se revisa la primera pestaña que corresponde a los procesos activos del sistema.

Ilustración 28.Procesos Activos del Sistema



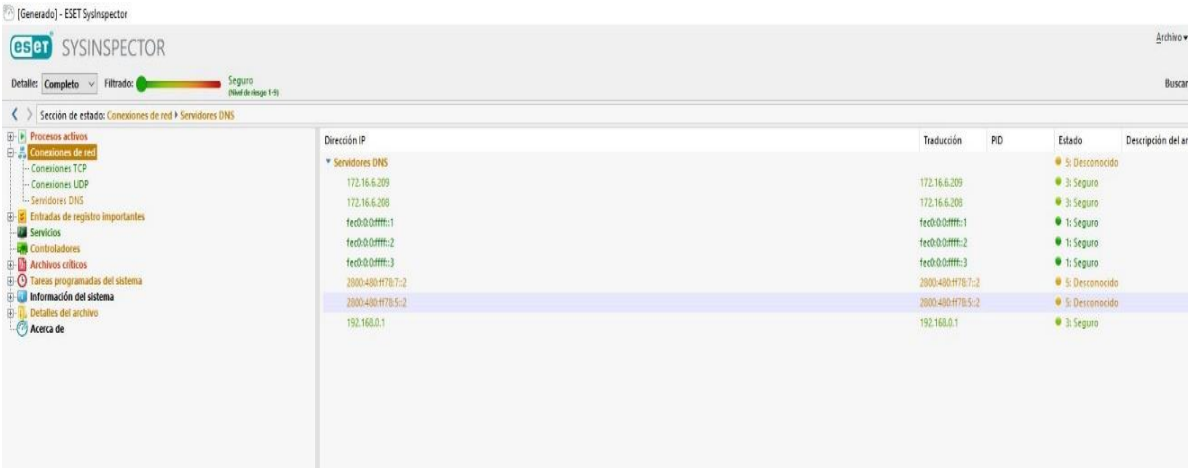
Fuente Creación Propia

SYSINSPECTOR permite visualizar una gama de colores dependiendo el riesgo que este genere en el equipo. Razón por la cual si el archivo se encuentra en rojo es porque fue detectado como una posible amenaza. Luego de darle clic al archivo se puede ver información sobre cuánto tiempo lleva instalado en el equipo, la versión de este, el código de encriptación sha1 y a que programas está vinculado.

Todo esto es fundamental para detectar si el archivo está generando o no un riesgo para el equipo donde se está ejecutando.

❖ **Paso 4:** Visualización de las conexiones de red

Ilustración 29.Conecciones de red SYSINSPECTOR



Fuente Creación Propia

Se puede observar el tipo de conexiones de la red, la IP que manejan y que servicio están ejecutando.

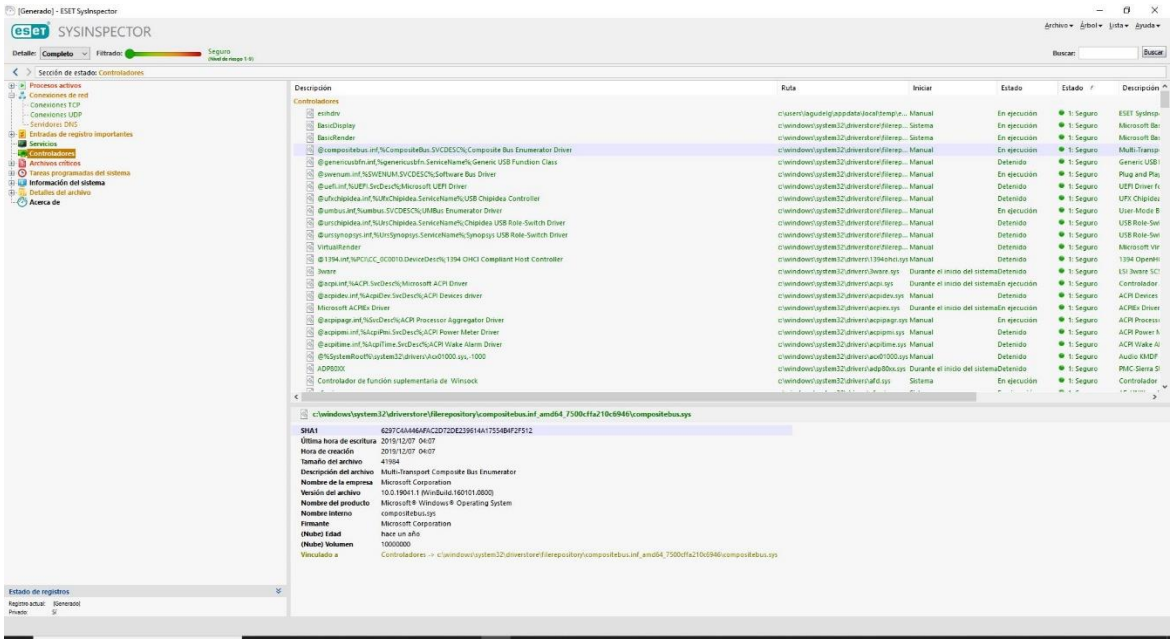
❖ **Paso 5:** Visualización de las entradas de registro importantes

Ilustración 30.Entradas de registro relevantes en el Sistema

Fuente Creación Propia

❖ **Paso 6:** Revisión de los controladores.

Ilustración 31.Revision controladores SYSINSPECTOR

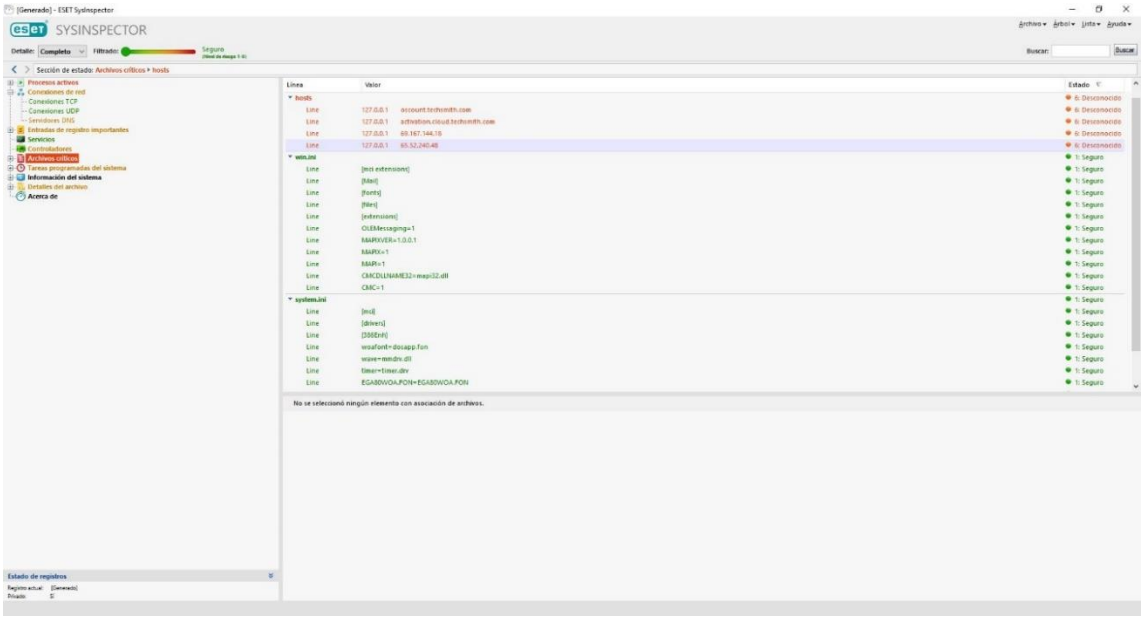


Fuente Creación propia

Se puede observar los controladores que tienen el sistema y toda la información asociada a este de tal manera que, si el color reflejado es verde, da a entender que no representa riesgo y no se encuentra roto ni obsoleto.

❖ **Paso 7:** Revisión de los servicios críticos del sistema.

Ilustración 32.Servicios críticos del sistema

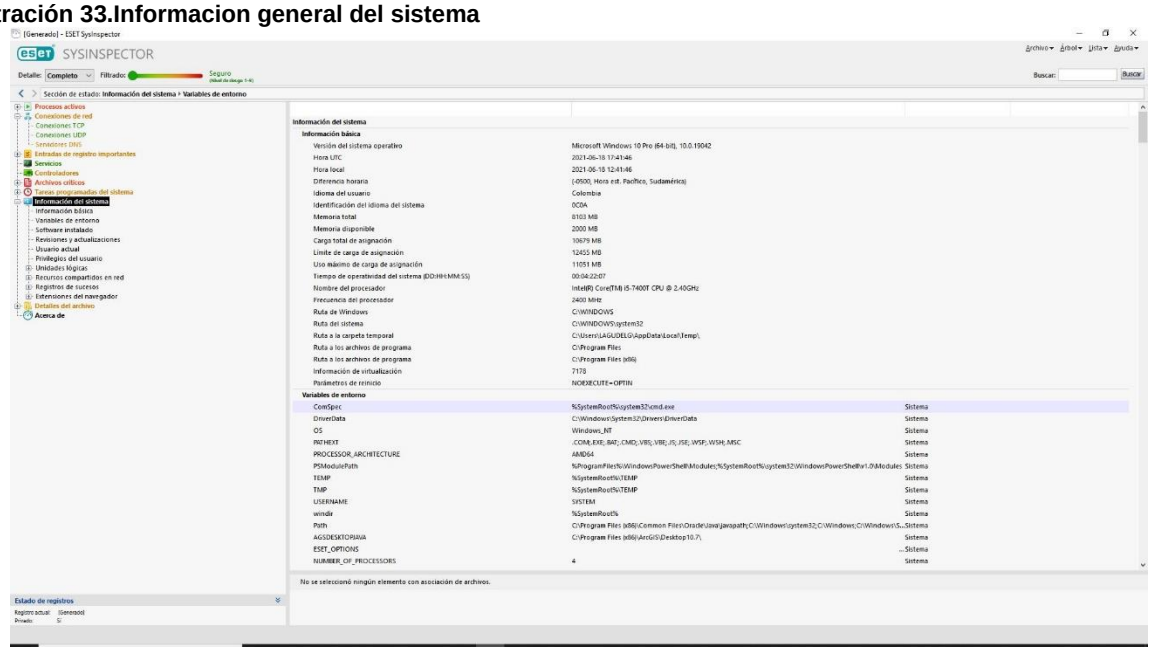


Fuente Creación propia

La herramienta revisa toda la información y detecta aquellos servicios que están representando un riesgo latente en el equipo principalmente porque la información no se muestra conocida por las librerías que usa SYSINSPECTOR para comparar cada uno de estos archivos.

❖ **Paso 8:** Información del sistema.

Ilustración 33.Informacion general del sistema

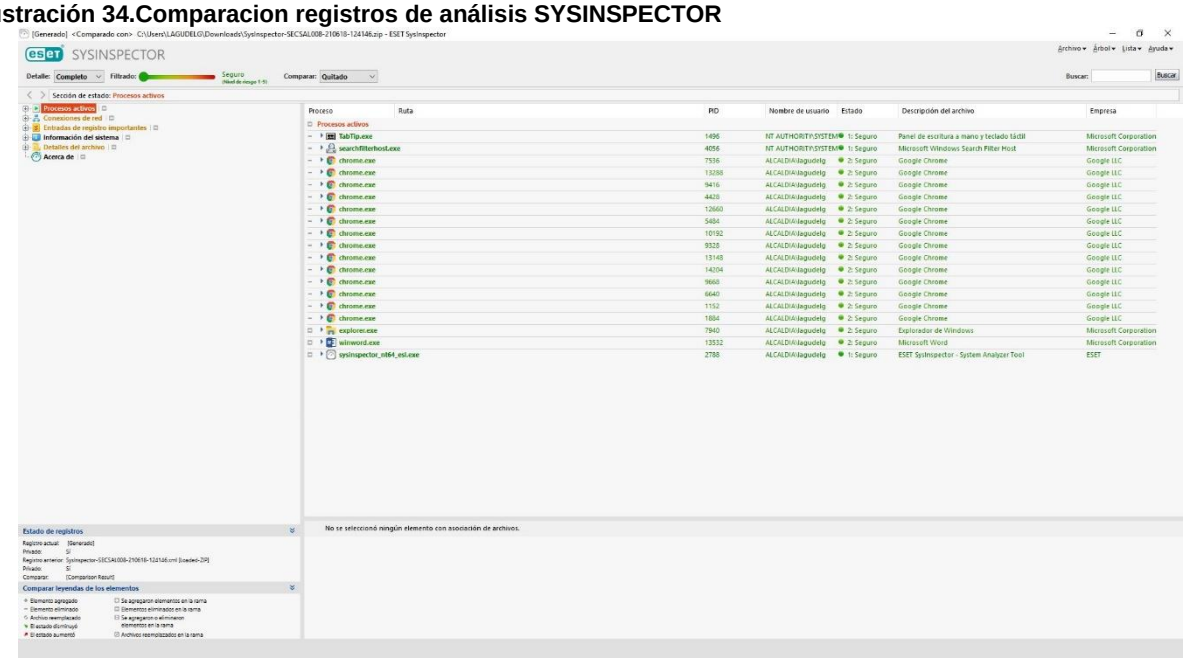


Fuente Creación propia

Es importante detectar la información del sistema a nivel general ya que ante un posible ataque esta puede ser alterada y puede cambiar los registros presentados en esta opción desde la herramienta.

❖ **Paso 9:** Comparación de registros.

Ilustración 34.Comparacion registros de análisis SYSINSPECTOR



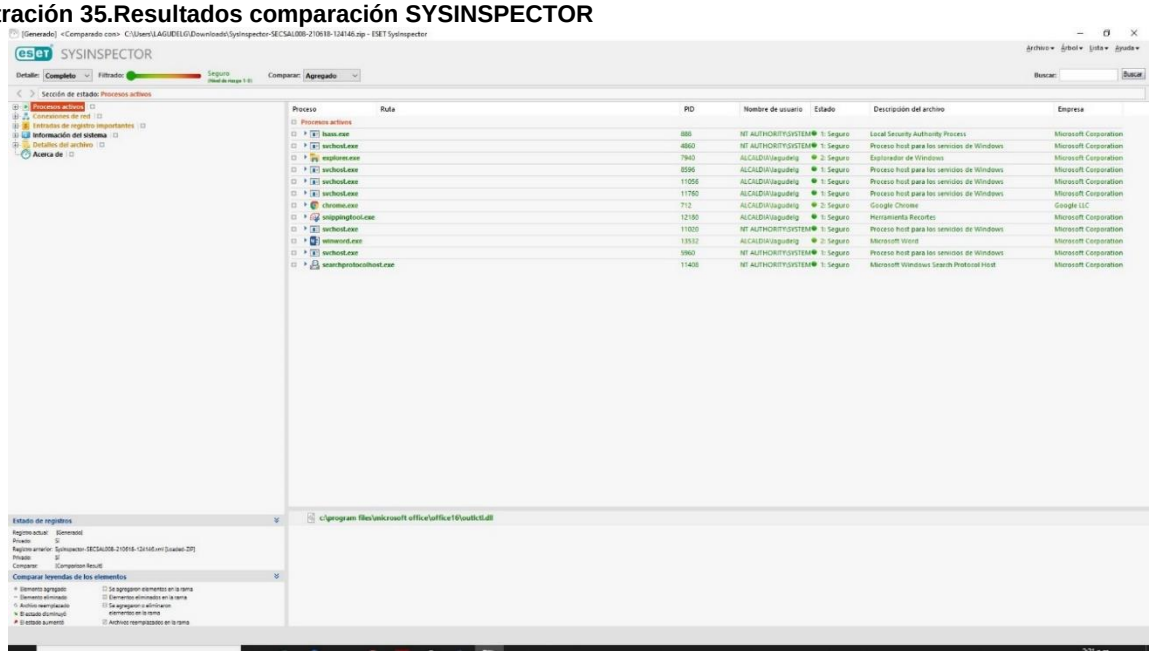
Fuente Creación propia

Es sin lugar a dudas una de las funcionalidades más importantes de la herramienta ya que esta permite guardar un escaneo para posteriormente compararlo con uno determinado.

De esta forma se puede verificar el sistema de hace x cantidad de tiempo con el que se encuentra ahora y detectar que servicios y que procesos se han creado visualizando al tiempo la criticidad de estos.

Para el equipo de trabajo de campo del CSIRT contar con esta comparación les permitirá detectar cambios de manera sencilla y poder estimar buenas prácticas de Seguridad Informática por parte del personal encargado del activo para de esta forma proceder a generar planes de mejora y recomendaciones para evitar futuros incidentes informáticos.

Ilustración 35.Resultados comparación SYSINSPECTOR



Fuente Creación propia

Tabla 5.Características Técnicas SYSINSPECTOR.

CARACTERÍSTICAS TÉCNICAS.	
Nombre Herramienta:	SYSINSPECTOR
Tipo de Herramienta:	Cliente Servidor. Software de escritorio.
Licenciamiento:	Es una herramienta gratuita para Windows.
Precio licencia.	
Licencias o usuarios necesarios para el CSIRT.	Para el funcionamiento y la ejecución de los Servicios del CSIRT. Se necesita tener esta herramienta en todos los usuarios del área de: • Trabajo de Campo • Laboratorio • Operaciones.
Características Técnicas.	Esta herramienta permite determinar los procesos en ejecución, archivos de registro, entre otros, a su vez mediante diferentes tipos de algoritmos y librerías de datos le asigna un nivel de riesgo a cada uno de los objetos registrados en el análisis.

Fuente: Creación Propia.

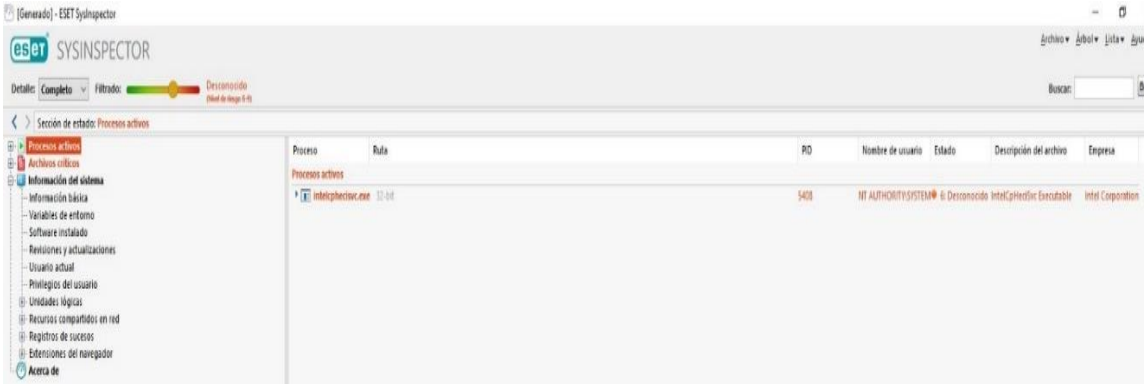
.6.4.3 PESTUDIO

Esta herramienta es ideal para realizar las funciones un CSIRT, principalmente porque es fácil de utilizar, no consume recursos y genera información acertada de diferentes archivos ejecutables en Windows.

Realiza un análisis del archivo .exe y los compara con diferentes librerías de antivirus con el fin de recopilar la reputación de este archivo en las bases de datos y poder determinar la procedencia correcto funcionamiento del ejecutable.

Su funcionamiento va ligado principalmente a SYSINSPECTOR ya que a través de esta herramienta se hace un análisis de los procesos, registros y redes del equipo determinado el riesgo que puede llegar a representar uno de estos procesos en el equipo.

Ilustración 36.Ubicación archivo vulnerable SYSINSPECTOR

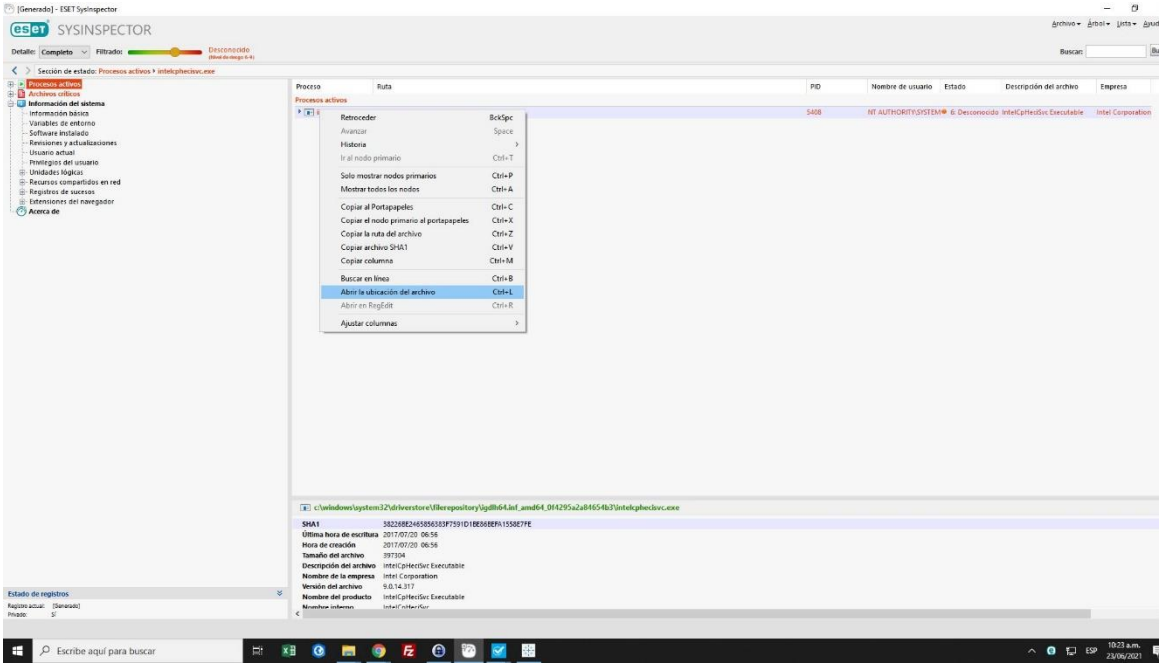


Fuente Creación propia

Posterior a realizar el Análisis con Sysinspector se determina que existe un proceso que contiene un ejecutable que se determina como desconocido de tal manera que el sistema no puede corroborar su procedencia y puede llegar a ser malicioso.

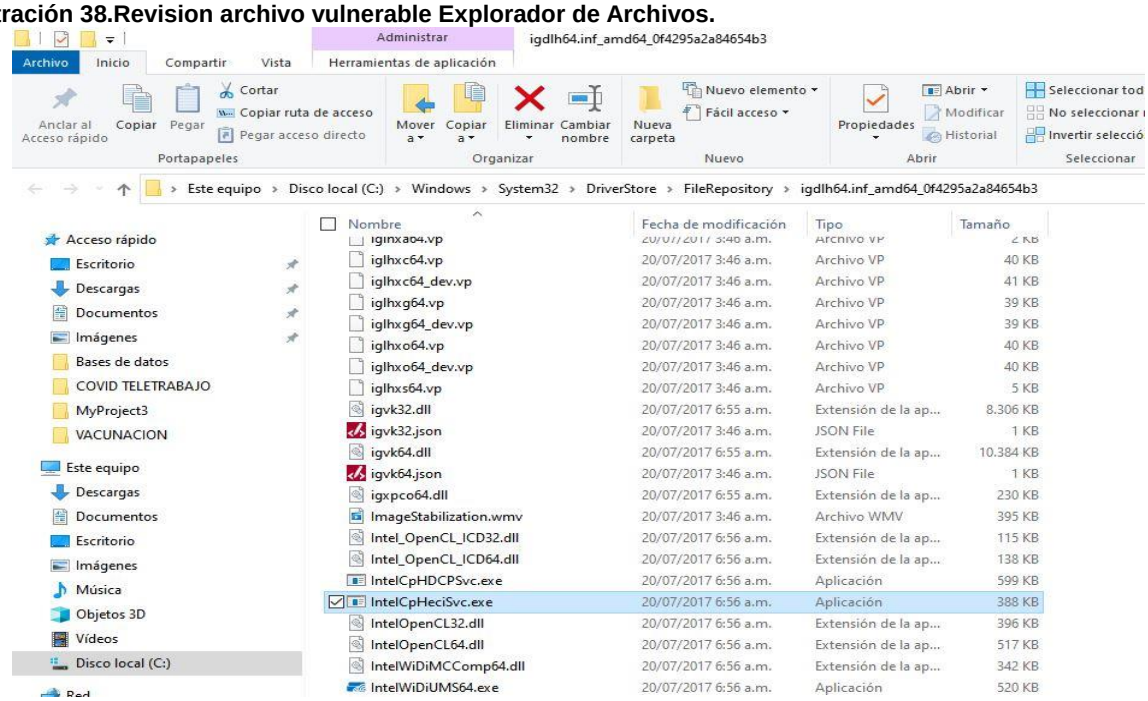
A partir de este archivo se determina la ubicación para posteriormente analizarla con PESTUDIO.

Ilustración 37.Selección archivo vulnerable SYSINSPECTOR



Fuente Creación propia

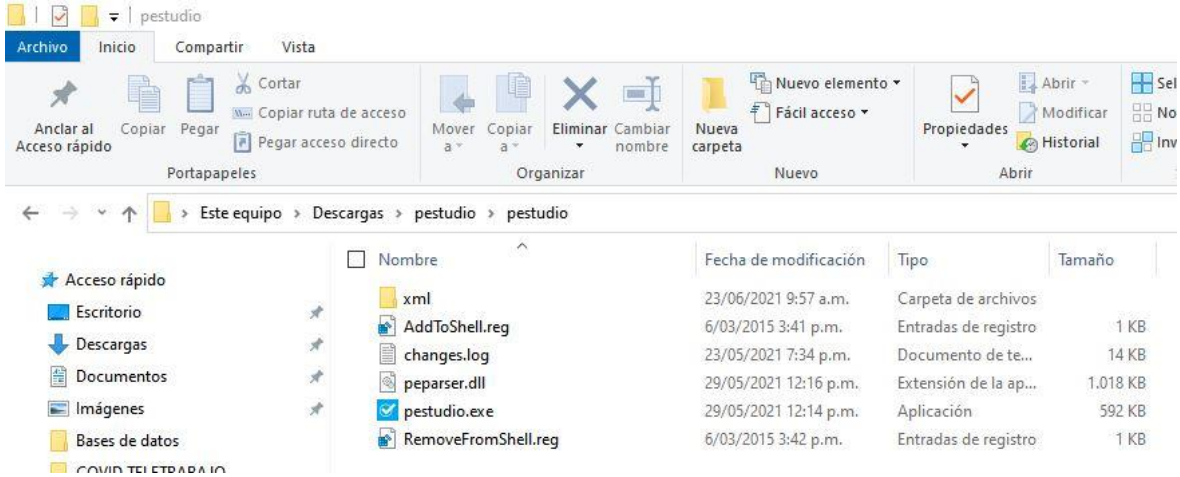
Ilustración 38.Revision archivo vulnerable Explorador de Archivos.



Fuente Creación propia

Luego de encontrar el archivo sospechoso, se ejecuta la herramienta PESTUDIO.

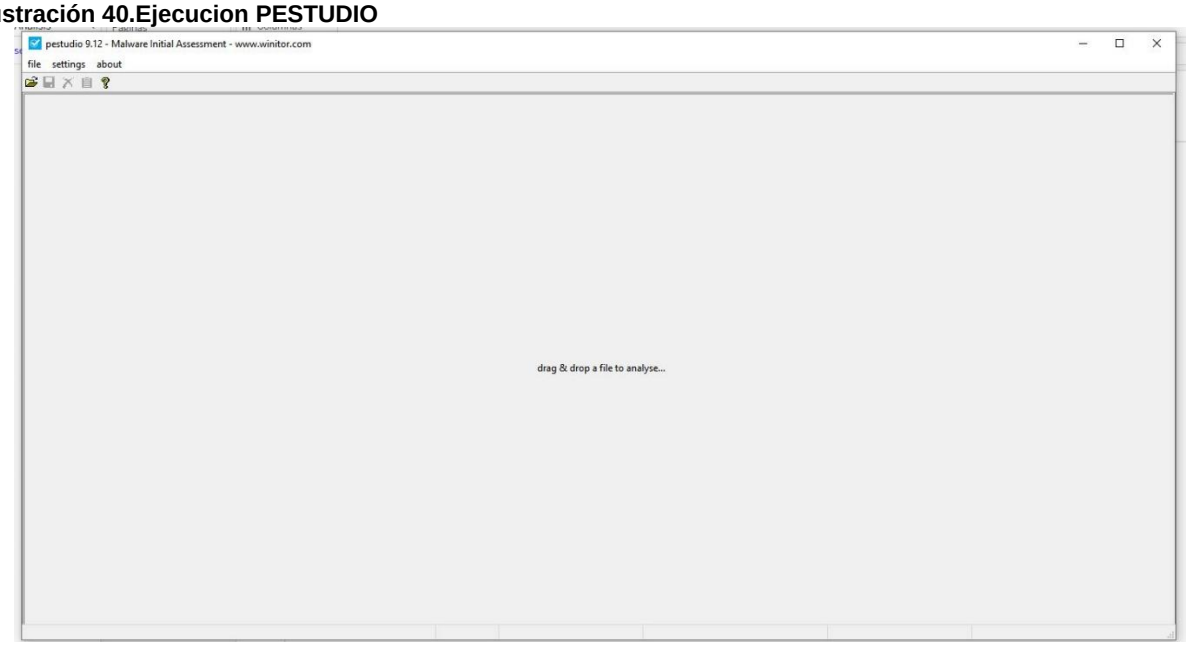
Ilustración 39.Ubicación ejecutable PESTUDIO



Fuente Creación propia

Se arrastra en este caso el ejecutable sospechoso a la herramienta.

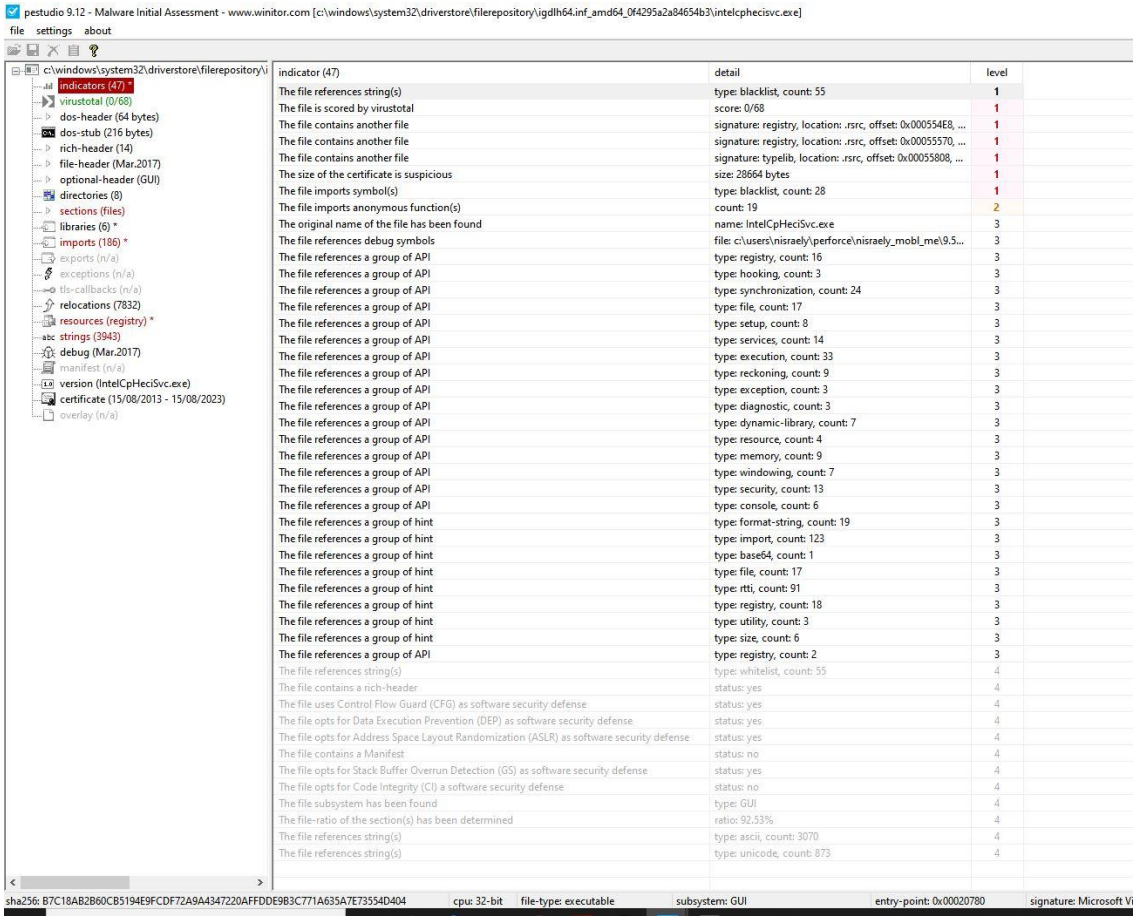
Ilustración 40.Ejecucion PESTUDIO



Fuente Creación propia

Luego de esto el sistema realiza el análisis del archivo y muestra los resultados mediante un panel con categorías semaforizadas por colores, en donde el color rojo hace referencia a la información más relevante en el sistema.

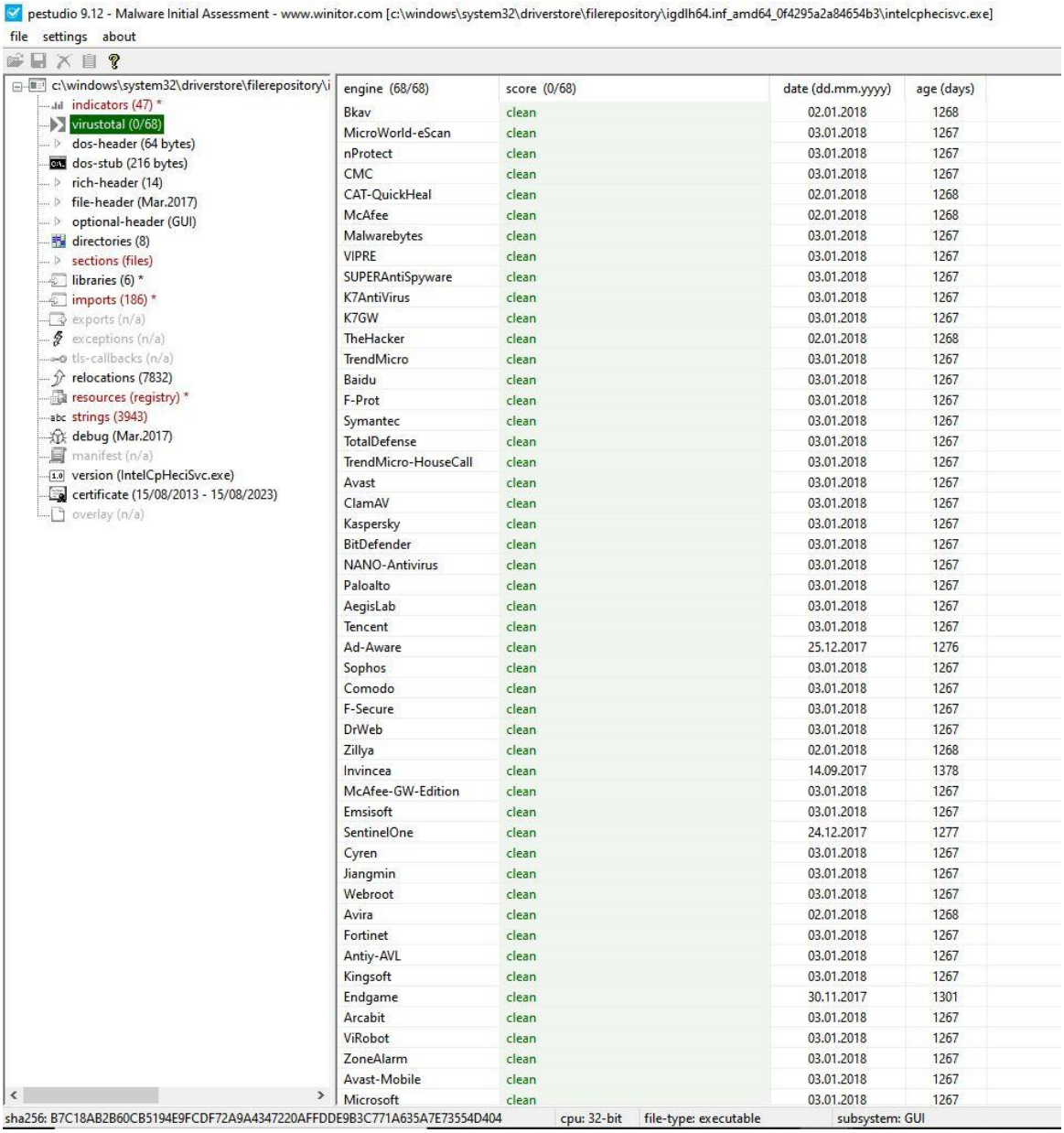
Ilustración 41.Analisis archivo vulnerable PESTUDIO



Fuente Creación propia

Sin lugar a dudas un aspecto fundamental de la herramienta es la revisión del archivo a través de Virus Total, el cual hace un análisis de este en todas sus bases de datos para posteriormente arrojar el resultado detectado del análisis.

Ilustración 42.Revision Virus Total PESTUDIO

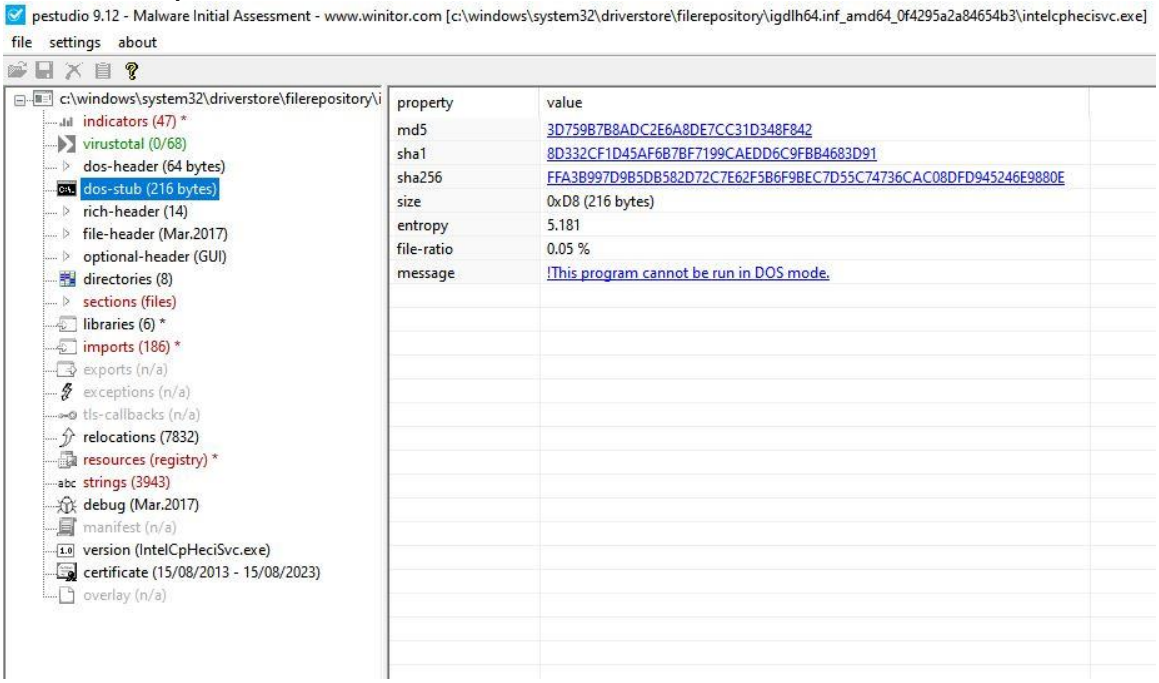


engine (68/68)	score (0/68)	date (dd.mm.yyyy)	age (days)
Bkav	clean	02.01.2018	1268
MicroWorld-eScan	clean	03.01.2018	1267
nProtect	clean	03.01.2018	1267
CMC	clean	03.01.2018	1267
CAT-QuickHeal	clean	02.01.2018	1268
McAfee	clean	02.01.2018	1268
Malwarebytes	clean	03.01.2018	1267
VIPRE	clean	03.01.2018	1267
SUPERAntiSpyware	clean	03.01.2018	1267
K7AntiVirus	clean	03.01.2018	1267
K7GW	clean	03.01.2018	1267
TheHacker	clean	02.01.2018	1268
TrendMicro	clean	03.01.2018	1267
Baidu	clean	03.01.2018	1267
F-Prot	clean	03.01.2018	1267
Symantec	clean	03.01.2018	1267
TotalDefense	clean	03.01.2018	1267
TrendMicro-HouseCall	clean	03.01.2018	1267
Avast	clean	03.01.2018	1267
ClamAV	clean	03.01.2018	1267
Kaspersky	clean	03.01.2018	1267
BitDefender	clean	03.01.2018	1267
NANO-Antivirus	clean	03.01.2018	1267
Paloalto	clean	03.01.2018	1267
AegisLab	clean	03.01.2018	1267
Tencent	clean	03.01.2018	1267
Ad-Aware	clean	25.12.2017	1276
Sophos	clean	03.01.2018	1267
Comodo	clean	03.01.2018	1267
F-Secure	clean	03.01.2018	1267
DrWeb	clean	03.01.2018	1267
Zillya	clean	02.01.2018	1268
Invincea	clean	14.09.2017	1378
McAfee-GW-Edition	clean	03.01.2018	1267
Emsisoft	clean	03.01.2018	1267
SentinelOne	clean	24.12.2017	1277
Cyren	clean	03.01.2018	1267
Jiangmin	clean	03.01.2018	1267
Webroot	clean	03.01.2018	1267
Avira	clean	02.01.2018	1268
Fortinet	clean	03.01.2018	1267
Antiy-AVL	clean	03.01.2018	1267
Kingsoft	clean	03.01.2018	1267
Endgame	clean	30.11.2017	1301
Arcabit	clean	03.01.2018	1267
ViRobot	clean	03.01.2018	1267
ZoneAlarm	clean	03.01.2018	1267
Avast-Mobile	clean	03.01.2018	1267
Microsoft	clean	03.01.2018	1267

Fuente Creación propia

De igual forma, se muestra la información que tiene que ver con la encriptación del archivo.

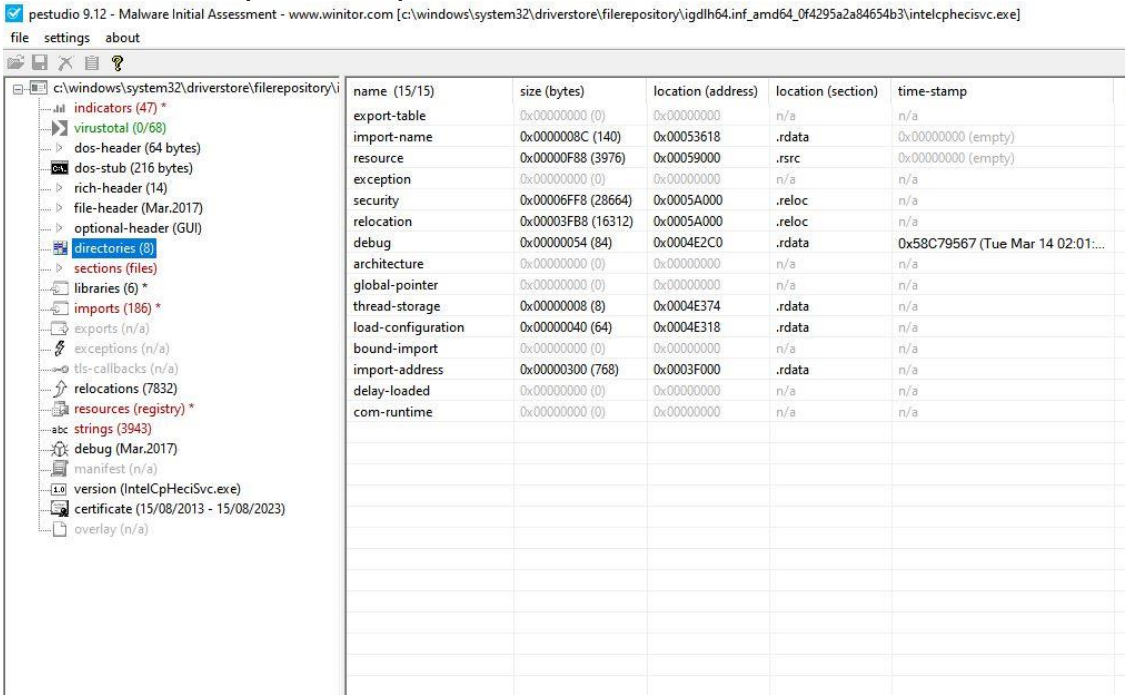
Ilustración 43.Encriptacion archivo vulnerable PESTUDIO



Fuente Creación propia

Muestra los directorios que contiene la aplicación.

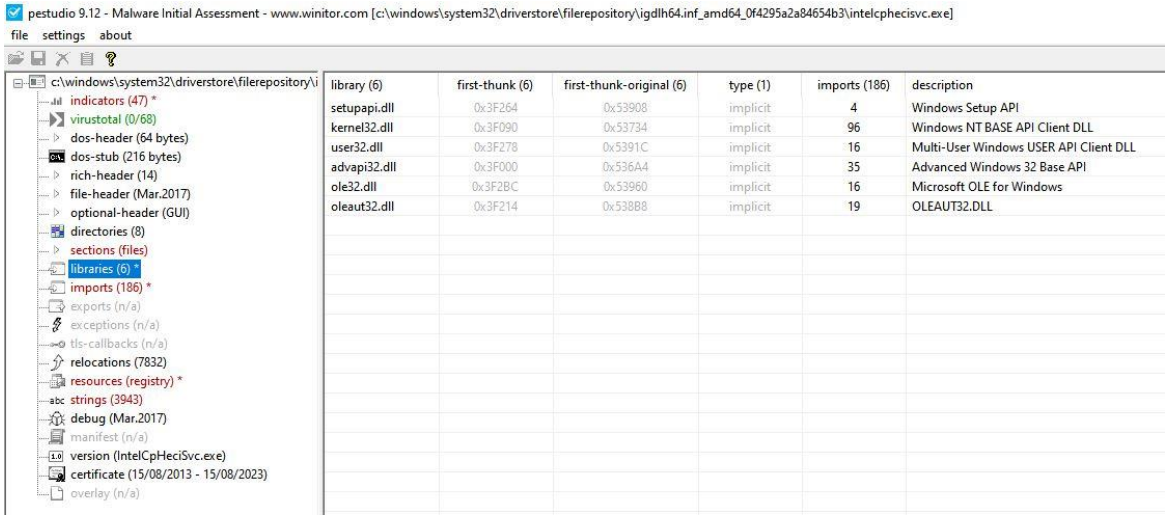
Ilustración 44.Directorios aplicación sospechosa PESTUDIO



Fuente Creación propia

Analiza las librerías y los .dll del ejecutable generando de esta forma una descripción que entregara una información adicional del archivo como tal.

Ilustración 45.Librerias de funcionamiento archivo vulnerable PESTUDIO



Fuente Creación propia

De la misma forma realiza análisis de diferentes aspectos fundamentales para determinar el peligro del archivo en el sistema.

En el caso de realizar el análisis con un archivo malicioso que para este caso será KMSPICO que se considera un malware, el sistema mostrará un comportamiento muy diferente al archivo analizado anteriormente.

Ilustración 46.Visualizacion KMSPICO en Virus Total PESTUDIO

Fuente Creación propia

Como se puede observar en la imagen, KMSPICO es considerado como un malware por diferentes librerías con las que cuenta Virus Total para realizar el análisis correspondiente.

De esta forma se podría llegar a determinar cuál fue el archivo ejecutable que desencadeno el Incidente de Seguridad Informática en la organización.

Tabla 6.Características Técnicas de PESTUDIO

CARACTERÍSTICAS TÉCNICAS.	
Nombre Herramienta:	PESTUDIO.
Tipo de Herramienta:	Cliente Servidor. Software de escritorio portable.
Licenciamiento:	Es una herramienta gratuita.
Precio licencia.	
Licencias o usuarios necesarios para el CSIRT.	Para el funcionamiento y la ejecución de los Servicios del CSIRT. Se necesita tener esta herramienta en todos los usuarios del área de: • Trabajo de Campo • Laboratorio • Operaciones. • I+D+I • Soporte TI.
Características Técnicas.	Esta es una herramienta portable que permite detectar toda la información de un archivo ejecutable para de esta forma realizar una evaluación inicial de un posible malware. Permite observar todos los indicadores de cada uno de los ejecutables de una manera amigable y fácil de entender.

Fuente: Creación Propia.

.7 CONCLUSIONES

En Colombia la incidencia de delitos informáticos en las Pequeñas y Medianas empresas ha venido en notable crecimiento, entre el 2019 y el 2020 el incremento de estos delitos fue del 54%. De esta forma las empresas se han visto afectadas por delitos como el hurto informático, la violación a los datos personales y el acceso abusivo a sistemas de información entre otros.

Lo anterior ha evidenciado deficiencias notables en aspectos de Seguridad Informática en las Pymes, a tal punto que muchos de estos no logran mantenerse en el mercado mucho tiempo después de un ciberataque ya que el daño ocasionado por este tipo de delitos fue tan catastrófico que la inversión económica que se necesitó para solucionarlo afecto altamente la estructura financiera de la organización.

Actualmente es prácticamente imposible estar completamente blindados de ataques de seguridad de la información, por el contrario, cada día surgen ataques mucho más sofisticados, más personalizados y más letales. Es por esta razón que nunca serán suficientes los esfuerzos aplicados dentro de organizaciones o Equipos de Respuesta a Incidentes Informáticos en cuanto a prácticas para mitigar y prevenir ataques informáticos.

Los propietarios de las diferentes fuentes de información que se manejan en las compañías, son absolutamente responsables del manejo que se les dé a estas. Es por esta razón que, al ser el activo más importante y más vulnerable, es necesario invertir recursos Físicos, Humanos y Económicos que permitan generar protocolos de seguridad para salvaguardar dicho activo.

Un CSIRT es una solución altamente efectiva ante temas de Ciberdelincuencia, esto debido a que estos equipos no solo se dedican a abordar ataques de Seguridad de la información, sino que también se dedican a retroalimentar diferentes comunidades en cuanto a comportamientos similares de ataques para de esta forma actuar antes de que se presente estos tipos de Incidentes.

La capacitación al personal no se debe de realizar solo para el Área de TI de una organización, por el contrario; la capacitación y la formación debe de hacerse en todas las áreas de una organización ya que es fundamental que los usuarios cuenten con conocimientos mínimos de ciberseguridad para de esta forma evitar ser flancos fáciles de ataques dirigidos.

Una vez se evidencie o se advierta a los diferentes entes la importancia de la implementación de este tipo de equipos, se darán avances importantes en cuanto a que no solo se beneficiaran empresas afiliadas a CSIRT sino toda la comunidad que haga

uso de información puesto que la labor de estas organizaciones es la de divulgar y retroalimentar acerca de posibles ataques o vulnerabilidades detectadas al orden del día. De igual forma a partir del uso de estos equipos también habrá cabida para el desarrollo de todos los aspectos que este implica, bien sea la capacitación, educación y demás mecanismos que conlleva realizar estas actividades.

En cuanto a los requerimientos tecnológicos para el funcionamiento de un CSIRT para las pequeñas y medianas empresas en Colombia, este debe contar con una serie de equipos de hardware que le permitan prestar los servicios que este tipo de Organizaciones ofertan, es fundamental realizar inversiones fuertes en temas como Servidores para aplicaciones, para backup y para laboratorios; todo esto con el fin de responder oportunamente a los requerimientos de las PYMES en el momento oportuno.

Para que un CSIRT sea efectivo y represente una alternativa de solución ante incidentes informáticos para las pequeñas y medianas empresas, este debe contar con software que les permitan partir desde el análisis que harán los usuarios finales constantemente a sus equipos para mediante análisis desde los profesionales del CSIRT detectar anomalías en el comportamiento del activo tecnológico, de igual forma deben adquirir herramientas tecnológicas que les permitan capturar la evidencia digital del ataque determinado para proceder a realizar la gestión del incidente como tal con herramientas de detección, recuperación y depuración de programas maliciosos en los ordenadores. Por último es fundamental adquirir o desarrollar herramientas que optimicen el proceso de restaurar la información y los equipos a la versión estable antes del incidente de seguridad informática, todo esto es fundamental para aumentar la confianza en los clientes y poder captar diferentes empresas que requieran no solo de la solución de los incidentes sino también la formación de sus profesionales para adoptar buenas prácticas de seguridad informática en la organización.

De igual manera un CSIRT adaptado a las pequeñas y medianas empresas debe contar dentro de su personal técnico con profesionales que no solo se encarguen de dar respuesta a los incidentes informáticos sino que también estén en la capacidad de investigar y desarrollar nuevas herramientas que optimicen todo el proceso y que les sirvan a las empresas del mercado como alternativas para evitar ciberataques, así mismo se requiere contar con profesionales que puedan manejar las relaciones públicas de la organización de tal manera que estén constantemente retroalimentando los diferentes canales de comunicación con el fin de captar clientes constantemente.

Crear laboratorios controlados en donde se prueben herramientas de software útiles para la ejecución de los servicios de un CSIRT para las pequeñas y medianas empresas es una excelente alternativa para evidenciar el proceso aplicado de cada una de estas y poder comprobar sus beneficios. Dentro de estas herramientas, es fundamental contar con alguna que permita capturar la imagen en su estado actual para posteriormente realizar técnicas de análisis digital, tal es el caso de FTK Imager la cual permite crear una imagen de una unidad del ordenador y generarla en múltiples formatos para posteriores

análisis; así mismo a través de SYSINSPECTOR se puede observar el estado de la máquina que está siendo monitoreada, de esta forma se pueden evidenciar procesos críticos de la organización que posteriormente serán analizados mediante PESTUDIO para poder determinar la criticidad de la aplicación y su reputación en las diferentes bases de datos de compañías de ciberseguridad, de esta manera se puede entrever que aplicaciones son seguras y cuales representan un riesgo latente para la organización.

Para diseñar la propuesta de la infraestructura lógica de un Csirt funcional para las pequeñas y medianas empresas debe de partir principalmente de un análisis del entorno en temas de Ciberseguridad para posteriormente proceder a realizar la propuesta como tal de las herramientas tecnológicas. Dentro de estas herramientas se tienen que tener presento todas aquellas que permitan ejecutar los servicios ofertados por el CSIRT tales como servidores de correo electrónico, backup, aplicaciones, equipos de alta gama que contengan diferentes sistemas operativos para de esta forma generar entornos controlados desde diferentes perspectivas, en cuanto a herramientas de software es importante contar con las más básicas tales como FTKImager, SYSINSPECTOR, PESTUDIO,CISCO WEBEX, entre otros que permitan la gestión del incidente de una manera precisa, controlada y eficaz.
Por último y no menos importante, la infraestructura lógica de un CSIRT que funcionara en el campo de las pequeñas y medianas empresas debe contar con una estructura organizacional del personal con el que podrá ejecutar sus procesos, a través de esta estructura se seleccionaran las profesiones necesarias para un mejor rendimiento y se podrán asignar funciones dentro de la organización con el fin de optimizar tiempo y recursos en aras de lograr un correcto desempeño de los objetivos organizacionales. Es por esta razón que dentro de los perfiles que se requieren para este tipo de equipos, se encuentran Ingenieros de Sistemas, Administradores de Sistemas Informáticos, Arquitectos de Software, Especialistas en Seguridad informática, entre otros. Todos estos perfiles apuntan a un manejo de los incidentes de seguridad informática desde un punto de vista técnico pero también desde un punto de vista estratégico, ya que dentro de estas profesiones se adquieren herramientas para adaptar las necesidades y las problemáticas en nuevas oportunidades de negocio.

.8 RECOMENDACIONES

Se recomienda que todas las organizaciones de mediana o alta capacidad estén subscritas o cuenten con el apoyo de un CSIRT esto debido a que no es fácil repeler ataques digitales y en muchos casos los profesionales de dichas organizaciones no cuentan con los conocimientos necesarios para de esta forma tratar estas amenazas. Es por esta razón que lo ideal es hacer uso de estos equipos que están altamente capacitados y cuentan con la infraestructura necesaria para actuar inmediatamente ante un incidente y por ende de esta forma se mitigaría el daño ocasionado.

En cuanto a las iniciativas para la creación de un CSIRT en los diferentes sectores de la economía, lo ideal es partir de definir el público objetivo ya que de esta definición se podrán desarrollar los servicios prestados. Esto porque cada sector de la economía trae consigo un fin determinado de ciberataques, de esta forma en algunos casos el CSIRT puede centrar su actuar en servicios proactivos y en otro tipo puede llegar a centrar sus funciones en servicios reactivos; lo que se busca en esta situación es optimizar los procesos y dar respuestas inmediatas a los diferentes incidentes de seguridad informática.

Es importante que un CSIRT para las pequeñas y medianas empresas tenga claro que debe generar las soluciones necesarias no solo para dar la gestión del incidente sino que debe centrar grandes esfuerzos en el proceso posterior a solucionar dicho incidente, esto principalmente por los daños colaterales que suele traer consigo este tipo de actos, de tal manera que estos equipos deben dedicar diferentes acciones en restaurar los activos tecnológicos a su versión segura más reciente y en brindarles las herramientas e información necesaria para evitar este tipo de acciones que suelen presentarse frecuentemente, de esta forma a través de procesos que le permitan a la organización víctima del ataque prevenir futuros incidentes, le servirá para recuperar la confianza de sus clientes y recuperarse económicamente de este ataque a través del funcionamiento correcto de sus servicios.

Para crear la estructura lógica de un CSIRT que actué dentro del sector de las Pequeñas y medianas empresas es importante que se realice una investigación de campo acerca de cómo se encuentran las tendencias de Ciberseguridad en este sector de la economía, de esta forma se podrán evidenciar los ataques más persistentes, los ataques más críticos e incluso los ataques que suelen ser más efectivos. Partiendo de esta investigación se debe proceder a crear la ejecución y los objetivos del Centro en base a este tipo de incidentes, de esta forma se darán soluciones efectivas y reales ya que en caso de que un incidente de Ciberseguridad se presente, ya existe un estudio reciente de las tendencias y ya se ha labrado un largo camino que permite actuar basados en la información ya publicada por diferentes Equipos y organizaciones; todo esto genera efectividad y rapidez a la hora de darle respuesta a un incidente de Seguridad Informática.

Dentro de una propuesta de infraestructura lógica para un CSIRT que preste sus servicios para las pequeñas y medianas empresas debe traer también consigo una propuesta de la estructura organizacional de este tipo de equipos. Este proceso es fundamental ya que mediante esta estructura se definirán los profesionales que se requieren para funcionar como tal en base a los servicios que se prestaran. De igual forma al diseñar la estructura organizacional, se debe tener en cuenta las responsabilidades de cada uno de estos profesionales y el área en la que actuara para así poder observar las áreas que cuentan con mayor apoyo de talento humano y cuáles de estas áreas deben ser reforzadas con nuevos profesionales. Así mismo esta estructura debe de estar directamente ligada al diseño tanto de la planta física como de la planta tecnológica del CSIRT. De esta forma se podrán evidenciar los espacios, la cantidad de equipos y las condiciones de cada área para que las funciones se presten de manera continua y se puedan mitigar posibles riesgos por temperatura, fallas eléctricas, entre otros.

.9 BIBLIOGRAFÍA

ACIS. Ciberseguridad: la aliada de las PyMEs durante la realidad actual. 2020. [En linea]. [Consulta: 21 de Junio 2021].Disponible en: https://www.acis.org.co/portal/content/noticiasdelsector/ciberseguridad-la-aliada-de-las-pymes-durante-la-realidad-actual

Asuntos: Legales, Judicial. [Sitio web]. Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis. [consulta: 2 de mayo de 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480

AGUILAR ANTONIO, Juan Manuel. Hechos ciberfísicos: una propuesta
De análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 25. 2020. [consulta: 20 de Junio de 2021]

AGUILAR CARCELES, Marta Maria. Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. Revista Criminalidad, 57 (1): 121-135. (2015). [consulta: 20 de Junio de 2021]

BARRIO ANDRES, Moises. [En línea].Delitos 2.0: Aspectos penales, procesales y de seguridad de los Ciberdelitos. [consulta: 17 Mayo de 2021].Disponible en: https://www.moisesbarrio.es/pdf/libro_delitos_2.0_ciberdelitos.pdf

BALLESTERO, Fernando. LA CIBERSEGURIDAD EN TIEMPOS DIFÍCILES ¿Nos ocupamos de ella o nos preocupamos por ella? Boletín económico de ICE 3122. 2020. [consulta: 20 de Junio de 2021]

Cámara Colombiana de Informática y Telecomunicaciones (CCIT), Tanque de Análisis y creatividad de las TIC(TicTac), Centro De Capacidades para la Ciberseguridad en Colombia (c4). [En línea]. Informe de las tendencias Cibercrimen en Colombia 2019-2020. Programa seguridad aplicada al fortalecimiento empresarial (SAFE). Octubre 29 de 2019. [consulta: el 26 de Mayo de 2021].Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

CANDO SEGOVIA, Mauricio Rodrigo.; MEDINA CHICAIZA, Patricio. Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10(1), 17-41. 2021. [consulta: 20 de Junio de 2021]

CANO VARGAS, Jaidur. Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso

de estudio Cibersecurity de Colombia LTDA. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA BOGOTÁ DC. 2020. [consulta: 20 de Junio de 2021]

CÁRDENAS SOLANO, Leidy Johanna.; MARTÍNEZ ARDILA, Hugo.; BECERRA ARDILA, Luis Eduardo. "Gestión de seguridad de la información: revisión bibliográfica". El profesional de la información, v. 25, n. 6, pp. 931-948. (2016). [consulta: 20 de Junio de 2021].

CCIT. TENDENCIAS DE CIBERCRIMEN EN COLOMBIA. Bogotá DC. 2019. [En linea]. [Consulta: 21 de Junio 2021].Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

CN-CERT. [Sitio web]. Centro Cristológico Nacional. [consulta: 17 de mayo de 2021]. Disponible en: https://www.ccn-cert.cni.es/

COLOMBIA.CONGRESO DE LA REPUBLICA DE COLOMBIA. [En línea].Bogotá, D.C. Ley 590 de 2000. (10 de Julio.). Por lo cual se dictan disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresas. [consulta: 17 de Mayo de 2021].Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0590_2000.html

COLOMBIA.CONGRESO DE LA REPUBLICA. [En línea].Bogotá, D.C. Ley 1273 del 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [consulta: 17 de Mayo de 2021].Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA.CONGRESO DE LA REPUBLICA. [En línea].Bogotá, D.C. Ley 1928 24 de Julio de 2018. Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", Adoptado el 23 de noviembre de 2001 en BUDAPEST. [consulta: 23 de Mayo de 2021].Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

COLOMBIA.CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. [En línea].Bogotá, D.C. CONPES 3854. (11 de abril de 2016). Política Nacional de Seguridad Digital. [consulta: 17 de Mayo de 2021].Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CORTES BORRERO, Rodrigo. Estado actual de la política pública de

Ciberseguridad y ciberdefensa en Colombia. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 14. Universidad de los Andes (Colombia). 2015. [consulta: 20 de Junio de 2021].

CSIRTs. El mapa interactivo de CSIRTs por países. [En linea]. [Consulta:25 de Junio 2021].Disponible en: https://derechodelared.com/mapa-csirts-por-pais/

CUJABANTE VILLAMIL, Ximena.; BAHAMON JARA, Martha.; PRIETO VANEGAS, Jair.; QUIROGA AGUILAR, Jorge. Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. Universidad Militar Nueva Granada. Revista Científica General José María Córdova. Bogotá DC. 2020. [consulta: 10 de Junio de 2021]

Deloitte. [Sitio web]. Ciber Riesgos y Seguridad de la Información en América latina & Caribe. Países más afectados por el Ransomware en Latinoamérica durante 2018. [consulta: 6 de mayo de 2021]. Disponible en: https://www2.deloitte.com/co/es/pages/risk/articles/ciber-riesgos-y-seguridad-de-la-info-en-america-latina-y-caribe.html

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL. Bogotá D. C. 2018. [Consulta: 17 de mayo de 2021].

DURAN GRANADOS, José Enrique. DISEÑO TÉCNICO DEL EQUIPO DE RESPUESTA ANTE INCIDENCIAS DE SEGURIDAD INFORMÁTICAS (CSIRT) EN LA EMPRESA “CYBERSECURITY DE COLOMBIA LTDA”. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA. PAMPLONA. 2020. [Consulta: 17 de mayo de 2021].

ESET. ¿Qué es ESET SysInspector? [En linea]. [Consulta: 21 de Junio 2021].Disponible en: https://support.eset.com/es/que-es-eset-sysinspector

FIRST. Improving Security Together. [Sitio Web]. FIRST is the global Forum of Incident Response and Security. [Consulta: 17 de mayo de 2021]. Disponible en: https://www.first.org/

FITHEN, Katherine. FRASER, Barbara. CERT Incident Response and the internet. Association for Computing Machinery. COMMUNICATIONS OF THE ACM. 1994.

FORTINET. [Sitio web]. América Latina sufrió más de 41 billones de intentos de ciberataques en 2020. [consulta: 2 de mayo de 2021]. Disponible en:

https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020

GARCIA VELASQUEZ, Javier Antonio. [en línea]. Propuesta de diseño e implementación de un centro de operaciones de Seguridad (SOC) y un centro de respuesta a incidencias (CSIRT) para la universidad de Ingeniería. 2018. Informe Final de Tesis para Optar al Título de Máster en Gestión de la Seguridad de la Información. Managua. Universidad Nacional de Ingeniería. Facultad de Ciencias y Sistemas.2016. [consulta: 17 de Mayo de 2021] .Disponible en: http://ribuni.uni.edu.ni/1825/1/90248.pdf

GIUSTO, Denise B. WeliveSecurity. [Sitio web]. .Países más afectados por el Ransomware en Latinoamérica Durante 2018. [consulta: 4 de mayo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/

IBIS COMPUTER. 5 prácticas de ciberseguridad para pymes en 2021. [En linea]. [Consulta: 18 de Junio 2021].Disponible en: https://www.ibiscomputer.com/blog/128-5-practicas-de-ciberseguridad-para-pymes-en-2021

INFOSECYRITY a Softline Company. SOC. [Sitio web]. Brindamos servicios de un centro de respuesta y monitoreo de incidentes utilizando tecnologías Big Data. [consulta: 17 de mayo de 2021]. Disponible en: https://in4security.com/

JARAMILLO H, Danilo.; PALACIOS A, Jackeline. Elicitación de Requisitos de Resiliencia para Sistemas de Información basado en el modelo CERT-RMM Requeriments elicitaction of resilience for Systems Information based on the model CERT-RMM. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação). 2014. [consulta: 17 de mayo de 2021]

LEAL MENDIVELSO, Jhon Alexander. DISEÑO TÉCNICO DE LA IMPLEMENTACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMATICA CYBER SECURITY DE COLOMBIA LTDA. UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE CIENCIAS BASICAS TECNOLOGÍA E INGENIERÍA BOGOTÁ D.C. 2020. [consulta: 17 de mayo de 2021]

LOPEZ VARGAS, Juan Diego.; GAONA GARCIA, Paulo Alonso. VULNERABILIDADES SOBRE MECANISMOS DE SEGURIDAD EN PLATAFORMAS LCMS OPEN SOURCE A NIVEL DE AUTENTICACIÓN. Universidad Manuela Beltrán. Facultad de Ingeniería. Bogotá DC. 2009. [consulta: 22 de mayo de 2021]

MEJIA, Jezreel.; MUÑOZ, Mirna.; RAMIREZ, Heltton. Propuesta de Marco de Trabajo para la Protección de un CSIRT. Centro de Investigación en Matemáticas, CIMAT A.C. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação). 2016. [consulta: 22 de mayo de 2021]

MEJIA, Jezreel.; RAMIREZ, Heltton. Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. Centro de Investigación en Matemáticas CIMAT A.C. Revista ibérica de Sistemas y Tecnologías de Información. Zacatecas, México. 2016. [consulta: 22 de mayo de 2021]

MILLAN, Alejandro V.BBC NEWS. [Sitio web]. Qué tiene que ver Perú con el virus WannaCry, protagonista del ciberataque a nivel mundial. [consulta: 4 de mayo de 2021]. Disponible en: https://www.bbc.com/mundo/noticias-america-latina-39938098

MONTES, SEBASTIAN. [Sitio Web]Empresas Colombianas solo invierten 20% de presupuesto en ciberseguridad. En: La *Republica.* Septiembre de 2018. [consulta: 17 de Mayo de 2021].Disponible en: https://www.larepublica.co/internet-economy/empresas-colombianas-solo-invierten-20-de-presupuesto-en-ciberseguridad-2768645

MUÑOZ, Mirna.; RIVAS, Lizbeth. Estado actual de equipos de respuesta a incidentes de seguridad informática. Centro de Investigación en Matemáticas, CIMAT A.C. RISTI (Revista Ibérica de Sistemas e Tecnologias de Informação). 2015. [consulta: 22 de mayo de 2021]

OSORIO SIERRA, Andrés Felipe.; MATEUS HERNÁNDEZ, Milton Javier.; VARGAS MONTOYA, Héctor Fernando. "Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware," Rev. UIS Ing., vol. 19, no. 3, pp. 131-142. 2020. [consulta: 10 de Junio de 2021]

OSPINA DIAZ, Milton Ricardo.; SANABRIA RANGEL, Pedro Emilio. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad Revista Criminalidad, 62(2), 199-217.Bogota DC. 2020. [consulta: 10 de Junio de 2021]

Portafolio, Economía. [sitio web].Delitos informáticos, la otra pandemia del coronavirus [consulta: 2 de mayo de 2021]. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

Ramírez Luna, Heltton Emmanuel; Mejía Miranda, Jezreel. [Sitio Web] Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica*, núm.1, febrero, 2015. Guadalajara, México. [consulta: 17 de

Mayo de 2021].Disponible en: https://www.redalyc.org/articulo.oa?id=512251501006

REVISTA SEMANA. [En Línea].Así está Colombia en el ranking de ciberseguridad mundial Bogotá 10 de octubre de 2019. [consulta: 16 de mayo de 2021]. Disponible en: (https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118).

REVISTA SEMANA.DINERO. [En Línea]. En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos .Bogotá. 10 octubre de 2019. [consulta: 16 de Mayo de 2021].Disponible en:(https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556).

REVISTA SEMANA. [En Línea]. El 43% de las empresas colombianas no están preparadas contra los ciberataques. Bogotá. 7 de junio 2016. [consulta: 16 de Mayo de 2021].Disponible en: https://www.semana.com/pais/articulo/colombia-tuvo-perdidas-de-1-billon-por-ciberataques/224404/

SERNA PATIÑO, Alexis Mauricio.; GIRALDO RAMIREZ, Diana Patricia. A technological analysis of Colombia's cybersecurity capacity: a systemic perspective from an organizational point of view", Revista Ingeniería Solidaria, vol. 15, n. ° 2, 2019. [consulta: 10 de Junio de 2021]

SHIERKA, Isabel.MORGUS, Robert. CSIRT Basics for policy-Makers [En linea].The History,Types & Culture of Computer Security Incident Response Teams. (Mayo 2015).[Consulta el 10 de Julio de 2021].Disponible en: https://www.gppi.net/media/Skierka_et_al_2015_CSIRT_Basics_for_Policy-Makers.pdf

SRITAPAN, Vincent. STEWART, Walter.; ZHU, Jake. TAPIE ROHM JR, C. International Information Management Association (IIMA). California State University San Bernardino, USA. 2011. [consulta: 10 de Junio de 2021]

TEJO MACHADO, Nadjila.MARTINEZ BASILE, Felipe.; AMATE, Flavio.; RAMIREZ LOPEZ, Leonardo. Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. Revista Científica General José María Córdova. 2021. [consulta: 10 de Junio de 2021]

WALKER,Terrence.[En línea]. Practical management of malicious insider threat – An enterprise CSIRT perspective,Information Security Technical Report. Volume 13, Issue 4,2008,Pages 225-234.[Consulta 24 de Julio 2021].Disponible en: https://www.sciencedirect.com/science/article/pii/S136341270800054X

WeliveSecurity. [Sitio web]. Martes de retrospectiva: el gusano Morris. [consulta: 6 de

mayo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/

ZULUAGA, Diego. Ciberseguridad para la operación centralizada y distribuida de generación de energía eléctrica en ISAGEN. Universidad EAFIT. Facultad de Ingeniería y Ciencia. 2020. [consulta: 10 de Junio de 2021].

WINITOR. Evaluación inicial de malware.[En linea]. [Consulta: 21 de Junio 2021].Disponible en: https://www.winitor.com/

ANEXOS

Anexos 1.Resumen Analítica Especializado –RAE

Fecha de Realización:	29/07/2021
Programa:	ESPECIALIZACION EN SEGURIDAD INFORMATICA
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Propuesta técnica de una infraestructura lógica para las operaciones propias de un CSIRT enfocado a las pequeñas y medianas empresas en Colombia.
Autor(es):	Giraldo Martinez Leidy Vanessa
Palabras Claves:	CSIRT, CIBERSEGURIDAD, PYMES, INFRAESTRUCTURA, COLOMBIA
Descripción:	Este documento contiene el diseño de la propuesta de la infraestructura lógica que debe de tener un CSIRT aplicado a las pequeñas y medianas empresas. Su desarrollo abarca aspectos como diagnóstico de Ciberseguridad en las MYPYMES, marcos aplicados de seguridad informática en este tipo de organización. Así mismo propone un portafolio de servicios basados en servicios proactivos y reactivos mediante el uso de herramientas tecnológicas que optimicen su funcionamiento. Se contempla de igual forma un diseño de estructura organizacional, estructura física y tecnológica de este CSIRT de tal manera que sus funciones estén enfocadas al tipo de organización objetivo. Para finalizar, esta propuesta comprende una serie de pruebas de software mediante las herramientas utilizadas para ofertar los servicios reactivos y proactivos.

Fuentes bibliográficas destacadas:

- Asuntos: Legales, Judicial. [Sitio web]. Ciberdelitos subieron 37% durante el primer trimestre de 2020, en los peores meses de la crisis. [consulta: 2 de mayo de 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480
- Cámara Colombiana de Informática y Telecomunicaciones (CCIT), Tanque de Análisis y creatividad de las TIC(TicTac), Centro De Capacidades para la Ciberseguridad en Colombia (c4). [En línea]. Informe de las tendencias Cibercrimen en Colombia 2019-2020. Programa seguridad aplicada al fortalecimiento empresarial (SAFE). Octubre 29 de 2019. [consulta: el 26 de Mayo

<table>
<tr><td colspan="2">de 2021].Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf
❖ GARCIA VELASQUEZ, Javier Antonio. [en línea]. Propuesta de diseño e implementación de un centro de operaciones de Seguridad (SOC) y un centro de respuesta a incidencias (CSIRT) para la universidad de Ingeniería. 2018. Informe Final de Tesis para Optar al Título de Máster en Gestión de la Seguridad de la Información. Managua. Universidad Nacional de Ingeniería. Facultad de Ciencias y Sistemas.2016. [consulta: 17 de Mayo de 2021] .Disponible en: http://ribuni.uni.edu.ni/1825/1/90248.pdf
❖ JARAMILLO H, Danilo.; PALACIOS A, Jackeline. Elicitación de Requisitos de Resiliencia para Sistemas de Información basado en el modelo CERT-RMM Requeriments elicitaction of resilience for Systems Information based on the model CERT-RMM. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação). 2014. [consulta: 17 de mayo de 2021]
❖ JARAMILLO H, Danilo.; PALACIOS A, Jackeline. Elicitación de Requisitos de Resiliencia para Sistemas de Información basado en el modelo CERT-RMM Requeriments elicitaction of resilience for Systems Information based on the model CERT-RMM. CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Información). 2014. [consulta: 17 de mayo de 2021]</td></tr>
<tr><td>Contenido del documento:</td><td>En la actualidad el crecimiento del uso de las Tecnologías de la Información y las telecomunicaciones ha empezado a estar presente en prácticamente todos los ámbitos de la sociedad; lo que ha desencadenado un uso masivo del ciberespacio en donde al día de hoy es que se realizan la mayoría de los procesos de la internet, Incluyendo los conflictos y ataques que empiezan a vulnerar no solo la seguridad de las organizaciones sino que incluso se han presentado ataques que han puesto en jaque la seguridad nacional de un país.
Según la firma Deloitte, en Colombia las organizaciones no se están poniendo al frente de la situación, sus estructuras no están preparadas para ataques de seguridad informática.
Esto deja entrever las empresas no se están tomando en serio todo el tema de seguridad informática, tampoco están centrando recursos económicos para empezar a abordar ese tema, Deloitte estimo que el 50% de todas las organizaciones solo destinan entre 1% y el 5% del presupuesto del área de TI para proteger todo el tema de Seguridad de la Información.

FORMULACIÓN DEL PROBLEMA</td></tr>
</table>

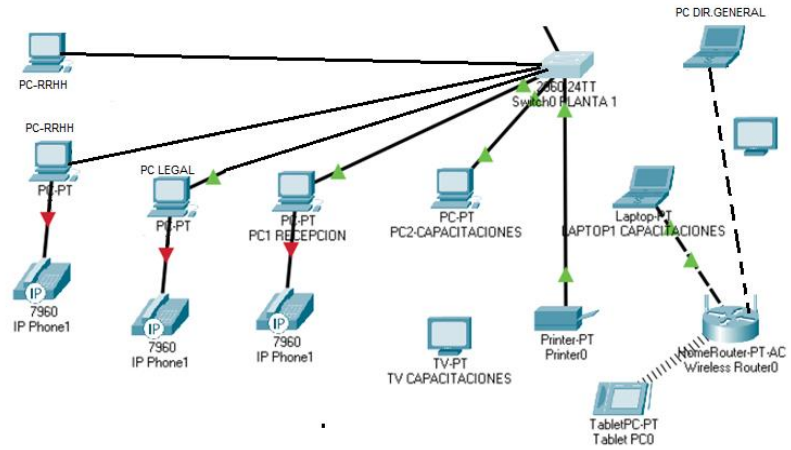
	¿Cuáles son los requerimientos de software y hardware necesarios para diseñar una propuesta de infraestructura lógica para las operaciones propias del centro de respuesta a incidentes de Seguridad Informática? **Objetivo 1: EXAMINAR EL PANORAMA ACTUAL DE LA CIBERSEGURIDAD EN PEQUEÑAS Y MEDIANAS EMPRESAS EN COLOMBIA Y LOS ATAQUES QUE HAN CAUSADO MAS IMPACTO EN LA OPERATIVIDAD DE LAS MISMAS.** En la actualidad se ha venido incrementando los delitos informáticos en cada uno de los sectores de la economía no solo de Colombia sino a nivel mundial. Este tipo de prácticas generan un gran impacto y afectación para aquellos que son víctimas de estos procesos. En Colombia según el estudio de tendencias del cibercrimen generado por el programa Seguridad aplicada al Fortalecimiento Empresarial del Tanque de Análisis y creatividad de las TIC (TicTac). Se presentan las diferentes cifras y técnicas de los ciberdelitos efectuados en el año 2019 y a su vez planea las posibles técnicas a las cuales se enfrentarían las empresas colombianas para el año 2020. En cuanto a los delitos más comunes según el estudio se plantean los siguientes: ❖ Hurto por medio informático. ❖ Violación de datos personales. ❖ Acceso abusivo a sistemas de información. **Recomendaciones Kaspersky Latinoamérica:** ❖ Identificación de los Riesgos. ❖ Mantener Actualizados los equipos de la organización. ❖ Realizar Copias de Seguridad periódicamente. ❖ Utilizar soluciones de Seguridad informática para asegurar los activos de la organización. **Marcos de Ciberseguridad aplicados a las pequenas y medianas empresas.**

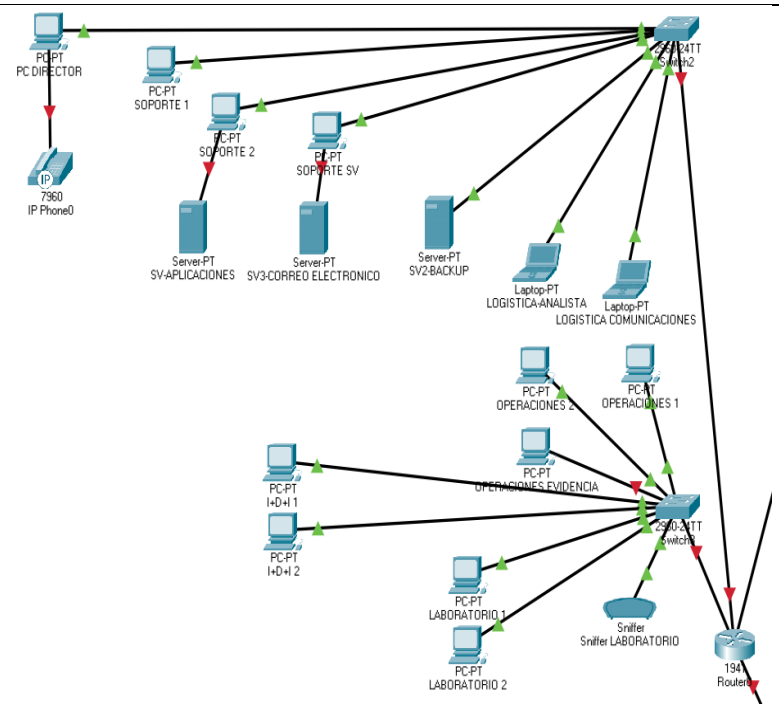
	❖ **ISO 27001:** Es una norma transversal, se adapta a cualquier tipo de organización y permite seleccionar los tipos de controles que se aplicaran. Planificar-Hacer-Verificar-Actuar ❖ **Marco CSF:** Normas y directrices de seguridad informática. Encuentra los sectores críticos de la estructura de la organización y prioriza las actividades en estos. ❖ **Cobit:** Construcción de políticas de seguridad, generación de buenas prácticas de control y herramientas tecnológicas. **Objetivo 2: ESTRUCTURAR LA INFORMACION RELACIONADA CON HERRAMIENTAS DE HARDWARE Y SOFTWARE QUE PERMITAN DESARROLLAR LAS ACTIVIDADES DEL CSIRT TENIENDO PRESENTE EL CATALOGO DE SERVICIOS.** Los servicios que se prestaran serán tanto reactivos como proactivos, es decir el Equipo de respuesta a incidentes informáticos no solo se centrara en ofrecer su portafolio de servicios basados en solucionar los problemas que presentan las organizaciones en un momento determinado, también prestara dentro de su portafolio procesos que permitan generar alertas, capacitaciones y demás ítems que sirvan como base en una organización para solucionar incidentes que no requieren ser escalados hasta este tipo de Equipos especializados. **SERVICIOS PROACTIVOS** ❖ **Análisis y monitoreo infraestructura tecnológica:** Este equipo cuenta dentro de su estructura organizacional con funcionarios que realizan un monitoreo remoto de las organizaciones para de esta forma determinar malas prácticas o maquinas potencialmente riesgosas para una empresa. Ellos serán los encargados de realizar un análisis de vulnerabilidades web de los diferentes Aplicativos y portales web que posee la organización para determinar posibles vulnerabilidades y proceder a subsanarlas para disminuir los riesgos. **Software y Hardware.** ❖ Nexpose ❖ Process Explorer ❖ IPS

	❖ **Auditorias de Seguridad Informática:** El objetivo de brindar este servicio a las pequeñas y medianas empresas es poder realizar una auditoria completa de toda la infraestructura tecnológica determinando no solo los equipos con un riesgo superior sino estableciendo planes de mejora que le permitan a la organización mitigar el impacto y la probabilidad de que un riesgo detectado pueda generarse. **Software y Hardware.** ❖ Magerit. ❖ Portátil Lenovo. ❖ **Desarrollo de herramientas de Seguridad:** Este servicio es fundamental para el CSIRT ya que dentro de su estructura organizacional cuenta con un área para la investigación y el desarrollo, así como para realizar laboratorios que les permitan determinar y crear herramientas que puedan solucionar incidentes de seguridad informática que no requieren un proceso tan exhausto en cuanto a su solución. **Software y Hardware.** ❖ VirtualBox ❖ VisualStudio ❖ **Educación, entrenamiento y concienciación sobre Seguridad Informática:** Este servicio que será ofertado en el CSIRT para las pequeñas y medianas empresas consiste principalmente en la creación de planes educativos y de formación en aspectos esenciales de la Seguridad Informática. **Software y Hardware.** ❖ Cisco Webex Room ❖ Cisco Webex Share **SERVICIOS REACTIVOS**

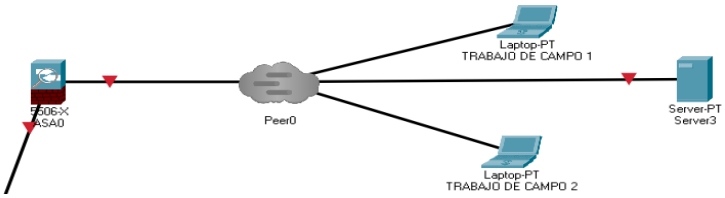
	❖ **Alertas y Avisos:** Dentro de este servicio se tiene como tal las publicaciones de alertas y avisos que corresponden a incidentes de Seguridad Informática presentes y detectados por las grandes compañías de Ciberseguridad en el mundo. **Software y Hardware.** ❖ OWASP Top Ten. ❖ CSIRTs by Country-Interactive Map ❖ Cisco Secure Email ❖ **Gestión de Incidentes:** Este es sin lugar a dudas el servicio más importante dentro de un CSIRT, de hecho, es un servicio indispensable para este tipo de organizaciones. Dentro de este se contempla ejecutar todo lo que corresponde a la gestión y manejo de un Incidente de Seguridad Informática, desde la recepción del incidente hasta la entrega del informe final a la organización atacada y las recomendaciones finales. **Software y Hardware.** ❖ Clasificación BHP Gnup ❖ Request Tracker for incident Response ❖ CVE Search ❖ Virus Total. ❖ Firewall Cisco ❖ Backup ❖ Servidor Cisco **Objetivo 3: ESTABLECER LOS REQUERIMIENTOS NECESARIOS EN RELACION A LA TECNOLOGIA DE HARDWARE Y SOFTWARE PARA EL DISEÑO DE LA INFRAESTRUCTURA LOGICA QUE PERMITAN DESARROLLAR LAS ACTIVIDADES DEL CSIRT** **DIRECTOR GENERAL:** El CSIRT contara con un director general que será el encargado de engranar toda el área administrativa como el área operativa. Este director será quien tome las decisiones finales relevantes en la compañía, cuenta con un subalterno que será el director operativo, de esta forma recibirá las sugerencias de este y tomara las decisiones que considera son las indicadas no solo

	para mejorar su efectividad como CSIRT sino también para lograr los objetivos organizacionales de la empresa. **RECEPCION:** En esta sección se encontrará la recepción del centro de respuesta a incidentes informáticos y también se contará con la sala de capacitaciones para generar planes educativos a los diferentes usuarios que hagan parte del CSIRT. En esta área se cuenta con un profesional que dará una revisión inicial al incidente y podrá generar un plan de acción para posteriormente pasarlo al equipo de operaciones quienes serán los encargados de dar respuesta a la problemática. ❖ **Recepción.** ❖ **Capacitación** ❖ **Revisión Inicial** **RRHH/LEGAL:** En esta sección se centraran todas las funciones de los recursos humanos y los procesos legales de la empresa. Cuenta con una oficina de jurídica y otra oficina de talento humano. **LOGISTICA** Dentro de esta sección se encuentran aspectos fundamentales para el funcionamiento del CSIRT. Esto principalmente porque es donde se encuentra la información almacenada de todo el equipo y de los clientes que alojan la información allí. También se tienen profesionales que apoyaran todo el tema de soporte y todo el tema logístico de tal manera que puedan generar un puente y puedan dar un manejo adecuado a los clientes de las pequeñas y medianas empresas. ❖ **Coordinación.** ❖ **Soporte TI** ❖ **Centro de datos** ❖ **Área logística.** **OPERACIONES** Desde esta sección se encuentra la parte más operativa del CSIRT desde todo el manejo del incidente hasta las

	investigaciones y desarrollo de nuevas herramientas para mejorar el funcionamiento como tal del equipo. ❖ **Operaciones CSIRT** ❖ **I+D+I** ❖ **Laboratorios.** **TRABAJO DE CAMPO** Quienes desempeñen esta función serán principalmente un Ingeniero de Sistemas y un Técnico en Sistemas que siempre estarán en las empresas de los clientes capturando toda la información necesaria para realizar la Gestión del Incidente Informático correctamente. El CSIRT para las pequeñas y medianas empresas contara con una sección que se ubicara siempre en las empresas donde se presentó el incidente. Desde allí los profesionales se encargarán principalmente de recolectar la evidencia digital y de preservar esta lo más original posible para de esta forma no solo dar respuesta al incidente informático sino también determinar la forma de ataque y posibles responsables detrás del mismo. ❖ **Trabajo remoto de Campo** ❖ **Recolección evidencia digital.** **Estructura Tecnológica CSIRT** **Planta 1:**  **Planta 2:**



Área Externa:



Objetivo 4: DESARROLLAR A PARTIR DE LABORATORIOS CONTROLADOS Y A REALIZACION DE PRUEBAS DE SOFTWARE, LA DEMOSTRACION DE LAS HERRAMIENTAS QUE PUEDEN UTILIZARSE PARA EJECUCION DE LAS TAREAS PROPIAS DEL CSIRT.

- **FTK Imager:** Dentro de un CSIRT es fundamental todo el proceso de recolección de evidencia ante un incidente de Seguridad Informática dentro de una pequeña o mediana empresa. Para esto lo ideal es iniciar con una copia

	completa de la unidad que fue atacada y realizar una revisión de qué fue lo que paso, que tipo de ataque se presentó y encontrar a un posible responsable de este. Es por este motivo que se hace uso de FTK Imager para generar una imagen de la unidad atacada y posteriormente ser llevada al centro de operaciones para iniciar con todo el proceso de análisis forense y solución de incidentes. ❖ **SYSINSPECTOR:** El CSIRT diseñado para las pequeñas y medianas empresas contara con un servicio proactivo que consiste principalmente en analizar y monitorear la infraestructura tecnológica de las organizaciones para detectar posibles amenazas o puertas traseras que estén siendo blanco de ciberdelincuentes para planear un ataque informático. Las principales funciones de SYSINSPECTOR son: ❖ Detectar procesos y servicios activos en el sistema señalando con un color determinado el nivel de riesgo que representa para el equipo. ❖ Detectar archivos sospechosos o que no contengan firma en el sistema. ❖ Realizar un escaneo del software instalado para posteriormente detectar inconvenientes con este mismo. ❖ Detecta los controladores que pueden llegar a estar obsoletos o que están generando un problema de incompatibilidad con el sistema. ❖ Detecta Sistemas operativos sin licencias, sin actualizaciones e incluso sin parches de seguridad instalados. ❖ Revisa las entradas de registro del sistema y las categoriza dependiendo el riesgo, las que se encuentran rotas las señala con rojo porque representan un riesgo para la organización. ❖ **PESTUDIO:** Esta herramienta es ideal para realizar las funciones un CSIRT, principalmente porque es fácil de utilizar, no consume recursos y genera información acertada de diferentes archivos ejecutables en Windows. Realiza un análisis del archivo .exe y los compara con diferentes librerías de antivirus con el fin de recopilar la reputación de este archivo en las bases de datos y poder

	determinar la procedencia correcto funcionamiento del ejecutable.
Marco Metodológico:	**Tipo de investigación:** El tipo de investigación utilizado en este proyecto aplicado es el descriptivo, esto principalmente porque se especificarán aspectos fundamentales de la estructura lógica de un CSIRT para las pequeñas y medianas empresas. **Enfoque de la Investigación**: cualitativo, principalmente porque la investigación está orientada a realizar una revisión bibliográfica de todo el fenómeno de los ataques informáticos e incidentes de seguridad de la información en las pequeñas y medianas empresas **Fuentes Primarias:** Las fuentes primarias utilizadas en esta investigación serán principalmente revistas científicas, Tesis, Informes de seguridad de la información y diarios o revistas que indiquen información importante para el desarrollo del proyecto aplicado. **Técnicas de recolección y análisis de información:** Las técnicas de recolección y análisis de la información estarán fundamentadas principalmente en la observación ya que a partir de la documentación adquirida mediante las fuentes primarias se permite dar una idea inicial de la Seguridad Informática en las pequeñas y medianas empresas.
Conceptos adquiridos :	❖ Para crear la estructura lógica de un CSIRT que actué dentro del sector de las Pequeñas y medianas empresas es importante que se realice una investigación de campo acerca de cómo se encuentran las tendencias de Ciberseguridad en este sector de la economía, de esta forma se podrán evidenciar los ataques más persistentes, los ataques más críticos e incluso los ataques que suelen ser más efectivos. ❖ Dentro de una propuesta de infraestructura lógica para un CSIRT que preste sus servicios para las pequeñas y medianas empresas debe traer también consigo una propuesta de la estructura organizacional de este tipo de equipos. Este proceso es fundamental ya que mediante esta estructura se definirán los profesionales que se requieren para funcionar como tal en base a los servicios que se prestaran. De igual forma al diseñar la estructura organizacional, se debe tener en cuenta las responsabilidades de cada uno de estos profesionales y el área en la que actuara para así poder observar las áreas

	que cuentan con mayor apoyo de talento humano y cuáles de estas áreas deben ser reforzadas con nuevos profesionales.
Conclusiones:	❖ En Colombia la incidencia de delitos informáticos en las Pequeñas y Medianas empresas ha venido en notable crecimiento, entre el 2019 y el 2020 el incremento de estos delitos fue del 54%. De esta forma las empresas se han visto afectadas por delitos como el hurto informático, la violación a los datos personales y el acceso abusivo a sistemas de información entre otros. ❖ Para que un CSIRT sea efectivo, este debe contar con software que les permitan partir desde el análisis que harán los usuarios finales constantemente a sus equipos para posteriormente mediante un análisis desde los profesionales del CSIRT detectar anomalías en el comportamiento del activo tecnológico. Es fundamental adquirir o desarrollar herramientas que optimicen el proceso de restaurar la información y los equipos a la versión estable antes del incidente de seguridad informática, todo esto es fundamental para aumentar la confianza en los clientes y poder captar diferentes empresas que requieran no solo de la solución de los incidentes sino también la formación de sus profesionales para adoptar buenas prácticas de seguridad informática en la organización. ❖ De igual manera un CSIRT adaptado a las pequeñas y medianas empresas debe contar dentro de su personal técnico con profesionales que no solo se encarguen de dar respuesta a los incidentes informáticos sino que también estén en la capacidad de investigar y desarrollar nuevas herramientas que optimicen todo el proceso y que les sirvan a las empresas del mercado como alternativas para evitar ciberataques, así mismo se requiere contar con profesionales que puedan manejar las relaciones públicas de la organización de tal manera que estén constantemente retroalimentando los diferentes canales de comunicación con el fin de captar clientes constantemente