DISEÑO PARA LA CONSTRUCCIÓN DE UN CSIRT COMO HERRAMIENTA DE GESTIÓN DE INCIDENTES Y DETECCIÓN DE VULNERABILIDADES PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

ESNEYDER SANCHEZ MAHECHA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

DISEÑO PARA LA CONSTRUCCIÓN DE UN CSIRT COMO HERRAMIENTA DE GESTIÓN DE INCIDENTES Y DETECCIÓN DE VULNERABILIDADES PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

ESNEYDER SANCHEZ MAHECHA

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

Esneyder Sánchez Mahecha

Yolima Mercado Palencia
Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., Fecha sustentación

DEDICATORIA

“No es el conocimiento, sino el acto de aprendizaje; y no la posesión, sino el acto de llegar a ella, lo que concede el mayor disfrute.”

CARL FRIEDRICH GAUSS

AGRADECIMIENTOS

Agradecido con mi madre que siempre ha estado cuando la he necesitado, en los buenos y en los malos momentos el logro es de ella, también agradecer a todas las personas que me han animado en este camino, soportando y comprendiendo que este camino no es fácil pero necesario para buscar un nuevo horizonte en ámbitos profesionales con la realización que requiere dicho proceso.

Gracias a todos

CONTENIDO

pág.

TABLAS

LISTA DE FIGURAS

GLOSARIO

CERT: Es una marca que está registrada como centro de coordinación dl Software Engineerind Institute de la universidad Cramegie Mellón, el cual fue el primer grupo que fue creado para dar respuesta a incidentes.

CODIGO DE CONDUCTA: Se establece como el reglamento que legaliza la conducta de los ingenieros y profesionales afines, su violación es sancionada mediante procedimientos establecidos.

CSIRT: Se identifica como una forma de describir al equipo de respuesta a incidentes, su función que es idéntica a un CERT**.**

DARPA: Agencia de defensa que es responsable de dar fondos para desarrollar diversas tecnologías que han tenido un alto impacto a nivel global.

FUERZA BRUTA: Llamamos así al método de ensayo y error que se realiza con diversos softwares, utilizando un diccionario que está cargado de un gran número de contraseñas que son comúnmente usadas o aparecen por defecto en sus fabricantes, con el objetico de descifrar la clave de la víctima.

INGENIERIA SOCIAL: Se denomina así a la práctica que implica obtener información confidencial a través de cierta manipulación de usuarios, por lo general se obtienen claves de acceso permisos sobre sistemas que hacen daño al organismo comprometido.

INICIDENTE DE SEGURIDAD: Se considera cualquier evento adverso que este confirmado o sea sospechoso, relacionado con los sistemas de seguridad o informáticos.

MALETIN FORENCE: Es el conjunto de elementos que cumplen una función específica para el levantamiento de información de los incidentes informáticos.

PROXY: Funciona como un intermediario entre los requerimientos que hace el cliente y un servidor de destino, todas las peticiones de conexión de los usuarios de la red deben pasar a través de este.

PRUEBAS DE PENETRACION: Se denomina al servicio el cual realiza explotación de vulnerabilidades para penetrar las defensas de un sistema, con el fin de capturar información sensible para los usuarios.

SERVICIO REACTIVO: Es considerado como un enfoque a la reparación de incidentes es decir se espera que se manifieste un problema para posteriormente dedicar unos recursos para solventarlo.

SERVICION PORACTIVO: Es considerado como el enfoque a la predicción de problemas, se toma como insumo los inconvenientes presentados así mismo se toman medidas para que no se presenten de nuevo, de igual forma se realizan ciertos tipos de auditorías que buscan predecir las fallas que se pueden presentar.

RESUMEN

Para la implementación del proyecto aplicado como se desea se va a tomar el escenario dos (Enfoque técnico-Estratégico), donde a través de una emulación se proyectará la integración de un CSIRT, en la compañía llamada Cibersecurity de Colombia LTDA la cual es una empresa colombiana que presta servicios de seguridad para la protección de la información, cuyo propósito es consolidarse como un centro de respuesta a incidentes cibernéticos en el ámbito CSIRT.

Dentro de sus objetivos se pretende desarrollaran funciones que brinden una protección activa y proactiva de la organización, resaltando la importancia de conocer los objetivos de la organización ya que estos van arraigados a los negocios, desarrollando esa educación y entrenamiento necesaria en las áreas de TI para la prevención de intrusión en los sistemas más importantes de la compañía.

Mediante el método científico se va a generar una recolección de información para posteriormente aplicarlo a entornos controlados, para analizar los diferentes contextos dados y así mismo obtener la información necesaria para aplicar los planes estratégicos.

ABSTRACT

For the implementation of the project applied as desired, scenario two will be taken (Technical-Strategic Approach), where through an emulation the integration of a CSIRT will be projected, in the company called Cibersecurity de Colombia LTDA which is a company Colombian company that provides security services for the protection of information, whose purpose is to consolidate itself as a center for responding to cyber incidents in the CSIRT field.

Within its objectives, it is intended to develop functions that provide active and proactive protection of the organization, highlighting the importance of knowing the objectives of the organization and that these are rooted in business, developing that education and training necessary in the areas of IT to intrusion prevention in the most important systems of the company.

Through the scientific method, a collection of information will be generated to later apply it to controlled environments, to analyze the different given contexts and also obtain the necessary information to apply the strategic plans.

INTRODUCCIÓN

Los equipos para la respuesta a incidentes de seguridad más conocidos como (CSIRT) buscan que las actividades perjudiciales frente a su seguridad tengan el menor impacto posible, por ello en sus políticas de mejoramiento es bueno crear un CSIRT en los diferentes ámbitos, generando los criterios y aportaciones para su creación, trabajando en conjunto con una misión ,visión ,alcance ,servicios ,tiempos y aspectos legales, tomando en consideración también los recursos técnicos , infraestructura y recursos humanos que son necesarios para establecer un CSIRT.

Teniendo en cuenta que la tecnología moderna y la constante conexión a internet por parte de la sociedad moderna, ha logrado permitir que el crecimiento de los servicios ofertados en la red sea muy alto, con ello los criminales cibernéticos están descubriendo nuevas formas cada vez más complejas para aprovechar las redes para sus propósitos delictivos.

Se plantea un escenario donde se implementan las herramientas necesarias para lograr mitigar las vulnerabilidades que pueden ser encontradas, así como prevenir las que pueden llegar a suceder en la organización, con una formulación de objetivos necesarios para llegar al objetivo principal que pretende el documento.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Las redes de comunicación y los sistemas de información se constituyen como un factor esencial en el desarrollo de la economía en entornos globales por ello la informática y las redes se han convertido en servicios públicos ubicuos, del mismo modo que servicios como la electricidad y agua corriente.

La seguridad de las redes de comunicación, los sistemas de información y en particular su disponibilidad, son elementos que afectan cada vez más a nuestra sociedad puesto que los sistemas de información más influyentes pueden enfrentarse a problemas debido a su complejidad o diversidad de los entornos de información, se producirán en casos graves ataques a la infraestructura física que prestan los servicios vitales para el bienestar de los ciudadanos del común.

Desde hace años diversos grupos dedicados a la seguridad de la información como los CERT/CSIRT[1], los equipos de detección y abusos de seguridad WARP colaboran para que el internet sea más seguro.

Un CSIRT es un equipo de expertos en seguridad de las telecomunicaciones cuya principal tarea es responder a los incidentes, el CSIRT presta servicios necesarios para ocuparse de los diferentes incidentes y ayuda a los diferentes clientes del grupo al que atiendan para recuperarse después de sufrir un incidente.

Para mitigar los riesgos y minimizar el número de inconvenientes, la mayor parte de los CSIRT ofrecen servicios preventivos y educativos, en donde se publican avisos

[1] Good Practice Guide for Management. Technical report, ENISA, 2010.

sobre el tipo de vulnerabilidades del software y el hardware en uso, se informa a los usuarios los programas maliciosos y virus que pueden aprovechar las brechas de seguridad, de modo que los diferente clientes pueden corregir y actualizar la lista de los posibles servicios.[2]

Aunque una de sus funciones adicionales es compartir la información obtenida y relacionada con incidentes se seguridad con otro grupo de CSIRT, con fines de difusión y educación, este tipo de actividad es muy conocida en diferentes áreas del desarrollo de software ya que su misma comunidad se trasmite los problemas y posibles soluciones para disminuir sus riesgos de ataques.

Las actividades de los CSIRT pueden llegar a ser vistas como servicios que se ofrecen a organizaciones desde una perspectiva de servicios reactivos y proactivos, o bien pueden ser contratados tercerizando cuando no se posee infraestructura o estudios necesarios para que la organización lo realice, los servicios reactivos se ejecutan cuando se genera un evento de seguridad indeseado e inesperado que es detectado como una solicitud de algún integrante de la organización, que observo una anomalía en la infraestructura tecnológica. Este tipo de actividades son una componente principal de los CSIRT y están estrechamente anclados a los planes de gestión de seguridad.

Mientras los servicios proactivos están diseñados para obtener información que contribuya a la protección de la infraestructura tecnológica, y a mejorar los procesos de seguridad con lo cual su objetivo principal es evitar que se presenten ataques o incidentes. Dentro de otras actividades también podemos encontrar que se deben incluir auditorias y evaluaciones en la configuración y mantenimiento de las herramientas de seguridad.

---

[2] Barbara Guttman and Edward Roback. An introduction to computer security: the NIST handbook. DIANE Publishing, 1995

La respuesta a los incidentes se considera una tarea compleja para muchas organizaciones, esta requiere de la implementación de un conjunto de actividades y medidas para lograr atender y dar solución a los eventos inesperados que van afectar a los activos de la organización, además de la efectiva planeación y generación de los documentos necesarios para capacitar al recurso humano, y de las herramientas necesarias para llevar acabo las actividades, por ello es necesario contar con una guía adecuada para la inmutación de un CSIRT y minimizar el impacto, garantizando la seguridad de TI en las organizaciones.[3]

[3] A.P. Jurg, E.P. Stals, and D.P Stikvoort. A Trusted CSIRT Introducer in Europe. Technical report, M&I/Stelvio, 2000.

1.2 FORMULACIÓN DEL PROBLEMA

En la actualidad y debido al crecimientos y la sofisticación de las amenazas a nivel informático se plantea un nuevo panorama donde debemos responder con rapidez a este tipo de incidentes, por ello la importancia de crear un CSIRT (Computer Security Incident Response Team), debemos tener en cuenta que la materialización de incidentes debe ser mínima, reduciendo las consecuencias y estableciendo actividades que disminuyen el impacto global sobre la organización, por ello debemos analizar.

¿Cómo diseñar un modelo para la gestión de un CSIRT como herramienta de gestión y prevención de incidentes?

2 JUSTIFICACIÓN

Los centros para la respuesta de incidentes de seguridad de la información hacen parte importante de las organizaciones por ello se debe establecer una seguridad especifica en la entidad, ya sea un gobierno o un país, lamentablemente no se encuentran muchos modelos o marcos de trabajo que permitan el establecimiento de la seguridad en un CSIRT, en el cual se describan los materiales necesarios tecnologías a utilizar y buenas prácticas que se deben ejecutar, este marco de trabajo brinda una ayuda para la organización Cibersecurity de Colombia LTDA.

El principal objetivo de establecer un grupo de respuesta a incidentes informativos, es contar con un punto donde se realiza un contacto dentro de las organizaciones para la recepción de las notificaciones de seguridad, manejo de incidentes y análisis de las vulnerabilidades de los recursos y servicios que se están prestando, los incidentes de seguridad que no son atendidos a tiempo pueden provocar graves efectos en los sistemas de información, por tal motivo es importante el diseño de una metodología que permitirá ,con eficacia y eficiencia establecer las herramientas necesarias para identificar las vulnerabilidades en la infraestructura tecnológica, y así mitigar el impacto final presentado sobre los activos de información ,aplicando los procedimiento reactivos y activos.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar una propuesta para la construcción de un CSIRT como herramienta de gestión de incidentes y detección de vulnerabilidades para la empresa Cibersecurity de Colombia LTDA.

3.1.1 OBJETIVOS ESPECÍFICOS

- Identificar los procesos que involucra un CSIRT como herramienta de gestión de incidentes en Cibersecurity de Colombia LTDA.

- Determinar las herramientas de software requeridos para la construcción de un CSIRT.

- Construir la arquitectura del laboratorio controlado y virtualizado del CSIRT para Cibersecurity de Colombia LTDA.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

la seguridad de la información está arraigada a las medidas provisorias que podemos llevar a cabo para defender y proteger la información bajo la disponibilidad e integridad, la información es presentada en diferentes formatos como lo pueden ser físicos y electrónicos, por ello las organizaciones deberían adoptar y crear metodologías que permitan resguardar los archivos y registros de estos medios, también deberían mantener el funcionamiento de la infraestructura tecnología de la compañía.

Se define la seguridad de la información como la defensa de los datos, para que nos sean modificados, o que sean destruidos de forma accidental o intencional ante la capacidad que poseen de operarla. Entonces la seguridad de la información se encarga de proteger los datos para que estén disponibles en los diferentes sistemas, pero protegiéndola de accesos no autorizados, también la seguridad de la información resguardará los datos que están disponibles en los sistemas de información y a los que solo tendrán acceso usuarios autorizados.

En la actualidad las tecnologías van avanzando a un ritmo muy acelerado dando soluciones globales a diversos problemas, y por ende también han existido amenazas informáticas que tiene como finalidad llegar a robar información personal, realizar ataques como de denegación de servicio, realizar fraudes con diversas tarjetas de crédito o también la llamada ingeniería social, en muchos de los estudios que realizan las compañías aparece con más detalle el historial de ataques que se pueden presentar.

Esto conlleva a que las organizaciones enfoquen parte de su trabajo al análisis de la seguridad de la información, y percibir que mecanismos se pueden utilizar para

disminuir o llegar a desaparecer el riesgo del robo de información como , firewalls herramientas antivirus y antispam ,una de las cuales hacen parte del diseño de seguridad donde integran las políticas ,los estándares, las normas ,y los modelos de gestión de tecnología y operaciones de la seguridad, por ello se entiende que las organizaciones poseen mecanismos de protección que pueden fallar, es necesario contar con procesos estructurados y personal especializado que pueda manejar los incidentes de seguridad de la información, en el menor tiempo posible.

4.1.1 Ataques informativos. Los ataques informáticos consisten en el beneficio de alguna debilidad o falla en el software o en el hardware, o lo más común que son fallas en la manipulación de los diversos programas por personas sin experiencia o falta de capacitación, al fin de obtener un beneficio económico, generando un fallo y efecto negativo en el sistema, repercutiendo directamente en los servicios y activos de la compañía. Para poder minimizar el ataque informático ,existen procedimientos y planes de mejora los cuales facilitan la lucha contra las actividades que ponen en riesgo la información, debemos tener en cuento que la educación es un componente importante ,al comprender cuáles son sus riesgos más comunes y asociados según su categorización, podemos comprender de qué manera se aborda al sistema informático ayudando a identificar los huecos de seguridad, para luego desplegar un sistema de estrategias que lo mitiguen hasta porcentajes aceptables o limites casi nulos.

4.1.2 CSIRT. Lo definimos como una organización que se responsabiliza de la recepción, e identificación para poder dar una respuesta a los incidentes de seguridad de la información, uno de los objetivos primordiales es desarrollar infraestructura y capacidades tecnológicas, y prevenir este tipo de incidentes.

4.1.3 Beneficios. Uno de los beneficios a destacar con un CSIRT será la capacidad para manejar una rápida respuesta que permitirá detener un incidente de seguridad informática, así como usar una buena práctica para recuperar el daño causado por el ataque. La comunicación que posea el CSIRT con las demás dependencias de la compañía puede facilitar el acceso compartido de los recursos y estrategias que permiten generar alertas tempranas, sobre problemas potenciales haciendo que sea muy eficiente el actuar.[4]

A través del tiempo los CSIRT han evolucionado de ser una organización que proveen respuestas a, ser compañías que trabajen proactivamente en la defensa y protección de los activos críticos y de la comunidad en general, este tipo de trabajo proactivo lo basamos en la actividad de concientización y servicios de educación, con el apoyo en el diseño de políticas de la seguridad informática y coordinación de seminarios e intercambio de información.

4.2 MARCO CONCEPTUAL

Dentro del proyecto se estipulan estándares para el cumplimento del nivel de servicio, mejor llamados en el ámbito profesional como ANS, donde se especificarán sus principales características y según el tipo de contrato se impondrán una serie de cláusulas para el cumplimiento de estas.

En el ámbito del Hardware, software y dependiendo de la compañía se diseñarán y se revisara la documentación concerniente al copyright, para la utilización de licencias free ya que nos basamos en pruebas de nivel local, pero respetando el licenciamiento de las aplicaciones que utilizaremos.

[4] Carpentier, J. F. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. Barcelona, España: Ediciones ENI.

4.2.1 Ventajas de tener un CSIRT: Se dispone de un equipo dedicado a la seguridad y ayuda a la organización para mitigar y evitar todo tipo de incidentes desde graves a mínimos y lograr proteger el patrimonio, entre otras posibles ventajas encontramos las siguientes:

- Se dispone de una coordinación organizada y centralizada para todo lo relacionado con las TI.
- Reaccionar a los incidentes de la TI de una manera ágil y eficiente, manejando el sistema de una forma centralizada.
- Tener a la mano los conocimientos técnicos necesarios para apoyar a los usuarios y asistirlos en recuperarse rápidamente.
- Se tratan las cuestiones jurídicas de una manera adecuada con los manuales correspondientes y se protegen en caso de plagio.
- Realizar un seguimiento de los procesos adecuados de Ti complementando con metodologías que mantienen actualizadas las políticas.[5]

4.2.2 Descripción de los diferentes tipos de CSIRT: Es muy importante tener en cuenta que cuando se pone en marcha un CSIRT, como con cualquier otro negocio debemos formarnos una idea clara de quienes formaran el grupo de clientes y a que tipo se enfocaran los servicios que se prestaran, por ellos a continuación se describen los diferentes clientes:

4.2.2.1 CSIRT del sector académico: El cual prestan servicios a centros académicos y educativos, descritos como universidades o centros de investigación y respectivamente a sus campus virtuales.

[5] Santos, J. C. Seguridad y alta disponibilidad. Bogotá, Colombia (2014).: Ra-ma Editorial.

4.2.2.2 CSIRT del sector CIP/CIIP: Se centran en la protección de la información (CIP) y de las infraestructuras vitales (CIIP), por lo general este tipo de CIRT especializados colaboran estrechamente con un departamento público de protección e infraestructura, este tipo de CSIRT abarcan los sectores vitales del país y buscan proteger a los ciudadanos.

4.2.2.3 CSIRT del sector público: Es tipo de equipos dan respuesta a incidentes cibernéticos sobre las entidades del sector público, un claro ejemplo de este sistema es el enfoque que tiene Asobancaria[6], donde a través de la investigación y colaboración de diferentes entidades públicas se pueden anticipar y mitigar los riesgos que se derivan de las amenazas cibernéticas.

4.2.2.4 CSIRT internos: Este tipo de CSIRT únicamente prestan servicios a la organización a la cual pertenecen, lo que describe mejor este tipo es el funcionamiento dentro de organizaciones de telecomunicaciones y bancos, por regla general estos CSIRT no poseen sitios web púbicos.

4.2.2.5 CSIRT comercial: Como su nombre lo expone se prestan servicios comerciales a sus clientes, de manera más clara en este tipo de caso se exponen a proveedor tres como internet, principalmente se enfoca a servicios con abuso de clientes finales.

4.2.2.6 CSIRT del sector militar: Se prestan servicios a entidades estrechamente relacionadas con organizaciones militares con fines de defensa en sus TI.

[6] Asobancaria (2021) https://www.asobancaria.com/csirt/

4.2.3 Servicios para un CSIRT: Dentro de los servicios para un CSIRT se debe garantizar que estén trabajando en conjunto con la necesidad de la compañía, por ello los clasificamos en las siguientes 4 formas.

- **Centro de operaciones de seguridad**: Lugar en el cual se realiza un análisis de los eventos informáticos presentados, para posteriormente verificar si es positivo o negativo.
- **Un grupo de respuesta a incidentes informáticos**: Se analiza cómo se puede hacer frente a los eventos presentados.
- **Un perito informático**: Se encarga de recolectar las evidencias necesarias para lograr tomar una decisión frente a lo sucedido, aparte de proponer una serie de directrices que logran mitigar el caso ocurrido.
- **Equipo de ingenieros:** Son los encargados de brindar el soporte necesario en las diferentes zonas y aspectos que necesiten los soportes encargados.

De acuerdo con lo anterior se pueden describir los tipos de servicios que componen un CSIRT como lo son los servicios activos, proactivos y el maneja de sus respectivas instancias.

Tabla 1 *.Servicios para un CSIRT*

Servicios reactivos	**Servicios proactivos**	**Manejo de instancias**
Advertencias y alertas.	Comunicados.	Análisis de las instancias necesarias.
Método para los incidentes.	Centro de observación tecnológica.	Respuesta o los incidentes con mayor número de casos.
Análisis de los incidentes.	Evaluaciones o auditorias de seguridad.	Coordinación para dar respuesta a una instancia.
Grupos de apoyo en las respuestas de incidentes.	Directrices para el mantenimiento de la configuración de información.	Gestión para la seguridad de la información.

Tabla 1. (Continuación)

Servicios reactivos	Servicios proactivos	Manejo de instancias
Gestión de la coordinación.	Creación de directrices y herramientas para la seguridad.	Análisis de los riesgos presentados.
Generación de respuesta a incidentes.	Servicios para la detección de intrusos.	Como generar continuidad para el negocio.
Como responder a incidentes en sitio.	Trasmisión de la información de seguridad.	Consultoría de seguridad.
Tratamiento de las Vulnerabilidades.		Sensibilización de la compañía.
Análisis de la vulnerabilidad		Educación/Formación.
Respuesta a la vulnerabilidad		Como se evalúan u certifican los productos.
Fuente: Construcción propia del autor		

4.2.4 Políticas de la información: Se define una serie de estándares que establecen políticas de la seguridad, esto con el fin de exponer las siguientes características.

Tabla 2 *.Políticas de la información*

Característica	Descripción
Alcance	Definimos el punto inicial y final de la política incluyendo al personal de sistemas.
Objetivos	Cuáles son los objetivos de dicha política y su descripción, involucrando su definición.
Asignación e identificación de roles	De acuerdo con una estandarización definen los roles correspondientes a la responsabilidad de cada integrante.
Responsabilidad	Al identificar los roles cada uno se plantea las reglas necesarias para cumplir con su rol.
Interacción	Qué tipo de interacción de debe tener entre las partes de la política implicada.
Procedimientos	De forma general se plantean los procedimientos, con una pequeña definición de cada uno de ellos.

Tabla 2. ***(Continuación)***

Característica	Descripción
Relaciones	Se describen el tipo de relaciones entre los servicios y políticas.
Mantenimiento	Se deben establecer políticas que permitan el mantenimiento de ella y especificar las pautas de actualización de estas.
Sanciones	Se definen las reglas a seguir para sancionar a quien no cumpla las políticas, así como el tipo de política de incumplimiento a aplicar.
Fuente: Construcción propia del autor	

4.2.5 Políticas de seguridad para un CSIRT. En las políticas de implementación de seguridad informática, se utilizan estándares como ISO/IEC 27002, en su área correspondiente, describiendo las siguientes características.

Para la implementación de las políticas de seguridad se usará el estándar ISO/IEC 27002, en su área de dominio “políticas de seguridad” describiendo en la siguiente tabla sus principales características.

Tabla 3 .Políticas de seguridad para CSIRT

Políticas de seguridad	Descripción de la política
Políticas para la clasificación de información.	Se clasifican las políticas para el acceso a la información que se requiera.
Políticas externas para que se pueda tener acceso a dicha información.	Se realiza una clasificación de los criterios para tener acceso a la organización, desde lugares externos.

Tabla 3. ***(Continuación)***

Políticas de seguridad	**Descripción de la política**
Política de aislamiento para la información.	Se clasifica la información para recopilar su tipo de naturaleza y criterios para su uso.
Política para la seguridad del internet.	Se otorgan lineamientos para exponer la manera adecuada para usar internet y seguridad de esta.
Política para la notación de incidentes.	Se realizan políticas para el tratamiento de la información consignada en las bitácoras de incidentes.
Política del tratamiento de incidentes.	Que medios se utilizan para identificar los incidentes.
Políticas para el entrenamiento y capacitación.	Que políticas genera la compañía, para que se pueda capacitar de una manera adecuada al personal.
Política para seleccionar personal	Criterios para el reclutamiento de personal, como son sus políticas frente a la seguridad que se quiere proveer y protección de la información de la compañía.
Política para los despidos.	Criterios para prevenir robos de información sensible, así como distribución de esta.
Política para los equipos personales.	Criterios para el uso de computadoras personales, y el uso adecuado de las mismas.
Política para el uso de correos electrónicos.	Lineamientos para el uso de correo electrónico.
Política en la red donde se encuentran las computadoras.	Lineamientos para el control de la red de la compañía interna y externa.
Política de telecomunicación de la información.	Lineamientos para establecer la comunicación entre los diferentes dispositivos de la compañía
Fuente: Construcción propia del autor	

4.2.6 Tecnologías para implementar en un CSIRT. Se deben definir las siguientes tecnologías para tener un énfasis de alta calidad, siendo un estándar en los CSIRT las tecnologías que se describen a continuación:

Tabla 4. Tecnologías por implementar en un CSIRT

Activo	**Objetivo del activo**
Servidores de virtualización de componentes	Se montan las pruebas necesarias para poder simular las características de lo esperado en el CSIRT
Servidores Web	Se deben montar los servicios necesarios para poder contener las plataformas web, para informar a la organización de los diversos casos y parametrización de estos.
Correo electrónico	Se crean correos electrónicos, o se define con los actuales de la compañía de acuerdo con sus roles.
Telefonía VoIP	Se instala el servicio o se le asigna los parámetros necesarios para funcionar con la infraestructura actual.
Servidor RTIR	Sistema que se debe vagar en una plataforma para asignar números de servicio.
Respaldo de datos	Asignación de tareas para la protección de la información mediante el respaldo de datos.
Herramienta SIEM	Genera bitácoras con el historial de dispositivos en el tráfico de red.
Firewall	Se definen la parametrización de la seguridad perimetral.
IDS/IPS	Aplicación que se encargara de filtrar los paquetes que circulan por la red.
Proxy	Encargado de procesar información fuera de la red.
Routers	Se unen 2 redes de Internet y LAN, además que reduce el dominio de broadcast.
Fuente: Construcción propia del autor	

4.3 MARCO HISTÓRICO

CSIRT significa “Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática)”, Este término CSIRT es el más usado en Europa en lugar del término llamado CERT, que se registró en estados unidos por el CERT Coordinación Center (CERT/CC).
A continuación, se usan diferentes abreviaturas para el mismo tipo de equipo:

- CERT o CERT/CC (Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación).
- CSIRT (Computer Security Incident Response Team, equipo de respuesta a incidentes de seguridad informática).
- IRT (Incident Response Team, equipo de respuesta a incidentes).
- CIRT (Computer Incident Response Team, equipo de respuesta a incidentes informáticos)[7]
- SERT (Security Emergency Response Team, equipo de respuesta a emergencias de seguridad)

Uno de los primeros incidentes fue un gusano que apareció en una importante infraestructura tecnológica a finales de los ochenta, el gusano fue llamado Morris el cual se propagó rápidamente y logro infectar a numerosos sistemas del mundo.

Este incidente fue lo que detono una alarma, en la cual el mundo se dio cuenta que existía una necesidad de cooperación y coordinación entre administradores de sistemas y gestores de TI para enfrentar este tipo de casos, En esta época el tiempo fue un factor decisivo se tenía que establecer una reglamentación muy organizada

[7] Convenciones CSIRT Disponible en https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

y estructurada para la gestión de incidentes, así unos días después del incidente “Morris”, la DARPA (Defense Advance Research Projects Agency) creo el primer CSIRT ubicado en la universidad Carnegie Mellón en Pittsburgh(Pensilvania).

Un tiempo después el modelo fue tomado por EUROPA y en 1992 el proveedor holandés SURF net puso en marcha el primer CSIRT de EUROPA, este modelo se siguió tomando por muchos equipos más y en la actualidad el inventario de actividades llega a más de 100 equipos conocidos en EUROPA.

Al pasar el tiempo los CSIRT ampliaron sus capacidades y pasaron de ser una fuerza de reacción a una fuerza que presta un servicio preventivo como alertas y demás actividades de prevención de incidentes.

4.4 ANTECEDENTES O ESTADO ACTUAL

La idea de crear un CSIRT surge [8]cuando la seguridad de las tecnologías de la información pasa a ser una parte fundamental de la actividad principal de la compañía o institución, por ello cuando los incidentes son relacionados con la seguridad de las tecnologías de la información se y hacen parte de un riego es donde se inician las operaciones para mitigar los riesgos que se pueden presentar.

En la gran mayoría de instituciones funciona un departamento de apoyo que funciona de forma regular, o bien un servicio que presta una asistencia técnica, pero realmente no se le da un trato adecuado o de la manera estructurada que debería tener, en general en el ámbito laboral debemos precisar de unas capacidades y una

[8] Ugas, L.). Uso y Difusión de las Tecnologías de Internet para el acceso a la Sociedad Red (2003. Tesis doctoral, Doctorado en Ciencias Gerenciales. Universidad Rafael Belloso Chacín, Vicerrectorado Investigación Gerenciales, Maracaibo, Venezuela.

atención especial, además de un enfoque que garantice que la empresa disminuirá los riesgos que está corriendo actualmente y los daños que se pueden producir.

En la mayoría de los casos el problema radica en la falta de coordinación y no lograr aplicar el tratamiento a los incidentes con el conocimiento que debería garantizar que en un futuro surjan otros incidentes del mismo ámbito y así mismo evitar posibles pérdidas financieras o pérdidas de reputación.

Como ya se ha expuesto el CSIRT pretende atender a un grupo en particular y ayudara a resolver los problemas e incidentes de seguridad de las TI, dentro de los objeticos se destaca elevar el nivel de conocimientos sobre la seguridad de la información e implantar la cultura necesaria para sensibilizar acerca de la seguridad, tal cultura intenta que se logren adoptar desde el principio las medidas necesarias y proactivas que reducen los costos de funcionamiento del propio sistema, en la gran mayoría de casos implantar esta cultura de cooperación lograra una eficacia en general.

¿Qué pasara si no se hace nada? Un manejo inadecuado de la seguridad de la información provocara daño mayor a largo y mediano plazo, además de afectar la reputación de la compañía o institución, aparte de pérdidas financieras y consecuencias legales.

¿Qué pasa si se implementa? Se aumentará la concientización acerca de la posibilidad de que aparezcan problemas de seguridad, lo cual ayudaría a resolverlos con una mayor eficacia y evitar las perdidas futuras.

¿Qué se conseguirá? Dependiendo en gran medida del negocio y de las diferentes pérdidas sufridas en el pasado, los procedimientos y las practicas se seguridad ganaran trasparencia, con lo cual protegeremos el patrimonio esencial de la empresa.

4.5 MARCO LEGAL

Dentro del proyecto se estipulan estándares para el cumplimento de los servicios, mejor llamados en el ámbito profesional como ANS, donde se especificarán sus principales características y según el tipo de contrato, se relacionan una serie de cláusulas para el cumplimiento de estas.

En el ámbito del Hardware, software y dependiendo de la compañía se diseñarán y se revisara la documentación concerniente al copyright, para la utilización de licencias free ya que nos basamos en pruebas de nivel local, pero respetando el licenciamiento de las aplicaciones que utilizaremos, complementando como se debe llevar la documentación dentro del proyecto.

4.5.1 CONPES 3701 Lineamientos de política para la Ciberseguridad y Ciberdefensa": La cual brinda lineamientos de política en Ciberseguridad y Ciberdefensa orientados a una estrategia nacional que logre contrarrestar el incremento de las amenazas informáticas, que están afectando significativamente al país.[9]

4.5.2 CONPES 3854 política nacional de seguridad digital: La cual brinda un apoyo en el enfoque de la política de Ciberseguridad y Ciberdefensa, con énfasis en sectores bancarios, pero con aplicabilidad a diferentes sectores de la industria, en la creciente y sofisticadas formas de afectar el desarrollo normal de las tecnologías TI.[10]

---

[9] MINTIC Compes 3701 de 2011 Lineamientos de política para la seguridad y Ciberdefensa https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

[10] MINTIC Compes 3854 de 2016 Politica nacional de seguridad digital https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

5 DISEÑO METODOLÓGICO

En el presente proyecto se pretende generar conocimientos a partir de la recolección de información en la primera fase, para después utilizar un laboratorio controlado y cumplir los métodos y técnicas necesarias, como se detalla a continuación los siguientes métodos.

5.1 Método deductivo

En el cual se pretende hacer uso de la problemática general del proyecto, realizando una serie de deducciones a nivel global para llegar a un nivel particular de dicho tema del proyecto, con el fin de lograr plantear un comité de respuesta a incidentes de seguridad, para ayudar a planear, desarrollar y mitigar los posibles problemas a nivel de información.

5.2 Método inductivo

Donde se plantea conocer las necesidades y problemas que actualmente posee “Cibersecurity de Colombia LTDA” en temas de seguridad informática, partiendo de los conocimientos particulares para luego generalizarlos.

5.3 Enfoque del sistema

Este tipo de enfoque pretende enfocarnos en profundidad en el análisis de los requerimientos necesarios para poner en marcha un CSIRT, pero también nos ayuda a analizar los componentes como módulos individuales, para entender que necesidades posee el cliente y así generar los informes finales que darán las pautas para poner en marcha un CSIRT y el mantenimiento de este, sin olvidar el análisis de seguridad para corregir prevenir rupturas en seguridad.

6 DESARROLLO DE LOS OBJETIVOS

6.1 IDENTIFICAR LOS PROCESOS QUE INVOLUCRA UN CSIRT COMO HERRAMIENTA DE GESTIÓN DE INCIDENTES EN CIBERSECURITY DE COLOMBIA LTDA.

6.1.1 Servicios Reactivos: Este tipo de servicios están diseñados para responder a las diferentes peticiones de asistencia, en las comunicaciones de incidentes del grupo que será atendido por el CSIRT y cualquier manera que pueda llegar a darse con los sistemas CSIRT, muchos de estos servicios serán iniciados a través de notificaciones de terceros o en visualización de controles, registros de sistemas de detección y alertas**.**

6.1.2 Advertencias y alertas: En este proceso se incluyen la información que describe el ataque de los intrusos, una vulnerabilidad, una alerta o un virus, donde se da una recomendación para tomar la acción necesaria en el menor tiempo posible, las alertas, advertencias o avisos son enviados como una reacción al problema resultante. Este tipo de información es creada por el grupo de CSIRT o bien es extraída de diferentes proveedores de otros CSIRT o de algún experto en seguridad.

6.1.3 Tratamiento de incidentes: En el tratamiento de los incidentes se incluye la recepción de este, el triage y la respuesta a las peticiones de comunicación, así como los análisis de incidentes y acontecimientos, dentro de sus principales actividades podemos destacar las siguientes:

- Actividades para proteger los sistemas y redes con afectación.
- Aportación de las actividades para dar solución y las estrategias de mitigación a partir de los avisos.
- Búsqueda de actividades inconsistentes dentro de las redes.

- Filtración del tráfico de red.
- Reconstrucción de los sistemas con definición incorrecta.
- Corrección y reparación de los sistemas.
- Desarrollo de estrategias de respuesta a incidentes.

Basándonos en la estructura anterior definimos las actividades de tratamiento de incidentes dependiendo del CSIRT y el servicio que se puede detallar y estructurar de acuerdo con las actividades a desarrollar.

6.1.4 Análisis de incidentes: En el análisis de incidentes se realiza un examen de toda la información que está disponible y de las pruebas o instancias relacionadas con el evento, la finalidad es averiguar el alcance del incidente y determinar los daños que ha causado, como también la naturaleza del incidente y estrategias definitivas o provisionales de respuesta. El CSIRT puede tomar los resultados del análisis de las vulnerabilidades para entender lo que ocurrió en el sistema en concreto, determinar el modelo y firmas intrusas, dentro de este modelo se puede dar dos procesos que son:

6.1.4.1 Recopilación de pruebas: Se trata la recogida, conservación, documentación y el análisis de las pruebas forenses del delito informático, para determinar los cambios en el sistema y ayudar a reconstruir el caso, a través de un laboratorio controlado. En las tareas de recolección de pruebas forenses, se debe realizar una copia de seguridad bit a bit de los diferentes sistemas afectados, se realiza una búsqueda de cambios en el sistema como programas nuevos, archivos, servicios, puertos abiertos, y la búsqueda de troyanos. Dentro de las actividades los miembros deben tener la capacidad de ser testigos parciales en los procedimientos.

6.1.4.2 Rastreo: Se realiza un rastreo de los orígenes de un intruso o identificación de los sistemas a los cuales llego a tener acceso, donde se originó el ataque y que otros sistemas utilizo como parte del ataque, esta etapa es comúnmente ejecutada de manera individual, pero es aceptable ejecutarla en colaboración con el personal encargado de la aplicación de ley o bien con los proveedores de internet u otras organizaciones interesadas.

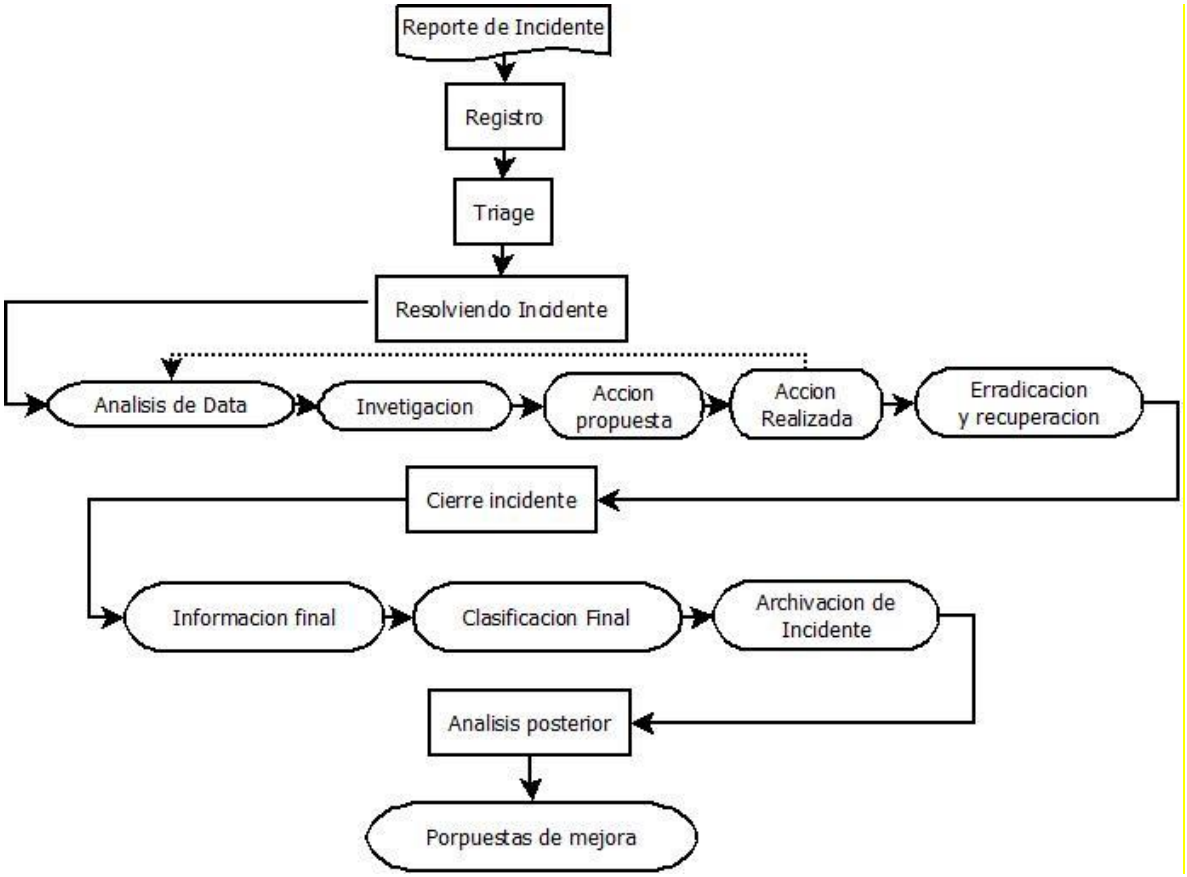
6.1.5 Respuesta a incidentes: En el CSIRT se presta asistencia directa a los incidentes para ayudar a los clientes del grupo de trabajo a recuperarse del ataque, El CSIRT no solo se limitará a dar soporte telefónico o por correo, sino que también se encarga de brindar un soporte físico analizando los equipos, para verificar que no se tenga afectación de Hardware. Si el CSIRT no se encuentra cerca del incidente de igual forma se debe desplazarse hasta donde sea necesario para dar respuesta, dependiendo de la capacidad se podrán disponer de equipo en las diversas sucursales para dar un soporte más oportuno.

6.1.6 Apoyo a la respuesta de incidentes: El CSIRT ayudara y también orientara a las víctimas del ataque informático para que logren recuperarse lo más pronto posible, donde se deberá usar las diferentes técnicas que estén disponibles por el equipo, no se incluye una acción.

6.1.7 Coordinación de respuesta a incidentes: El CSIRT debe coordinar las tareas de las áreas para dar respuesta entre las partes implicadas en el incidente, por lo general se estructuran con, una víctima del ataque, los sitios implicados y cualquier otro sitio que precise asistencia para el análisis del ataque, también es importante incluir a las partes que brindan soporte a la TI de la víctima, como son los proveedores de servicios de internet. Las tareas de coordinación pueden abarcar la recogida de información sobre los contactos, las notificaciones a los sitios implicados en el análisis de información.

6.1.8 Tratamiento de la vulnerabilidad: Se incluye la recepción de la información y las comunicaciones sobre las vulnerabilidades, tanto del software como del hardware, el análisis de la naturaleza del ataque y los efectos de las vulnerabilidades, dado que existen diversas formas de desarrollar las actividades para tratar la vulnerabilidad este servicio se detalla más en base al tipo de actividad que realiza la compañía y el tipo de asistencia que presta, con lo cual se presenta el siguiente diagrama para observar sus árbol de proceso.

Ilustración 1 .Tratamiento de vulnerabilidades



Fuente: Construcción propia del autor

6.1.9 Análisis de la vulnerabilidad: Después de realizar el análisis y exámenes técnicos de las vulnerabilidades, se incluyen unas verificaciones de las sospechas que arroja el examen técnico en los diversos campos, donde se puede incluir el análisis del código fuente y el uso de un depurador para averiguar donde se está produciendo la vulneración hasta la reproducción de escenario afectado.

6.1.10 Respuesta a vulnerabilidades: Se establece la respuesta adecuada para mitigar o reparar alguna vulnerabilidad, lo que puede incluir el desarrollo o búsqueda de las correcciones y soluciones provisionales, así como la notificación de los entes comprometidos, en este proceso incluimos un tipo de aplicación que da respuesta a mediante soluciones provisionales a la afectación.

6.1.11 Manejo de instancias: Vamos a llamar instancia a cualquier elemento, fichero u objeto encontrado en el sistema que puede estar destinado a investigar o atacar a los sistemas y redes que estén usando medidas para esquiar la seguridad, en las instancias se incluyen los virus informáticos, los troyanos, gusanos o secuencias de comando maliciosas. En el tratamiento de las instancias se incluye la recepción de la información y copias de las instancias utilizadas en los ataques, una vez se reciba será analizada y lo que concluya la investigación se pasara a la siguiente área, con el diseño de los mecanismos de control.

6.1.12 Respuesta a instancias: Este tipo de proceso consiste en determinar cuáles son las acciones adecuadas para detectar y eliminar las instancias de un determinado sistema, esto puede implicar la creación de firmas digitales para que se pueda añadir al software de monitoreo para la detección de intrusos.

6.1.13 Coordinación de respuesta a las instancias: Este servicio consta de poner en común y sintetizar con los demás investigadores, a los proveedores y demás expertos en seguridad los resultados de los análisis y el tipo de estrategias de respuesta a las instancias, las actividades incluyen una notificación y la síntesis del análisis técnico de las diferentes fuentes, también se incluirá el mantenimiento de los ficheros públicos y de los clientes atendidos.

6.1.14 Servicios proactivos: Este tipo de servicios esta diseñados para mejorar la infraestructura y el tipo de procesos de seguridad de los clientes atendidos antes de que llegue o se detecte el incidente y reducir su impacto y su alcance en caso de que sea necesario.

6.1.15 Comunicados: Se incluirán las alertas de intrusos, las advertencias de vulnerabilidades y los avisos necesarios sobre seguridad, este tipo de comunicados informarán a los clientes y usuarios sobre las herramientas y vulnerabilidades recientemente detectadas. Los comunicados permiten que los usuarios puedan proteger sus equipos y redes de las nuevas tecnologías que impactaran la infraestructura.

6.1.16 Observatorio de tecnología: El CSIRT posee un área específica para observar los nuevos desarrollos técnicos, las actividades de los atacantes y las tendencias en el rastreo de futuras amenazas, los temas analizados son ampliables para incluir disposiciones jurídicas según sea el caso, este tipo de proceso comprende la lectura de las bitácoras de seguridad, para tener actualizado el equipo con los últimos estándares frente a seguridad.

6.1.17 Evaluación o auditorias de seguridad: Este tipo de proceso consiste en el estudio y el análisis de la infraestructura de seguridad de la organización, basándose en los requisitos que se establecieron por las normas, también incluimos un estudio de las prácticas de seguridad de la organización.

6.1.17.1 Revisión de la infraestructura: Se revisan los manuales de las configuraciones tanto de hardware como de software, los enrutadores, cortafuegos, servidores y los demás dispositivos informáticos, para asegurar que se están adaptando a las políticas de seguridad y las configuraciones estándar de la industria.

6.1.17.2 Revisión de las mejores prácticas: Entrevista a los usuarios y administradores del sistema, para determinar si este tipo de prácticas de seguridad están adaptas a la política de seguridad definitiva de la organización.

6.1.17.3 Escaneo: Se usarán detectores de vulnerabilidades o de virus para indagar que sistemas y redes están vulnerables, por lo general se usa software que filtra el trafico de red revisando la integridad de los paquetes y rastreando posibles animalias.

6.1.17.4 Pruebas de penetración: Se realiza una comprobación a nivel de los sitos atacando deliberadamente las redes y sistemas principales, en la realización de estas pruebas se debe contar con la autorización de la dirección ya que las políticas de algunas organizaciones prohíben este tipo de prácticas, aunque también se pueden subcontratar un tercero para realizar el análisis con altos conocimientos técnicos en la realización de auditorías y evaluaciones.

6.1.17.5 Configuración y mantenimiento de las herramientas y aplicaciones: En este proceso identificamos la manera adecuada para configurar y mantener de modo seguro las herramientas, aplicaciones e infraestructura informática. Además de lograr orientar el CSIRT puede actualizar la configuración y realizar el mantenimiento de las herramientas necesarias y servicios de seguridad, como pueden ser los sistemas de detección de intrusos, filtros, cortafuegos, redes privadas y demás sistemas que estén involucrados, este tipo de servicio incluye una presentación ante la dirección de cualquier problema que surja en las configuraciones o con el uso de las herramientas y aplicaciones del CSIRT.

6.1.18 Difusión de información relacionada con la seguridad: Este proceso proporciona al grupo de usuarios una colección completa donde pueden buscar la información de la seguridad TI y recomendaciones que deben tener cada uno de ellos para salvaguardar y reportar irregularidades, donde podemos incluir lo siguiente:

- Directrices para la comunicación e información de contacto del CSIRT.
- Ficheros de alertas con advertencias y todo tipo de comunicados.
- Documentación sobre las mejores prácticas en la actualidad.
- Asesoramiento sobre la seguridad informática de manera general.
- Políticas y procedimientos con listas de comprobación.
- Desarrollo de las actualizaciones y difusión de ellas.

La información será desarrollada por el equipo del CSIRT y entregada a los equipos de TI, gestión humana o relacionada con los medios, incluyendo información procedente de fuentes externas.

6.2 DETERMINAR LAS HERRAMIENTAS DE SOFTWARE REQUERIDOS PARA LA CONSTRUCCIÓN DE UN CSIRT.

Según Kijewisky[11] , el CERT INCIBE y Home en los trabajos mencionan que uno de los activos más importantes dentro de un CSIRT es el personal, ya que se gasta demasiado tiempo y recurso económico en la capacitación, además de los perfiles necesarios para las labores de los CSIRT, por ello es indispensable definir las herramientas necesarias para que funcione de manera adecuada.

6.2.1 Sitio Web Público: Según Penedo[12] en el trabajo se menciona que muchas personas, el primero contacto que tiene un CSIRT se realiza mediante una página web, en ella podremos encontrar la misión, visión, servicios, datos de contacto y las publicaciones sobre la seguridad, así como los manuales necesarios para concientizar al personal, de hecho es indispensable para poder clasificar e manera más sencilla la incidencia del mismo así como el proceso interno del CSIRT, hasta el momento no se define en que lenguaje codificar la página web ,pero podemos utilizar la misma de la compañía para posteriormente asignar el apartado necesario para su fácil acceso y entendimiento.

[11] P. Kijewski and A. Kozakiewicz, "Security Research at NASK: Supporting the Operational Needs of a CERT Team and More," SysSec Workshop (SysSec), 2011 First, Amsterdam, 2011, pp. 96-99.

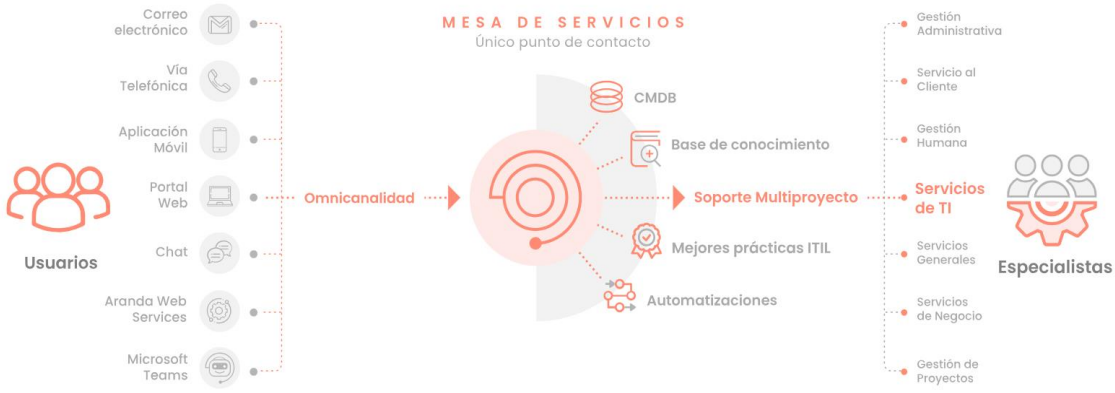
[12] D. Penedo, "Technical Infrastructure of a CSIRT," Internet Surveillance and Protection, 2006. ICISP '06. International Conference on, Cote d'Azur, 2006, pp. 27-27. DOI: 10.1109/ICISP.2006.32

6.2.2 Correo electrónico: Funciona para recibir los informes de los incidentes del grupo en particular, también tiene la función de coordinar a los equipos y realizar los comentarios necesarios para prestar el apoyo a la víctima del incidente[13].De igual forma es posible usar las listas de correo electrónico para la suscripción de los boletines informativos.

6.2.3 Teléfono: Se usará para comunicarse con los usuarios y con otros CSIRT y con los proveedores. En ocasiones el reporte del incidente se puede realizar vía telefónica, cuando esto sucede es una buena práctica anotar todos y cada uno de los detalles del incidente, destacando que una comunicación en tiempo real permite el levantamiento de cada uno de los detalles necesarios y de manera rápida.

6.2.4 Herramienta de manejo de incidentes: Se gestiona mediante la herramienta Aranda[14] software ITSM multiproyecto enfocado a procesos de gestión y servicios que implementa las mejores prácticas, mesa de servicios con un único punto de contacto.

Ilustración 2. Mapa funcionalidades Aranda



[13] Proyecto AMPARO, Manual básico de: Gestion de incidentes de seguridad informática (2012) Consulta: abril 2014 [Online] http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf.

[14] Aranda software https://arandasoft.com/en/productos/service-management/

6.2.5 Sistemas operativos: La elección a utilizar va a depender de los factores como el tipo de red, el perfil del equipo de trabajo y los costos, en la actualidad los sistemas Windows ya son maduros y son flexibles, algunas de sus herramientas de y hacking están disponibles para esta plataforma[15]. OSX es un sistema operativo que se deriva de una BSD por lo cual es una buena alternativa para utilizar comandos Shell y las diversa utilizadas de red, al igual incluye un compilador algunas cabeceras y librerías que permiten una construcción sencilla como Nmap. Linux se convierte en la elección número uno para ,los criminales informáticos y consultores de seguridad debido a que es una plataforma muy versátil ,y el kernel nos permite un buen soporte en sus diferentes componentes, La gran mayoría de ataques basados en IP y herramientas de penetración poder ser construidas y ejecutadas en Linux sin problemas debido a que incluyen todo tipi de bibliotecas de red como libcap, por ello también es bueno posee alternativas para lograr virtualizar el sistema que sea necesario para llegar al objetivo de identificación de los ataques.

6.2.6 Tecnologías de acceso remoto: El acceso remoto a los servicios de CSIRT para las labores de administración y de soporte en teletrabajo es una de las recomendaciones que el CCN[16].Para hacer uso de tecnologías como telnet, steltet y el SSH para la administración remota[17].

---

[15] Shing-Han Li, David C. Yen, Shih-Chih Chen, Patrick S. Chen, Wen-Hui Lu, Chien-Chuan Cho Effects of virtualization on information security Computer Standards & Interfaces, Volume 42, Issue null, Page 1

[16] Centro Criptológico Nacional. (2013, junio) www.ccn-cert.cni.es/. Consulta: noviembre 2020 [Online]. https://goo.gl/WNLRJB

[17] Proyecto AMPARO, Manual básico de: Gestión de incidentes de seguridad informática., 2012

6.2.7 Respaldo de datos: El respaldo de datos lo consideramos como un mecanismo de seguridad que todos deberían poseer, un respaldo permite tener una última esperanza de regresar los datos originales después de que un desastre ocurra[18].Las múltiples copias deben ser administradas y almacenadas fuera del CSIRT para agregar redundancia en la información, el procedimiento y los medios de respaldo deber ser aprobados con cierta periodicidad para asegurar la integridad, los medios permitidos puede ser discos duros o respaldo en nube, solo que este último método no es muy recomendado ya que es un tercero quien la administra[19].

6.2.8 Herramientas de peritaje informático: El análisis forense es uno de los servicios más importantes, si un CSIRT realiza una adecuada investigación forense puede llegar a identificar que ocasiona el problema y toar las medidas necesarias por ello a través del portal del institucional y estándares de tecnología NIST, podremos encontrar una clasificación muy clara de las herramientas que nos permiten realizar las búsquedas de forma sencilla de las distintas herramientas filtradas según su funcionalidad[20].

---

[18] SANS Institute. (2006) https://www.sans.org/. Consulta: noviembre 2020 [Online]. http://goo.gl/FhlnbD

[19] ITECO CERT. (2009, agosto) www.inteco.es. Consulta: octubre [Online]. www.inteco.es/extfrontinteco/icd/pdf/Cortafuegos_VPN_IDS_IPS.pdf

[20] NIST Computer Forensics Tools & Techniques Catalog Consulta: noviembre 2020 [Online]. https://toolcatalog.nist.gov/

6.2.9 Firmas electrónicas: Es un método de cifrado que asociara la identidad de las personas con un equipo informático o al mensaje o documento, en función del tipo de firma, con ello se asegura el tipo de firma, por ello en el directorio activo se cargaran previa organización el listado que será aceptado y estipulado junto con la política necesaria para actualizar el directorio frente al cambio que se puedan plantear o nuevo clientes que ingresen a la compaña[21].

6.2.10 Servidor DNS: Este sistema de nomenclatura jerárquico para las computadoras ,servicios o recursos que se conectan a internet ,asocia la información con nombres de dominio asignado a cada uno una función para resolver los nombres inútiles para que podamos identificarlos de manera binaria ,con el propósito de poder localizar y direccionar las diferentes peticiones , por ello es recomendable que el nombre del dominio sea de tipo compañía-CSIRT.org para que facilitemos la memorización del corrió o sito web[22].

6.2.11 Conexión de alta velocidad: Dependiendo de los servicios que se estén gestionando en el CSIRT, es la velocidad de conexión un punto muy importante por ello es recomendable contar con un servicio de grande velocidad en ambos sentidos, ya sea para recolectar información a través de URL o páginas web, así como para hacer pruebas a algún servidor, en la actualidad se poseen tecnología de fibra óptica simétrica permitiendo velocidades de conexión simétricas de hasta 300mb/s[23].

---

[21] Centro Criptológico Nacional. (2013, junio) www.ccn-cert.cni.es/. Consulta: Noviembre 2020 [Online]. https://goo.gl/WNLRJB

[22] Yolanda S Baker and Sambit Bhattacharya, "Analyzing Security Threats as Reported by the United States Computer Emergency Readiness Team (US-CERT)," ISI, 2013

[23] Velocidad simétrica Movistar/. Consulta: noviembre 2020 [Online] https://ofertas.movistar.co/hogar/fibra-optica

6.2.12 Caja fuerte: Es un tipo de compartimiento de seguridad que fue inventado para que su apertura sea muy complicada para las personas sin autorización y así salvaguardar los elementos de más grande valor, son fabricadas de un tipo de metal de alta resistencia y resguardan el contenido mediante una clave secreta y ese tipo de claves va variando de acuerdo a las políticas que estén pactadas en la compañía ,forma parte del emplazamiento de un CSIRT el cual uso es guardar la información sensible respecto a las incidencias de seguridad tratadas ,así como los documento críticos en papel[24].

6.3 CONSTRUIR LA ARQUITECTURA DEL LABORATORIO CONTROLADO Y VIRTUALIZADO DEL CSIRT PARA CIBERSECURITY DE COLOMBIA LTDA.

6.3.1 Disponibilidad: La disponibilidad de los servicios del laboratorio controlado dependerán de las horas de trabajo de la organización donde este esté ubicado o la entidad donde sea ejecutado, por lo general se busca es generar un plan que permita gestionar las pruebas activas.

6.3.2 Requerimientos de personal: No existe una cantidad exacta para el personal técnico que se necesita para mantener un CSIRT ya que cada uno es totalmente diferente, trabajan en ambientes cambiantes y su objetivo principal varía de acuerdo con su necesidad, por ello partiendo de una experiencia colectiva de la propia comunidad se pueden dar las siguientes definiciones:

[24] ENISA, "Cómo crear un CSIRT paso a paso," 2006 Consulta: noviembre 2022 [Online] https://goo.gl/JIENW8

6.3.2.1 Cantidad: Para la entrega de un servicio central con respuesta y anuncios se necesitan mínimo dos personas a tiempo completo, para un servicio que contemple mayor cantidad de pruebas y que se pueda mantener un índice alto se deben proyectar entre 6 a 8 personas.

6.3.2.2 Competencias: se requerirá personal con niveles de estudio avanzado en informática y pentesting que tengan las siguientes características:

- Creativo, flexible y con espíritu de trabajo en equipo
- Capacidades análisis en minería de datos
- Capacidad de analítica
- Abierto de mente y con muchos deseos de aprender
- Resistente al stress

6.3.2.3 Competencias técnicas: Relación del conocimiento a nivel técnico de cada herramienta como lo es:

- Conocimientos en SO Linux y Unix
- Conocimiento en SO Windows
- Conocimiento en equipamiento como (Rputer, switches, DNS, Proxy, Mail, etc.)
- Conocimiento en protocolos de internet (SMTP, HTTP, FTP, telnet, SSH, etc.)
- Conocimiento en amenazas como lo son (Dos, Phishing, sniffing, etc.)
- Conocimiento en evaluación de riesgos e implementaciones practicas

6.3.2.4 Entrenamiento: En este plan se incluirán dos fases fundaméntales que son el entrenamiento para el staff que recién está tomando las actividades del CSIRT, como también un entrenamiento con un tercero para mejorar continuamente las habilidades iniciales y mantenerse actualizados en la tecnología actual.

6.3.2.5 Código de conducta: Un código de conducta o ética es un conjunto de reglas tipo staff del CSIRT que parametriza cómo comportarse profesionalmente durante la jornada de trabajo o pruebas, y principalmente en horario fuera de oficina. Se tiene en cuenta que el comportamiento fuera de la oficina es bastante relevante ya que la información o incidentes recolectados en los CSIRT deben ser socializados en ambientes de TI y Ciberseguridad.

6.3.3 Workstation de trabajo: Se gestionan 2 equipos para el tratamiento de los incidentes y demás personal, con un portátil HP Elitebook 840 G6 el cual posee las siguientes características:

- Sistema operativo W10
- Procesador Core i7 8565U
- Memoria Ram 8GB SDRAM DDR4-2400 1x8
- Almacenamiento NVMe TLC de 512Gb
- Monitor WLED FHD IPS de 14 pulgadas
- Puertos 2 USB 3,1; Thunderbot Type-C; RJ45
- Cámara de infrarrojos 720p

6.3.4 Maletín forense: Posee los componentes más importantes para realizar una inspección y recolección de información frente a un incidente, realizando un peritaje de manera profesional

6.3.4.1 Clonadora de discos: Este tipo de dispositivos nos permite realizar una copia exacta de los elementos que se encuentre en un equipo o servidor, cabe resaltar que este tipo de copias sirven hasta para dejar imágenes ISO que posteriormente pueden replicarse para realizar las pruebas necesarias.

6.3.4.2 Bloqueadores de escritura: Cuando los peritos informáticos se enfrentan al análisis de los discos duros para realizar su respectivo peritaje, deben tomar las medidas correspondientes, por ello la primera es clonar el disco para no utilizar el original, la segunda precaución es no analizar el disco clonado conectando directamente al ordenador personal sino a través de una bloqueadora de escritura, esta herramienta permite analizar lo que contiene el disco en modo bloqueo ,sin tener que preocuparse de que algún sector sea afectado o que realiza escritura accidental ,lo que permite mantener la cadena de custodia durante el análisis forense.

6.3.4.3 Disco portátil: Este disco permite recolectar información forense manteniendo archivos y evidencia fotográfica, cabe resaltar que este tipo de disco no se debe utilizar en todos los dispositivos, se deben pactar las políticas necesarias para proteger su contenido y poder realizar el peritaje con responsabilidad.

6.3.4.4 Lector de tarjetas: El dispositivo permite leer y escribir la información necesaria de los dispositivos como USB micro-USB Type-C entre otras, permitiendo la flexibilidad de lectura entre dispositivos.

6.3.4.5 Cámara de fotos: La cámara digital es indispensable cuando se realiza un robo de información o acceso a lugares físicos dentro de entidad, permitiendo que se realice el análisis posterior de la escena del crimen, identificando los patrones que se pueden dar y así mismo generar las políticas para que no se pueden volver a presentar.

6.3.4.6 Etiquetadora: El dispositivo es necesario para inventariar los elementos según las políticas de gravedad y clasificación de dispositivos, junto con la serie de códigos que lo guardaran en el historial facilitando su búsqueda en el futuro.

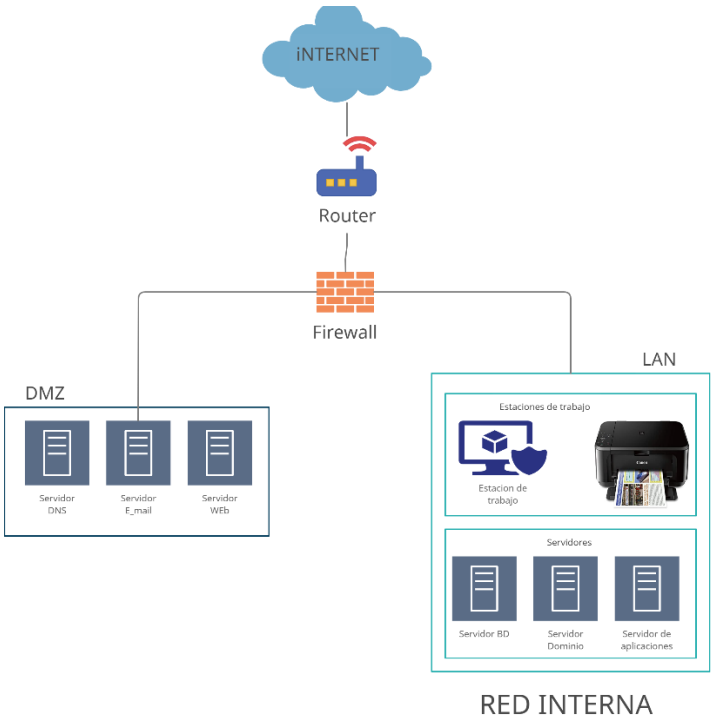
6.3.5 Infraestructura de red: La infraestructura de red del CSIRT debe estar aislada de la red de la organización, en donde debe tener su estructurará propia de subredes y dominios, se recomienda que el CSIRT contenga una estructura de red de computadores aislada, que permitirá implementar segmentos de redes con las funciones específicas de cada prueba, al menos deben tener dos segmentos dentro de la red del CSIRT:

- Red de la operación en ambiente de producción: donde se almacenarán los datos y se ejecutarán las tareas relativas de los servicios.
- Red para laboratorio: Donde se aplicarán pruebas y estudio controlados.

6.3.5.1 Diagramas sugeridos: A continuación, se describen los diferentes diagramas que describen los escenarios más comunes en las organizaciones, y que se aplicaran a Cibersecurity de Colombia LTDA.

6.3.5.1.1 Diagrama 1 Red básica segura

Ilustración 3. Red básica segura



Fuente: Construcción propia del autor

Tabla 5. Debilidades y fortalezas del modelo matricial

Fortalezas	Debilidades
• Se comparte flexiblemente recursos humanos entre los diferentes productos. • Se logra la coordinación para satisfacer las demandas de los clientes. • Se proporcionan oportunidades para desarrollar las habilidades funcionales y en los productos. • Es la más adecuada para organizaciones de tamaño mediano y que contiene productos múltiples.	• Consume un índice alto de tiempo, que implica reuniones frecuentes. • Se requiere un esfuerzo considerable pata mantener el poder. • Implica que los participantes tengan buenas habilidades interpersonales. • No funcionara a menos que los integrantes entiendan y adopten relaciones colegialas en vez de tipo vertical.
Fuente: Construcción propia del autor	

6.3.5.1.2 Diagrama 2 Red segura redundante

Ilustración 4. Red segura redundante

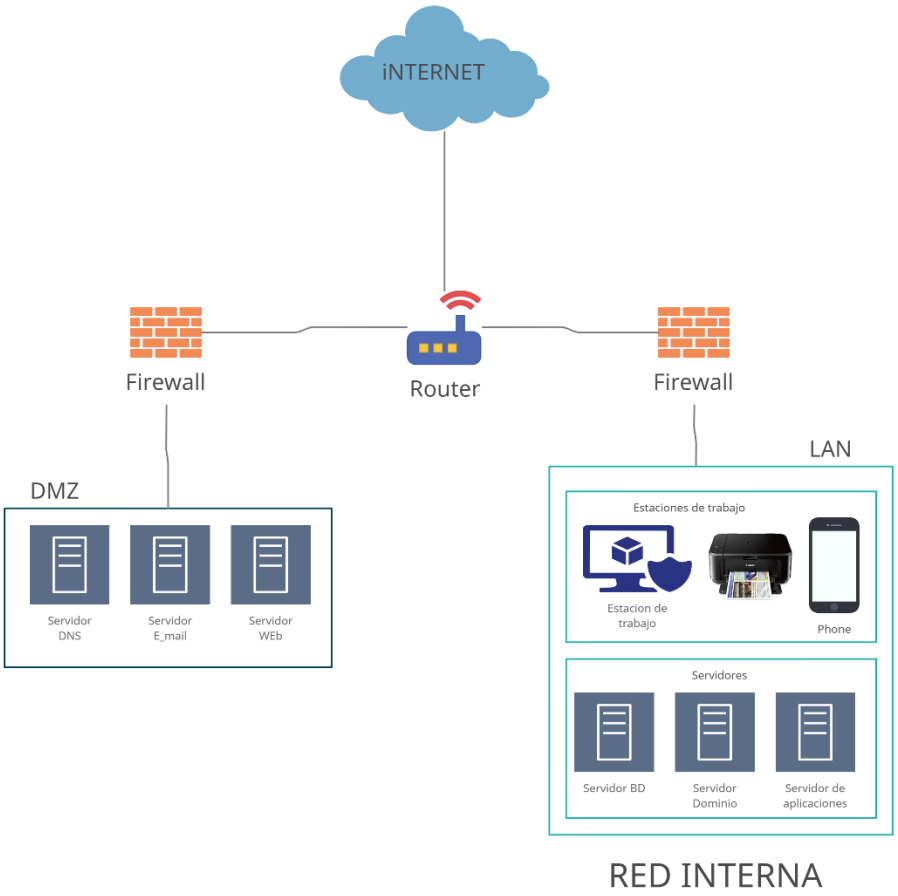
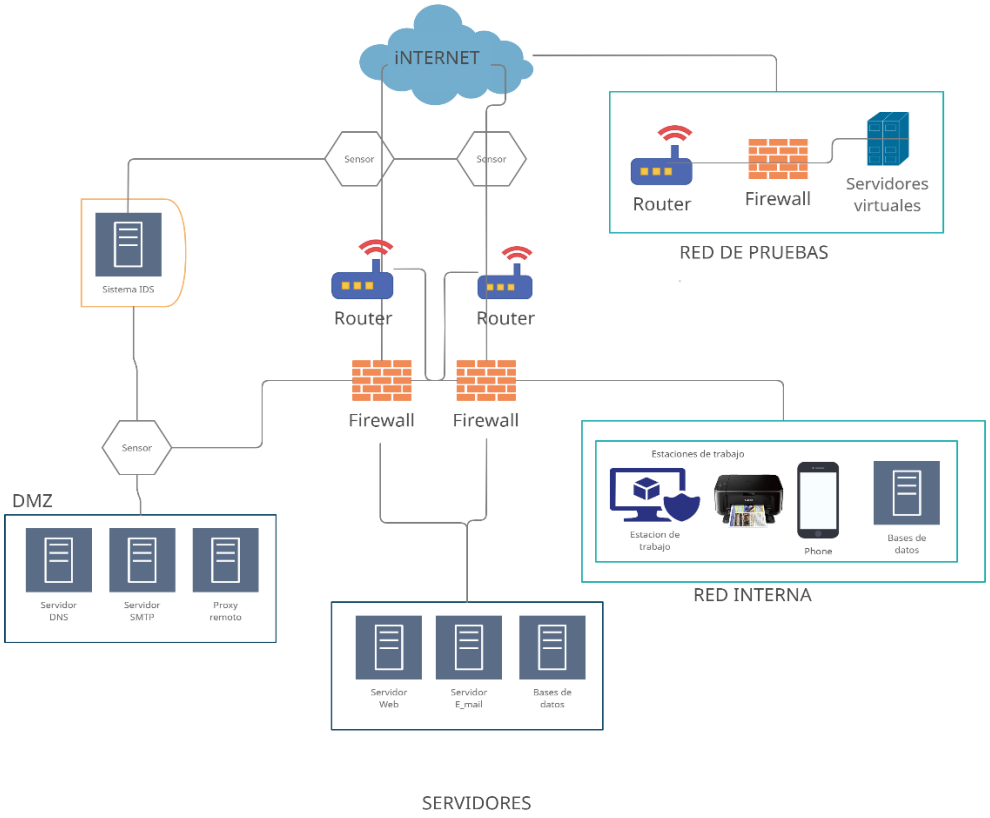


Tabla 6. Descripción sobre esquema de red segura redundante

Detalle	Descripción
Característica	• Esquema que brinda servicios reactivos. • Se compone de dos segmentos de red regulados por Firewalls. • Se debe tener un acceso mínimo de 2Mbps
Software	• Se tiene la opción de usar software libre.
Fuente: Construcción propia del autor	

6.3.5.1.3 Diagrama 3 Red segura segmentada y redundante

Ilustración 5. Red segura segmentada y redundante



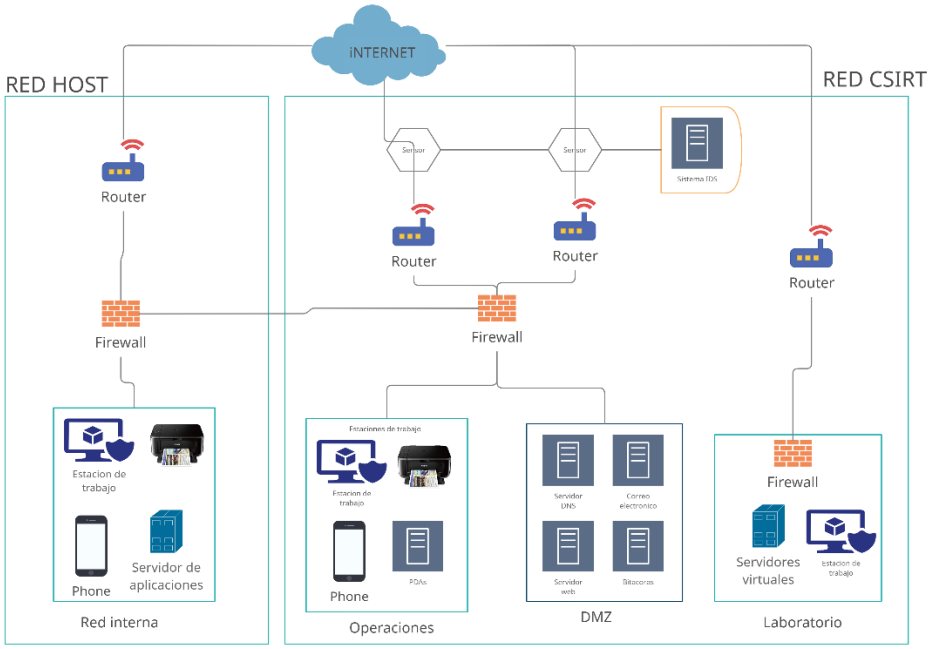
Fuente: Construcción propia del autor

Tabla 7. Descripción de esquema de red segura segmentada y redundante

Detalle	Descripción
Característica	• Sensores con sistema de detección de intrusos. • Enlace de internet redundante. • Esquema que brinda servicios reactivos y proactivos. • Accesos entre segmentos regulados por varios firewalls • Alta disponibilidad de los servicios. • Enlace principal de 8Mbps. • Enlace secundario de pruebas con conexión de 2Mbps
Software	• Se tiene la opción de usar software libre.
Fuente: Construcción propia del autor	

6.3.5.1.4 Diagrama 4 Red segura segmentada y separada para la organización.

Ilustración 6. Red segura segmentada y separada para la organización



Fuente: Construcción propia del autor

Tabla 8, Descripción de esquema de red segura segmentada y separada para la organización

Detalle	Descripción
Característica	• Posee separación física de la red CSIRT y la organización. • Enlaces de acceso a internet redundantes para el CSIRT. • Sensores y servidor con sistemas IDS. • Red aislada para pruebas en el laboratorio. • Niveles de acceso interno. • Enlace para la organización de 2 Mbps. • Enlace redúndate CSIRT 4Mbps. • Enlace para el laboratorio de 2Mbps
Software	• Se tiene la opción de usar software libre.
Fuente: Construcción propia del autor	

6.3.6 Infraestructura de hardware: Está conformada por todos los elementos físicos dentro de la oficina o lugar físico, que contiene los servidores, centros de datos y elementos de red, en la siguiente tabla se listan los elementos necesarios.

Tabla 9. Descripción de elementos físicos CSIRT

Equipo	Elemento
Estaciones de trabajo	• Computadores portátiles • Accesorios: Discos duros, pendrive, CD, etc.
Equipos de seguridad en ambientes físicos	• Caja fuerte con protección de fuego para almacenamiento de documentos y copias de seguridad. • Infraestructura que proteja contra incendios (Prevención, detección y alarma). • Sistema de refrigeración y aire acondicionado compatible con especificación frente a los equipos adquiridos. • Infraestructura con protección frente a fallas de suministro eléctrico (Estabilizadores generadores y demás).
Equipos y medios de conectividad	• Switches • Routers • Firewall • Intranet • Backups • Dispositivos de seguridad (Antivirus IDS, IPS) • Enlace de internet que cuente con velocidad necesaria para soportar la operación • Cableado estructurado • Acceso (VPN)
Otros	• Impresora multifuncional • Trituradora de papel • Dispositivos para la creación de copias de seguridad en los diferentes entornos • Proyector multimedia
Fuente: Construcción propia del autor	

6.3.7 Infraestructura de software: Está conformada por todo el software que se solicita para realizar las pruebas en los diferentes entornos como lo puede ser dominios, Emails, evaluación de vulnerabilidades, etc., que se a continuación se describen.

6.3.7.1 Herramienta de dominios e IP: Este tipo de aplicación se encarga de traducir las solicitudes de nombres de dominio comparándolas con una base de datos con listas negras para identificar su autenticidad, como por ejemplo www.example.com estaría asociada a la IP 198.212.43.212, si se encontrara asociada a una IP diferente a la anteriormente expuesta se daría por terminada la conexión.

- DomainTools https://www.domaintools.com
- Domain Dossier http://centralops.net/co/DomainDossier.aspx
- ANS Mapping to IP https://team-cymru.com/community-services/ip-asn-mapping/
- GeoLite2 https://dev.maxmind.com/geoip/geolite2-free-geolocation-data
- RIPEstat https://stat.ripe.net/about/

6.3.7.2 Herramientas de email: Este tipo de herramienta analiza las cabeceras de los mensajes email dentro de la organización, con la opción de revisarlo sin la necesidad de abrirlo, a través de una lista negra filtra lo que considera como spam o posible amenaza para los equipos.

- Google Apps Messageheader https://toolbox.googleapps.com/apps/messageheader/
- MX Toolbox https://mxtoolbox.com/EmailHeaders.aspx

6.3.7.3 Herramienta de monitoreo de red: Este tipo de herramientas recopilan y procesan datos de netflow o sflow que se envían a dispositivos con versiones compatibles, que son soportador por IPV4 e IPV6.

- Nfdump http://nfdump.sourceforge.net
- Nfsen http://nfsen.sourceforge.net

6.3.7.4 Herramienta de auditoria: Son un conjunto de herramientas que permiten el escaneo de redes y monitorización de estas, buscando vulnerabilidades en los diferentes componentes que tiene la red.

- Nmap https://nmap.org
- autoScan-Network http://www.autoscan-network.com
- Wireshark https://www.wireshark.org
- AbuseHelper https://github.com/abusesa/abusehelper

6.3.7.5 Herramientas de vulnerabilidades: Son las herramientas que permiten adquirir información de vulnerabilidades a través de prueba de penetración o también llamado “Pentesting” junto con un desarrollo de firmas para realizar una detección de intrusos en diversos sistemas operativos para tener una calificación del nivel de seguridad.

- Nessus https://www.tenable.com/products/nessus/nessus-professional
- Vega https://subgraph.com/vega/index.en.html
- Metasploit https://www.metasploit.com
- SQLcheck https://www.softpedia.com/get/Internet/Servers/Database-Utils/SQL-Check.shtml
- Burp Suite https://portswigger.net/burp
- Kali Linux https://www.kali.org

6.3.7.6 Herramienta de detección: Este tipo de herramientas se encarga de detectar intrusos a través de la red con una serie de reglas, aunque también trabajan con patrones que pueden ser maliciosos, una de las ventajas de este tipo de herramientas es que podemos ver por consola el comportamiento en tiempo real.

- Snort https://www.snort.org
- Tripwire https://sourceforge.net/projects/tripwire/

6.3.7.7 Herramientas de análisis forense: Este tipo de herramientas permiten levantar la mayor cantidad de información concerniente al incidente de seguridad, para posteriormente replicarlo y así mismo tomar las medidas para mitigarlo.

- Sleuth Kit http://www.sleuthkit.org
- Autppsy http://www.sleuthkit.org/autopsy/
- EnCase http://www.sleuthkit.org/autopsy/
- FTK,Forensic Toolkit https://accessdata.com/products-services/forensic-toolkit-ftk
- Tcpxtract http://tcpxtract.sourceforge.net

6.3.7.8 Herramientas de Malware: Se define el malware como cualquier tipo de software malicioso que está diseñado para infiltrarse en un dispositivo sin el conocimiento del usuario, sabiendo esto existe muchos tipos de malware, pero así mismo existe una variedad de herramientas que se van actualizando con una biblioteca, normalmente en cada antivirus de los diferentes sistemas operativos.

- VirusTotal https://www.virustotal.com/gui/home/upload
- Malware Hash Registry https://team-cymru.com
- Malwr https://malwr.com
- Hybrid Analysis https://www.hybrid-analysis.com

- MISP, Malware information Sharing https://mispriv.circl.lu/users/login
- Malware Domain List http://www.malwaredomainlist.com

6.3.7.9 Herramientas de WIFI: Es tipo de herramientas se encargan de filtrar las redes y revisar el tráfico que circula a través de ella en los diferentes canales frecuencias y protocolos que están disponibles actualmente.

- Acrylic WIFI Scanner https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wlan-scanner-acrylic-wifi-free/
- InSSIDER https://www.metageek.com/products/inssider/

6.3.7.10 Herramientas análisis de data: Este tipo de herramienta nos permiten revisar el comportamiento de los diferentes datos que se van indexando, por lo general estas apps funcionan con expresiones regulares en los blogs.

- Splunk https://www.splunk.com

6.3.7.11 Herramientas de cifrado: Estas herramientas permiten el cifrado de información sensible dentro de los análisis y resultados de los componentes anteriores, siempre protegemos el flujo de los datos con este tipo de parámetros.

- VeraCryp https://archive.codeplex.com/?p=veracrypt
- GnuPG https://archive.codeplex.com/?p=veracrypt

6.3.7.12 Herramientas de rastreo de incidencias: Este tipo de herramienta funcionan como la mesa de ayuda de una mesa TI, crea casos dándole estados para poder determinar el nivel de complejidad y atención que necesite, con componentes adicionales que permiten una medir gestión.

- OTRS https://otrs.com/es/home/
- RTIR https://otrs.com/es/home/

6.3.7.13 Bases de datos: las bases de datos son básicamente el almacenamiento de toda la información concerniente al CSIRT, la cantidad y tipo dependen mucho del sistema, después de la estructuración del sistema se puede desplegar la BD para comenzar la ingesta de datos.

- MySQL https://www.sqlite.org/index.html
- SQLite https://www.sqlite.org/index.html
- PostgresSQL https://www.postgresql.org

7 CONCLUSIONES

En la identificación de los procesos dentro de un CSIRT se analiza cómo influyen en el uso correcto del CSIRT y en la gestión de incidentes a lo largo del tiempo. Cada componente genera un árbol adecuado que optimiza la gestión del CSIRT. Estos componentes nos permiten estructurar el CSIRT desde cero en nuestra organización Cibersecurity LTDA y establecer las bases para su gestión a largo plazo, adaptándonos a los cambios tecnológicos que puedan surgir.

Finalmente, para la construcción de un CSIRT como herramienta de gestión de incidentes y detección de vulnerabilidades, debemos tener claridad en los procesos que se involucran, tales como los servicios de notificación de los incidentes a través de una herramienta de gestión , su posterior tratamiento y análisis para identificar las diferentes instancias afectadas con la recopilación de las pruebas generando el rastreo y así mimo una respuesta al tipo de incidente detectado, su tratamiento y posterior divulgación a las diferentes áreas para mejorar la seguridad.

No obstante, este proceso se acompaña de las herramientas de software necesarias para la gestión, identificación y divulgación de la información con las tecnologías que permitan el adecuado peritaje, en el laboratorio virtualizado propuesto con arquitectura segura segmentada y separada donde se realizaran las pruebas con la disponibilidad y requerimientos de personal con las competencias técnicas necesarias en sus Workstation.

8 RECOMENDACIONES

Se debe usar Software de seguridad en todas las redes de la compañía, así como en cada uno de sus dispositivos. Se resalta que los criminales siempre usaran una combinación de diferentes dispositivos para lograr acceder a las redes, por ello es importante lograr parchar cada elemento del sistema.

En la instalación de Software no se debe optar por programas gratuitos ya que estos pueden extraer la información personal de los dispositivos, además de que en algunos casos se tiene acceso al código fuente y esto genera una vulnerabilidad alta en el sistema donde estén implementados.

No dar clic en los links de correos bancarios o de dudosa procedencia, debemos teclear directamente el link en la URL, aunque estamos dentro de la red corporativa no estamos exentos de que personas dentro de la misma organización y bien correos basura o se logren filtrar correos fraudulentos.

Se debe usar un conjunto de contraseñas seguras no solo para ingresar a os diversos portales sino también para el acceso de nuestros propios archivos, esto se debe hacer con contraseñas que combinen letras, números y otros caracteres, con políticas que ajusten este cambio cada cierto periodo de tiempo.

Nunca se deben ignorar las actualizaciones de software, y se debe asegurar la versión necesaria en los sistemas operativos, en algunos casos puede que la vida útil de un software llegue a su final, entonces entrara en el caso como poder migrar los elementos y que gestión se debe hacer sin afectar su integridad.

Se debe verificar que todos los sitios que se estén accediendo deben tener encriptación SSL (Secure Sockets Layer) por sus siglas. Por lo general en la parte

superior derecha aparece un icono con un candado que lo confirma, o bien que el sitio este escrito con https y no http.

Finalmente, una de las prácticas más básicas es el respaldo de la información en dispositivos externos, y almacenado en lugares donde será protegido de factores meteorológicos.

9 BIBLIOGRAFÍA

ARANGO GOMEZ. Oscar Dario, El ABC de la seguridad informática: guía práctica para entender la seguridad digital, 2023, 93 p.

ASOBANCARIA. Implementación y puesta en marcha CSIRT para el sector financiero. {En línea} {Consultado abril 2022}. Disponible en Internet: https://www.asobancaria.com/wp-content/uploads/CSIRT-Financiero-Asobancaria-julio-2018.pdf

CASTAÑEDA. Marlon Stiven, Panorama de Ciberataques más Recurrentes en Colombia 2021 y 2022, 2022, 6 p.

CONGRESO DE COLOMBIA. Ley 1273 2009, {En Línea}. {Consultado julio 2022}.Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.

CSIRT . Equipos de Ciberseguridad y Gestión de Incidentes españoles {En línea}. {Consultado agosto 2023}. Disponible en: https://www.csirt.es/index.php/es
CSIRTS. Committed to connecting the world {En línea}. {Consultado agosto 2022}. Disponible en: https://www.itu.int/en/ITUD/RegionalPresence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

DEFINICIÓN DE CSIRT. OAS {En línea}. {Consultado septiembre 2022}. Disponible en : https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

DEFINING COMPUTER. security incident response teams America Ciber Defense Agenci {En línea}. {Consultado abril 2022}. Disponible en Internet: https://www.us-

cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

DEPARTAMENTO NACIONAL. política nacional de explotación de datos (bigdata). {En línea}.{Consultado agosto 2022} Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3920.pdf

GAMBOA SUAREZ. Jose, Importancia de la seguridad informática y ciberseguridad en el mundo actual, 2020, 12 p.

GONZÁLEZ. Edwin Mauricio, Actualidad de Colombia en seguridad de la información, 2014, 6 p.

PEREZ Ernesto Estévez. CSIRTs ITU {En línea}. {Consultado septiembre 2016} Disponible en: https://www.itu.int/en/ITUD/RegionalPresence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

QUIROZ ZAMBRANO. Silvia, Seguridad en informática: consideraciones, 2017, Vol. 3,676-688 p.

RUIZ. Claudia Bibiana, Los ciberdelito y la ciberseguridad: una cuestión de género, 2023, No. 13, 73-84 p.

UIT. Measuring the Information Society Report {En línea}.{Consultado septiembre 2022} Disponible en: http://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

ANEXOS

1. Rae Diseño para la construcción de un CSIRT como herramienta de gestión de incidentes y detección de vulnerabilidades para la empresa Cibersecurity de Colombia Ltda.

Tabla 5. Rae

Fecha de Realización:	14/12/2020
Programa:	Especialización en seguridad informática
Línea de Investigación:	Gestión de la información
Título:	DISEÑO PARA LA CONSTRUCCIÓN DE UN CSIRT COMO HERRAMIENTA DE GESTIÓN DE INCIDENTES Y DETECCIÓN DE VULNERABILIDADES PARA LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA
Autor(es):	Sánchez Mahecha Esneyder
Palabras Claves:	CSIRT, ciberespacio, Ciberdefensa, infraestructura crítica
Descripción:	Diseño para construir un CSIRT como herramienta de gestión de incidentes y detección de las vulnerabilidades de la empresa Cibersecirity de Colombia ,a través de la identificación de los procesos que involucran en un CSIRT ,herramientas de software necesarias para la construcción del mismo y diseño de la arquitectura de laboratorio que virtualizar los elementos que se presenten para su análisis, con el objetivo de disminuir los incidentes informáticos y obtener el control necesario para el tratamiento ,así como las bitácoras que pueden ayudar a las demás organizaciones para prever un daño significativo dentro de la organización.
Fuentes bibliográficas destacadas:	

ARANGO GOMEZ. Oscar Dario, El ABC de la seguridad informática: guía práctica para entender la seguridad digital, 2023, 93 p.

ASOBANCARIA. Implementación y puesta en marcha CSIRT para el sector financiero. {En línea} {Consultado abril 2022}. Disponible en Internet: https://www.asobancaria.com/wp-content/uploads/CSIRT-Financiero-Asobancaria-julio-2018.pdf

CASTAÑEDA. Marlon Stiven, Panorama de Ciberataques más Recurrentes en Colombia 2021 y 2022, 2022, 6 p.

CONGRESO DE COLOMBIA. Ley 1273 2009, {En Línea}. {Consultado julio 2022}.Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.

CSIRT . Equipos de Ciberseguridad y Gestión de Incidentes españoles {En línea}. {Consultado agosto 2023}. Disponible en: https://www.csirt.es/index.php/es
CSIRTS. Committed to connecting the world {En línea}. {Consultado agosto 2022}. Disponible en: https://www.itu.int/en/ITUD/RegionalPresence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

DEFINICIÓN DE CSIRT. OAS {En línea}. {Consultado septiembre 2022}. Disponible en : https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

DEFINING COMPUTER. security incident response teams America Ciber Defense Agenci {En línea}. {Consultado abril 2022}. Disponible en Internet:

https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

DEPARTAMENTO NACIONAL. política nacional de explotación de datos (bigdata). {En línea}.{Consultado agosto 2022} Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3920.pdf

GAMBOA SUAREZ. Jose, Importancia de la seguridad informática y ciberseguridad en el mundo actual, 2020, 12 p.

GONZÁLEZ. Edwin Mauricio, Actualidad de Colombia en seguridad de la información, 2014, 6 p.

PEREZ Ernesto Estévez. CSIRTs ITU {En línea}. {Consultado septiembre 2016} Disponible en: https://www.itu.int/en/ITUD/RegionalPresence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

QUIROZ ZAMBRANO. Silvia, Seguridad en informática: consideraciones, 2017, Vol. 3,676-688 p.

RUIZ. Claudia Bibiana, Los ciberdelito y la ciberseguridad: una cuestión de género, 2023, No. 13, 73-84 p.

UIT. Measuring the Information Society Report {En línea}.{Consultado septiembre 2022} Disponible en: http://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

Contenido del documento:	El documento consta de:

	• Definición del problema, justificación y objetivos propuestos • Un Marco referencial donde se incluyen: marco teórico, conceptual, histórico y legal. Una sección de desarrollo de objetivos que consta con tres ítems: • 1 Identificación los procesos que involucra un CSIRT como herramienta de gestión de incidentes en Cibersecurity de Colombia LTDA. • 2 Determinación de las herramientas de software requeridos para la construcción de un CSIRT. • 3 Diseño la arquitectura del laboratorio controlado y virtualizado del CSIRT para Cibersecurity de Colombia LTDA.
Conceptos adquiridos:	• Definición de un CSIRT dentro de la organización como método de recepción e identificación de incidentes para dar respuesta a problemas de seguridad. • El taque informático que consiste en la búsqueda de una falla para aprovecharse de un recurso de interés frente a hacker. • Cada construcción de un CSIRT debe tener definición de los conceptos básicos para poder enfrentar los diferentes incidentes, de la misma forma que los servicios necesarios para la gestión de estos. • Definición de las principales políticas para ejecutar y mantener el CSIRT dentro de la organización como Core de su TI. • Cada una de las personas que hacen parte de CSIRT deben tener un conocimiento elevado en sus sectores facilitando la interpretación y el análisis de los diferentes incidentes.

	• El concepto de seguridad no solo se rige por un conjunto de reglas sino también por el conjunto de elementos que pueden ayudar a proteger los diferentes activos de información.
Conclusiones:	• Todas las organizaciones dentro de su equipo de TI deberían tener un equipo de CSIRT, para permitir la correcta gestión de los incidentes y el tratamiento para prevenir que los mismos surjan en un futuro. • La cultura de seguridad no solo está dada por las reglas que implementa la alta dirección, sino también por el cuidado y correcta gestión de los diversos empleados en sus actividades diarias para salvaguardar la información. • No todas las compañías pueden tener un CSIRT, pero si pueden implantar diferentes políticas que permiten proteger su información, o se puede optar por terceros que dan servicios especializados por un bajo costo.