DISEÑO DOCUMENTAL DE UN CENTRO DE RESPUESTAS E INCIDENTES INFORMÁTICOS -CSIRT

HECTOR DANIEL OCAMPO LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2022

DISEÑO DOCUMENTAL DE UN MARCO DE TRABAJO PARA DAR DESARROLLO A LAS ACTIVIDADES PROPIAS DEL CSIRT

HECTOR DANIEL OCAMPO LÓPEZ

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

Ing. EDGAR MAURICIO LOPEZ
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Popayán - Cauca., 20 de septiembre de 2022

A mi madre,

Todo lo que soy y espero ser, se lo debo a mi Madre.

Abraham Lincoln.

TABLA DE CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZA: objeto o persona que representa el potencial de daño de un riesgo

ADDRESS RESOLUTION PROTOCOL (ARP): protocolo de resolución de direcciones, es el protocolo encargado de encontrar la dirección de hardware de un terminal que corresponde a una dirección IP

AUTENTICACIÓN: proceso de acceso seguro a un sistema informático

BACKDOOR: un backdoor o Puerta trasera, es un medio para acceder a un sistema informático eludiendo los mecanismos de seguridad tales como la autenticación y verificación de credenciales.

BUFFER OVERFLOW: el desbordamiento de buffer o buffer overflow en inglés, es un error informático que se produce cuando la información que intenta procesar un software sobrepasa su capacidad de procesamiento y memoria, lo cual puede ser usado por ciber delincuentes para manipular de manera ilegal los sistemas informáticos.

CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS (CSIRT): también conocidos como equipo de respuesta a emergencias informáticas (CERT), entre otros, es el nombre dado a un equipo que proporciona y brinda una serie de servicios (manejo de incidentes, monitoreo, manejo de vulnerabilidades, etc.) y es el encargado de manejar todos los incidentes de seguridad informática en una organización[1]

CONPES: Consejo Nacional de Política Económica y Social, es el documento en donde se plantean proyectos y programas para suplir las necesidades del país

DNS: Domain Name System, es el servicio encargado de enlazar las direcciones IP con los nombres de dominio

CIFRADO: procedimiento mediante el cual determinada información se vuelve ilegible haciendo uso de un algoritmo de seguridad, de tal manera que la información no es accesible a personas no autorizadas, para el acceso a esta información se debe contar con un mecanismo de descifrado, el cual varía dependiendo del algoritmo de encriptación.

CROSS SITE SCRIPTING: es un ataque informático de tipo inyección, en el cual se inyecta un script malicioso en el código de una aplicación o sitio web de confianza, de esta manera el usuario objetivo ejecuta la aplicación o accede al sitio web sin saber que está siendo víctima de un ataque informático, de esta manera el atacante puede acceder a la información que se esté ejecutando en el navegador del usuario tales cookies, tokens de sesión, etc.

[1] ENISA. HOW TO SETUP CSIRT AND SOC. Good Practice Guide. En: DEFINITIONS OF CSIRT AND SOC. ENISA, 2020.

CVE (Common Vulnerabilities and Exposures): es una base de datos que publica información sobre incidentes de seguridad, vulnerabilidades de sistemas, eventos de seguridad, entre otros.

DOS: la denegación de servicios o Denial of Service en inglés, es un tipo de ataque informático que tiene como objetivo por lo general servidores web, en este tipo de ataque, el atacante hace uso de diferentes técnicas para inundar con peticiones http un servidor, lo cual genera un desbordamiento en la capacidad de procesamiento, por consiguiente, hace que sea imposible acceder a los servicios alojados en el servidor

DDOS: es un tipo de denegación de servicios en el cual el atacante usa diferentes computadores, previamente infectados, para inundar con peticiones un servidor.

EXPLOIT: aplicación diseñada con el fin de sacar provecho de una vulnerabilidad en un sistema informático.

INCIDENTE INFORMÁTICO: es un evento de seguridad que deriva en la infracción y violación de una política de seguridad y que puede comprometer los activos de información.

INFORMATION GATHERING: La obtención de información por su significado en español, comprende todas las actividades enfocadas a recolectar la mayor cantidad de información sobre un objetivo tal como sistema operativo, software, servidores, puertos, dirección IP, entre otros, con el fin de aumentar las probabilidades de eficacia de un test de penetración o bien sea un ataque informático por parte de un ciberdelincuente

MALWARE: es un término que se usa para describir una amplia variedad de software malicioso diseñado para dañar dispositivos, servicios y software.

PLAN DE CONTINUIDAD DE NEGOCIO: es un conjunto de procedimientos y políticas establecidas por una organización con el fin de garantizar el funcionamiento de esta después de cualquier incidente

RIESGO: posibilidad de que se produzca un daño a la organización.

SEGURIDAD: cualquier medida que impida la materialización de riesgos y eventos no deseados en un sistema informático.

SISTEMA DE DETECCIÓN DE INTRUSOS: mecanismo de seguridad usados para prevenir accesos no autorizados a los sistemas informáticos de una organización, protegiendo así a las redes de la organización de amenazas externas provenientes de redes externas como internet

SOCIAL ENGINEERING: la ingeniería social por su significado en español, es una amplia gama de actividades que se efectúan a través de la interacción humana que tienen como fin manipular al objetivo con el fin de inducir errores de seguridad informática u obtener información sensible sobre los sistemas de información de una organización o cualquier tipo de información que ponga en peligro la continuidad de negocios.

VIRUS INFORMÁTICO: software malicioso que tiene como objetivo alterar el normal funcionamiento de un sistema informático, con la capacidad de replicarse en múltiples terminales.

VULNERABILIDAD: riesgo de que un sistema informático pueda sufrir daños

RESUMEN

Este trabajo tiene como objetivo explicar el funcionamiento de un CSIRT (Computer Security Incident Response Team). Metodológicamente, se utilizará la revisión documental de estudios e investigaciones de ciberseguridad, recopilación bibliográfica de autores referentes mundiales en temas de CSIRT/CERT. Se determinarán las políticas, procedimientos, requerimientos tecnológicos y técnicos, entre otros. La necesidad de implementar este centro de respuesta, nace a raíz de la aparición de nuevas amenazas de seguridad informática, las cuales buscan vulnerar la seguridad de la organización y acceder de manera ilegal a la información o causar daños a esta, aunado a ello, el incremento de los niveles de conectividad a internet y las condiciones de virtualidad derivadas de la adaptación de las organizaciones debido a la pandemia del COVID-19. Se busca con ello, mitigar y reducir el impacto de un ataque informático, así como también generar buenas prácticas de seguridad y comprender los mecanismos de seguridad y los compromisos de la organización para garantizar el correcto funcionamiento del CSIRT

Palabras claves: ciberseguridad, CSIRT, tecnología, amenazas, ataques, vulnerabilidad, información, internet.

ABSTRACT

This work aims to explain the operation of a CSIRT (Computer Security Incident Response Team). Methodologically, the documentary review of cybersecurity studies and research, bibliographic compilation of world reference authors on CSIRT/CERT issues will be used. The policies, procedures, technological and technical requirements, among others, will be determined. The need to implement this response center arises as a result of the appearance of new computer security threats, which seek to violate the security of the organization and illegally access information or cause damage to it, coupled with this, the increased levels of internet connectivity and virtual conditions derived from the adaptation of organizations due to the COVID-19 pandemic. This is sought to mitigate and reduce the impact of a computer attack, as well as to generate good security practices and understand the security mechanisms and the organization's commitments to guarantee the correct functioning of the CSIRT.

Keywords: cybersecurity, CSIRT, technology, threats, attacks, vulnerability, information, internet.

INTRODUCCIÓN

Con la creciente aparición de amenazas de seguridad informática que trae consigo el desarrollo tecnológico, cada día se hace necesario enfocar y realizar más esfuerzos con el fin de mantener y proporcionar un nivel de seguridad a la información de las organizaciones. Aunque muchas veces se tengan altos estándares de seguridad, no es posible llegar a un estado ideal de seguridad en el cual los riesgos sean reducidos a cero, es por ello por lo que se debe contar con un equipo apto y procedimientos en caso de que un riesgo se materialice y se vea comprometida la información de la organización. Para ello existen los Centro de Respuesta a incidentes Cibernéticos (CSIRT), los centros de asistencia, también denominados equipos, surgen para dar respuesta a incidentes donde se compromete la seguridad, básicamente la función principal de estos equipos es responder con rapidez ante los riesgos materializados.

Generalmente los centros de respuesta a incidentes cibernéticos esa conformado por un equipo de personas altamente especializadas y entrenadas para afrontar y resolver los retos que conlleva dar respuesta a un ataque o incidente informático , dichos especialistas deben contar con capacidades de coordinación, trabajo en equipo, manejo de situaciones de crisis, y lo más importante ser aptos para prevenir, detectar y brindar una respuesta ágil y efectiva con el fin de disminuir los impactos que pueda generar un incidente en la organización.

Un Centro de Respuesta a incidentes Cibernéticos no solamente cumple con responder con rapidez ante los riesgos materializados, de acuerdo con welivesecurity.com, un CSIRT también debe garantizar que después de un incidente se puedan operar los sistemas informacionales con normalidad en el menor tiempo posible y con el menor impacto tolerable, de tal forma que se logre prevenir eventos similares que puedan ocurrir en un futuro, es decir un CSIRT no solo actúa al momento de la ocurrencia de un incidente si no también antes y después de estos.

En este trabajo se va realizar un estudio de la forma como operan los CSIRT, presentando los lineamientos, políticas, procesos y procedimientos para la gestión de la seguridad de la información al interior de una organización, de tal forma que se pueda establecer las directrices y normas a seguir en su implementación, de manera que puedan determinar de forma precisa las actividades de administración, gestión y operación propias de su quehacer, en relación con los recursos existentes y los servicios ofrecidos respecto a los incidentes de ciberseguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Históricamente hablando se puede decir que el evento que impulsó a las organizaciones a enfocarse en la seguridad informática fue el ataque efectuado el 2 de noviembre de 1988 , en el cual un gusano llamado “Morris” en referencia a su creador Robert Tappan Morris, lo que resultó en que una gran porcentaje de los servidores que se encontraban conectados a ARPANET quedaran fuera de servicio, entre estos servidores de Harvard, Princenton, Nasa, Johns Hopkins entre otros, lo que llevó a los expertos de seguridad informática a determinar cómo podrían mejorar la respuesta a incidentes de seguridad informática. Como resultado de esta reunión se determinó la creación de un centro de coordinación del equipo de respuesta a emergencias informáticas (CERT/CC). A partir de este momento empieza el crecimiento y la creación de varios equipos de respuesta a emergencias informáticas, cada una con diferentes propósitos, requerimientos y constitución, por ello la interacción entre los diferentes CSIRT se hacía difícil al no contar con estándares o convenciones que parametrizaran el funcionamiento, procedimientos y políticas de estos mismos. Posteriormente en 1989, ocurrió un ataque de tipo gusano de mayor impacto, este incidente fue llamado el “Wank worm” y dejo en evidencia la necesidad de comunicación e interacción entre los diferentes equipos, a raíz de esta problemática nace FIRST (Forum o Incident Response and Security Teams), este foro tiene como misión principal, aumentar la interacción y la integración de los equipos de seguridad y respuesta a incidentes informáticos alrededor del mundo y hacer de internet un lugar más seguro para todos .

Así como FIRST, existen otras entidades referentes en seguridad informática a nivel mundial, por ejemplo, ENISA (European Union Agency for Cibersecurity), esta agencia tiene como principal objetivo alcanzar un alto nivel común de ciberseguridad informática en Europa, fue creada en el 2004 y entre sus funciones se encuentran contribuir a las ciber políticas de la Union Europea, mejorar la fiabilidad de productos y servicios TIC mediante la creación de esquemas de certificación en ciberseguridad, cooperar con los miembros de la unión europea a hacer frente a los retos de ciberseguridad. Otro referente mundial es INCIBE (Instituto Nacional de Ciberseguridad de España), el cual tiene como fin principal trabajar para aumentar los niveles de seguridad y confianza digital y contribuir al desarrollo seguro del ciberespacio en España, además también de ser los encargados de operar el centro de respuestas a incidentes de seguridad informática de referencia para España el INCIBE-CERT.

1.2. FORMULACIÓN DEL PROBLEMA

La creciente acelerada evolución tecnológica por la cual está pasando la humanidad actualmente, ha conllevado a la Cuarta Revolución Industrial, una revolución que ha estado desarrollándose desde mediados del siglo pasado, la cual tiene como eje principal la integración de las tecnologías digitales, el ámbito biológico y el físico. Un factor divergente con respecto a las demás revoluciones industriales que han surgido a lo largo de la historia de la humanidad es que esta cuarta revolución está enmarcada en la aceleración producto de la convergencia tecnológica, la cual conlleva a un crecimiento exponencial y gracias al fenómeno de globalización tiene un impacto mayor alrededor del mundo.

Este inminente impacto de la Cuarta Revolución Industrial conllevará a que los gobiernos y organizaciones cambien sus modelos de funcionamiento con el fin de operar de manera más rápida y ágil apoyándose en las plataformas globales digitales soportados en tecnologías como Big Data, Cloud Computing, Internet de las Cosas, Ciberseguridad, 5G, industria 4.0, entre otras tecnologías enmarcadas dentro de las tendencias TIC generadas por INCIBE[2] , estos nuevos modelos de operación permitirán a las organizaciones operar de manera más rápida, ágil y optima, a pesar de todas las bondades que traen consigo la implementación de tecnologías en los modelos de operación de las organización, también existe un factor a tener en cuenta el cual es la seguridad y o los posibles riesgos inherentes al uso de la tecnología, tal como menciona Klaus Schwab, fundador y director general del Foro Económico Mundial, en su libro la cuarta revolución industrial, “estas trasformaciones significan que las empresas necesitan invertir fuertemente en sistemas de ciber datos de seguridad para evitar la disrupción directa de delincuentes o activistas, o los fallos involuntarios en la infraestructura digital” .

Siendo consciente de la importancia de la seguridad informáticas y del inminente impacto de la Cuarta Revolución Industrial, el Gobierno Colombiano ha venido desarrollando estrategias de preparación de los escenarios y ambientes en el país. En el 2011 mediante la formulación del documento CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa, se dieron los primeros pasos en el campo de la seguridad informática, este documento tenía como objetivo fortalecer las capacidades para enfrentar amenazas cibernéticas, lo que dio origen a equipos de respuestas a incidentes informáticos como el COLCERT, (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), posteriormente en el 2017 se formula el documento CONPES 3854, el cual tenía como objetivo fortalecer las múltiples partes involucradas en la seguridad digital, a pesar de que estos documentos marcaron un hito y un paso importante en ámbitos de seguridad informática, los resultados esperados no se cumplieron ya que estas políticas públicas fueron principalmente dirigidas al gobierno nacional, y fue escaso el interés que demostraron las múltiples partes interesadas[3] por lo que fue muy poco el avance respecto

[2] INCIBE. Tendencias en el mercado de la Ciberseguridad. En: Mapa de Tendencias TIC. Madrid: INCIBE, 2016. p19.

[3] De acuerdo al Documento CONPES 3854 Política Nacional de Seguridad Digital, las múltiples partes interesadas son: “Gobierno nacional y territoriales, organizaciones públicas y privadas, Fuerza Pública, propietarios u operadores de las infraestructuras criticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades”

a temas de defensa y seguridad en los entornos digitales. Al dirigir principalmente la implementación de las políticas de seguridad del CONPES 3854 al Gobierno Nacional, la baja incorporación de múltiples partes interesadas en las políticas de seguridad informáticas, generó diferentes problemáticas, por ejemplo, que organizaciones públicas y privadas no se sintieran preparadas ante incidentes informáticos (amenazas cibernéticas, ataques cibernéticos, etc.), baja fiabilidad del uso de las plataformas electrónicas, desconfianza en el manejo de datos personales, falta de desarrollo de acuerdos y convenidos de intercambio de información, falta de desarrollo de mecanismos y estrategias relacionados con defensa y seguridad de entornos digitales, lo que finalmente resultó en el desarrollo de un ambiente de baja confianza digital, generando en Colombia una disminución en el índice de competitividad digital 2020 generado por el IMD World Competitiveness Center[4] cayendo del puesto 58 al 61 entre 63 países en total, lo cual resalta falencias en factores como el talento humano, la educación y la implementación de tecnologías, lo cual conlleva a un atraso tecnológico en Colombia.

Como se puede observar anteriormente, un atraso tecnológico y de competitividad digital, genera entre otras cosas bajos índices de confianza digital lo que a su vez desencadena en una baja interacción con los servicios digitales, bajo intercambio de información, divisas y bienes digitales, lo cual influye directamente en la arquitectura tecnológica y los esfuerzos de implementación, educación y formación en áreas relacionadas con la tecnología, por consiguiente, no se lograría la implementación de modelos de operación soportados por las tecnologías emergentes de la Cuarta Revolución industrial.

Se puede concluir entonces que, uno de los factores fundamentales en el entorno digital es la confiabilidad de las organizaciones y las personas en los entornos informáticos, es por ello, que se requiere fortalecer las infraestructuras de seguridad informáticas en Colombia; una de estas infraestructuras y quizá una de las más importantes son los Equipos de respuesta a incidentes informáticos, mediante estos grupos de trabajo se podrían fortalecer los procesos de confiablidad en diferentes sectores gubernamentales y privados interesados en ambientes tecnológicos, impulsando así el uso de tecnologías e incentivando el intercambio de información, y demás servicios digitales. Con base a lo anterior y teniendo en cuenta el uso de los Equipos de Respuesta a Incidentes de Seguridad Informática como principal herramienta para elevar los indicies de confiabilidad digital e incentivar el desarrollo tecnológico y basado en estas premisas, la presente investigación pretende explicar ¿Cómo son gestionados e implementados los servicios y actividades de un CSIRT?

[4] El IMD World Competitiveness Center, es un equipo de trabajo que pertenece al International Institute for Management Development (IMD), la cual es una de las escuelas de negocios más importantes del mundo, quienes mediante el centro mundial de competitividad se encargan de generar diferentes rankings mundiales, entre ellos: ranking de competitividad, ranking de competitividad digital, ranking de ciudades inteligentes, entre otros.

2. JUSTIFICACIÓN

La creciente aparición de amenazas de seguridad informática que trae consigo el desarrollo tecnológico producto de los defectos en el diseño de los sistemas informacionales, hace necesario enfocar y realizar más esfuerzos con el fin de mantener y proporcionar un nivel de seguridad a los activos digitales de las organizaciones. Aunque muchas veces se tengan altos estándares de seguridad, no es posible llegar a un estado ideal de protección en el cual los riesgos sean reducidos a cero; es por ello, por lo que se debe contar con un equipo apto y que ponga en práctica los procedimientos necesarios en caso de que un riesgo se materialice y se vea comprometida la información de la organización.

Para ello existen los Centros de Respuesta a incidentes Cibernéticos, estos equipos de trabajo surgen de la necesidad de dar respuesta a incidentes en donde se compromete la seguridad informática. Básicamente la función principal del CSIRT es responder con rapidez ante los riesgos materializados, después de la pandemia por covid 19, la gran mayoría de empresas se vieron forzadas a migrar sus procesos a ambientes virtuales, muchas de estas no estaban preparadas para afrontar dichos cambios en sus procesos operativos y más aún cuando no se dimensionan los problemas de seguridad que surgen por la poca información y preparación. Así mismo según Eduardo Carozo[5], estos grupos de trabajo también son encargados de generar alertas y advertencias notificando a las partes afectadas, Entre sus funciones está también la de llevar a cabo una adecuada gestión de los incidentes, recopilar información para efectuar un análisis de las causas, vulnerabilidades y amenazas que permitieron que se materializara estos hechos.

La importancia del Centro de Respuesta es bastante alta ya que son los encargados de efectuar el manejo de los incidentes de seguridad y de efectuar todas las tareas necesarias para mantener la continuidad del negocio de la organización, reducir el impacto de los incidentes, efectuar informes detallados sobre los incidentes en donde se especifica la naturaleza del mismo, su origen, los activos afectados, así como también elaborar los mecanismos de protección para prevenir futuros ataques o incidentes, entre otras funciones.

Es por ello que se hace necesario que las organizaciones tengan conocimientos sobre cómo implementar un Centro de Respuesta a incidentes Cibernéticos y todas las actividades que derivan de ello como por ejemplo, los procedimientos para efectuar requerimientos técnicos y de personal, organización, funciones, políticas de seguridad, entre otros, esto se podría lograr mediante la elaboración de un marco de trabajo que sirva como referencia para las organizaciones al momento de implementar un CSIRT, de esta manera, se garantiza que los Centros de respuesta cumplan con los requisitos mínimos y necesarios para su funcionamiento, de tal manera que se encuentren enmarcados dentro de políticas y procedimientos coherentes que permitan su correcto funcionamiento.

[5] CAROZO B., Eduardo. Centro de respuesta a incidentes informáticos... ¿Para qué? En Revista Seguridad cultura de prevención para TI. Vol. 16. (ago. 2018).

3. OBJETIVOS

3.1. OBJETIVOS GENERAL

Documentar el diseño de un CSIRT apoyado de estándares y modelos de seguridad informática

3.2. OBJETIVOS ESPECÍFICOS

1. Establecer los procedimientos y políticas de seguridad necesarios para la implementación de un Centro de Respuesta a Incidentes Informáticos.

2. Evaluar los diferentes recursos tecnológicos (hardware y software) junto con los servicios necesarios para el funcionamiento del CSIRT.

3. Examinar los diferentes estándares, modelos y recomendaciones de seguridad informática aplicables a un CSIRT.

4. Proponer un flujo de procesos para el desarrollo de las actividades al interior del Centro de Respuesta a Incidentes Informáticos.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

4.1.1 Definición de CSIRT

Según ENISA[6] (European Union Agency for Cibersecurity), en el libro Como implementar un CSIRT y un SOC[7], el termino CSIRT, también conocido como CERT, SIRT, entre otros, es un equipo que tiene como rol principal manejar los incidentes de seguridad informática, este proceso comprende el análisis, detección, transferencia de conocimientos, gestión de las vulnerabilidades, planes de continuidad de negocios, entre otros. Con el pasar de los años los CSIRT han evolucionado y ya no solo se encargan de manejar los incidentes de seguridad informáticos, sino también de prestar servicios de seguridad más complejos, comprendiendo actividades como alertas, formación, implementación de mecanismos de seguridad informática, gestión de riesgos, integración con entidades de seguridad, etc. entre otros.

4.1.2 Referentes teóricos

Como se menciona anteriormente, debido a la evolución de los CSIRT y a la incorporación de nuevas actividades dentro de sus funciones, los CSIRT establecen dentro de su funcionalidad la cooperación entre agencias de seguridad, por lo cual los centros de respuesta deben cumplir con algunos estándares que garanticen un correcto funcionamiento inter agencial. Una de las organizaciones encargadas de estandarizar y garantizar la cooperación entre agencias es Forum of Incident Response and Security Teams (FIRST), fue creado a partir del incidente del gusano Morris, tiene como función principal la integración de los equipos de respuesta a incidentes informáticos en cada país alrededor del mundo con el fin de hacer de internet un lugar más seguro para todos.

Otro referente relevante que sirve como fundamento teórico para el desarrollo de este trabajo es la Agencia de las Naciones Unidas para la Ciberseguridad (ENISA), dicha organización se encarga de buscar que los estándares y niveles de ciberseguridad sean altos en todo el territorio europeo. ENISA fue creada en el año 2004 y ofrece servicios enfocados a mejorar la fiabilidad de productos y servicios TIC mediante esquemas de certificación en ciberseguridad, capacitaciones y generación de conocimiento, garantizando así la cooperación entre los diferentes estados miembros de la comunidad europea para afrontar los retos de ciberseguridad. Esta organización también genera contenido académico y guías relacionadas con la implementación y puesta en funcionamiento de CSIRT; dentro de la documentación que se va a emplear se encuentran Cómo crear un csirt paso a paso – ENISA, How to setup up csirt and soc, good practice guide – ENISA.

[6] ENISA (European Union Agency for Cibersecurity), agencia que tiene como principal objetivo alcanzar un alto nivel común de ciberseguridad informática en Europa, fue creada en el 2004 y entre sus funciones se encuentran contribuir a las ciber políticas de la Union Europea

[7] ENISA. HOW TO SETUP CSIRT AND SOC. *Good Practice Guide*. En: Computer security incident response teams. ENISA, 2020. P6.

Otra organización que sirve como referente conceptual de análisis para el desarrollo de este trabajo es el Instituto de Nacional de Ciberseguridad de España (INCIBE), la misión principal de INCIBE es afianzar la confianza digital, mejorar los niveles de ciberseguridad y contribuir para el uso seguro del ciberespacio a través de los mercados digitales en España, son también los encargados de administrar el INCIBE CERT.

INCIBE también es referente en relación a investigaciones en el campo de ciberseguridad, en donde abarcan temáticas como almacenamiento seguro, confianza digital, cifrado, hacking ético, seguridad en servicios, entre otros temas. Al igual que ENISA, INCIBE también cuenta con bibliografía que servirá de entorno conceptual para esta investigación, dentro de los recursos teóricos que pueden ser aplicados tenemos los siguientes: Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía – INCIBE, Guía nacional de notificación y gestión de ciberincidentes – INCIBE, Guía básica de protección de infraestructuras críticas- INCIBE.

Por último, en Colombia podemos encontrar bibliografía concerniente a los CSIRT, el documento Lineamientos del equipo de respuesta a incidentes de seguridad de la información y el Lineamiento para gestión de incidentes y vulnerabilidades de seguridad de la información, generados por la presidencia de la república, dichas publicaciones contienen información relativa a las directrices y pautas relacionadas con el manejo de incidentes y vulnerabilidades de ciberseguridad aplicables a los CSIRT en Colombia, lo cual sirve de punto de partida para alienar los conceptos de las entidades expertas en ciberseguridad y CSIRT tales como INCIBE, ENISA, FIRST, entre otros, con lo que se espera de un CSIRT en Colombia.

4.2. MARCO CONCEPTUAL

En el desarrollo de este trabajo de grado se hará uso de un marco teórico referencial que permita fundamentar los aspectos técnicos y la terminología relacionada con los centros de respuesta a incidentes cibernéticos.

4.2.1 AMENAZA:

Evento o condición que tiene el potencial de causar perdida de activos y las consecuencias o impactos derivados de dicha perdida. [8].

4.2.2 INCIDENTE:

Evento anómalo o inesperado, conjunto de eventos, condición o situación en cualquier momento durante el ciclo de vida de un proyecto, producto, servicio o sistema[9].

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST-SP 800-160. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. En: GLOSARY. Gaithersburg, MD: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2016. p. 175.

[9] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST-SP 800-160. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. En: GLOSARY. Gaithersburg, MD: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2016. p. 168.

4.2.3 PLAN DE RESPUESTA A INCIDENTES INFORMATICOS:

Es un conjunto de instrucciones y procedimientos que permite al personal de TI detectar, responder y recuperarse a un incidente de seguridad informático

4.2.4 RIESGO:

Es la medida del grado en el cual una entidad es amenazada por una potencial circunstancia o evento, en función de: (i) el impacto adverso, o la magnitud del daño que ocurriría si la circunstancia o el evento ocurre; y (ii) la probabilidad de ocurrencia[10].

4.2.5 SEGURIDAD:

Libertad de aquellas condiciones que pueden causar la pérdida de activos con consecuencias inaceptables[11].

4.2.6 VULNERABILIDAD:

Debilidad en un sistema, procedimientos de seguridad de un sistema, controles internos, o implementación que puede ser explotada o activada por una amenaza[12].

Así mismo se debe tener en cuenta que los CSIRT tienen diferentes campos de actuación, los cuales varían de acuerdo con su propósito, misión y alcance. Según la OEA[13], los CSIRT pueden ser agrupados de acuerdo con la comunidad a la cual le prestan los servicios como se presenta a continuación:

4.2.7 CSIRT DE INFRAESTRUCTURAS CRITICAS:

Estos CSIRT, tienen su enfoque en la protección de todas las infraestructuras críticas de una nación, estos CSIRT pueden ser operados por privador o por organizaciones gubernamentales.

4.2.8 CSIRT ACADÉMICO:

Tienen su enfoque principal en instituciones de la educación como, por ejemplo, colegios, universidades, institutos, etc., la complejidad y el tamaño del CSIRT depende de la institución.

---

[10] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST-SP 800-53A. Assessing Security and Privacy Controls in Information Systems and Organizations. En: GLOSARY. Gaithersburg, MD: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2016. p. 710.

[11] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST-SP 800-160. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. En: GLOSARY. Gaithersburg, MD: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2016. p. 171.

[12] Ibid., p. 176.

[13] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSIRT nacional. Washington, D.C. 2016

4.2.9 CSIRT COMERCIALES:

Se encargan de suplir todos los servicios de un CSIRT a las organizaciones cuando estas deciden tercerizar los servicios ofrecidos por los CSIRT, esto debido a diferentes razones como limitaciones tecnológicas, talento humano, capacitación, etc.

4.2.10 CSIRT GUBERNAMENTAL:

Se encargan de suplir los servicios del CSIRT a las instituciones del estado con el fin de garantizar los niveles de seguridad adecuados en toda la infraestructura tecnológica gubernamental y los servicios que ofrecen a los ciudadanos.

4.2.11 CSIRT NACIONAL:

Este CSIRT es el centro de coordinación nacional de respuesta a incidentes informáticos, su función depende de la existencia de otros CSIRT, por ejemplo, si en un país no existe un CSIRT de infraestructura critica, el CSIRT nacional hará las veces de este.

4.2.12 CSIRT DEL SECTOR MILITAR:

Tiene su enfoque principal en proveer los servicios a todas las instituciones militares y dar soporte a su infraestructura tecnológica y servicios que ofrecen.

4.2.13 CSIRT DE PROVEEDORES:

Ofrecen servicios de CSIRT a un proveedor o fabricante de productos específicos, por ejemplo, HP CSIRT y Adobe PSIRT.

4.2.14 CSIRT DEL SECTOR DE PEQUEÑAS Y MEDIANAS EMPRESAS:

Debido al poder económico y la necesidad de estas empresas, por lo general no les es posible implementar equipos de respuesta a incidentes informáticos, es por ello por lo que existen estos CSIRT, los cuales cubren las necesidades de negocios las Pymes.

4.3. MARCO HISTÓRICO

El origen de los CSIRT surge como consecuencia a de un ataque a la infraestructura global tecnológica a finales de los 80, dicho ataque, causado por el gusano Morris, de gran impacto en la comunidad tecnológica a nivel global, ya que afectó aproximadamente 60.000 terminales que se encontraban conectada a internet; para ese entonces, era una gran cantidad de dispositivos, lo que generó que los administradores desconectaran las terminales de internet con el fin de prevenir infecciones, generando así la caída de servicios y de las redes de internet a nivel mundial, es aquí donde organizaciones alrededor del mundo ven la importancia de crear mecanismos de defensa y protección ante ataques informáticos y generar procedimientos de gestión ante incidentes informáticos. Una de las primeras organizaciones en crear un equipo de respuesta a incidentes informáticos (CSIRT), fue la Defense Advanced Research Projects Agency (DARPA), quienes crearon el primer CSIRT conocido como CERT Coordination Center (CERT/CC), ubicado en

Estados Unidos. Otras organizaciones a nivel mundial vieron la importancia y la necesidad de implementar sus propios equipos de respuestas a incidentes informáticos, con el fin de satisfacer esta necesidad. SURF[14] creó el primer CSIRT de Europa, llamado SURFnet-CSIRT, actualmente SURFcert, a partir de este momento y siguiendo las nuevas tendencias de seguridad, se crearon diversos CSIRT alrededor del mundo, con el fin de mantener las organizaciones protegidas ante algún incidente informático.

En Colombia, el origen de los CSIRT se remonta al año 2012, mediante la implementación del documento CONPES 3701, en el que se establecieron acuerdos nacionales para enfocar los esfuerzo en el ámbito de la defensa y seguridad cibernética; documento que marca un hito en la lucha contra el crimen cibernético en Colombia, a partir de allí nace el colCERT, (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), el cual tiene como función principal la ciberseguridad y ciberdefensa nacional; es decir, la protección de infraestructura critica de las entidades gubernamentales, así como también brindar asesoría a entidades privadas.

Otro equipo de respuesta de incidentes de seguridad informática en Colombia es el CSIRT-PONAL; equipo de respuesta de incidentes creado por la policía nacional en colaboración con la fiscalía, con el fin de investigar y brindar atención a los posibles casos de ciberdelincuencia que afectan a la sociedad en general. De igual manera el sector bancario, que maneja información de carácter sensible vio la necesidad de crear un CSIRT, denominado CSIRT Financiero, cuyo gestor fue Asobancaria. Este CSIRT se enfoca en el sector financiero y es el primer CSIRT en establecer un modelo colaborativo entre entidades bancarias.

4.4. ESTADO ACTUAL

De acuerdo con el índice de Ciber Seguridad Nacional, generado por NCSI (National Cyber Security Index)[15], Colombia se ubica a nivel mundial en el puesto número 65 y el numero 10 a nivel continental en relación a la ciber seguridad; según José Caballero Economista Senior del IMD Wolrd Competitiveness Center, “se origina debido a una recesión del marco tecnológico y las actitudes adaptativas”, esto no solo indica una retraso tecnológico, si no también resalta otras falencias en factores como el talento humano, tecnología, educación, entrenamiento en el ámbito de investigación y ciencia. Otro de los factores que derivan de esta disminución en competitividad digital es la falta de confianza en los entornos digitales, de acuerdo con el índice de evolución Digital 2017 del HBR, Colombia ocupa el puesto 32 entre 42 países, con un puntaje de 2,33, lo cual lo ubica por debajo del promedio global, este deficiente índice de confianza digital genera poca interacción y acceso a servicios digitales por parte de usuarios y organizaciones.

Una posible estrategia para mejorar el índice y la situación actual sobre ciber seguridad en Colombia (retraso tecnológico, bajos índices de confianza digital, poca investigación y desarrollo del ámbito tecnológico, entre otras), es un plan integral de fortalecimiento de las

[14] Es una asociación de instituciones de educación e investigación holandesas, que tiene como fin desarrollas los mejores servicios digitales y fomentar el intercambio de conocimientos.
[15] NCSI. ÍNDICE DE CIBER SEGURIDAD NACIONAL [sitio web]. [Consultado: 20 de abril de 2021]. Disponible en: https://ncsi.ega.ee/country/co/

organizaciones públicas y privadas, teniendo como base el panorama de seguridad y los nuevos retos generados a causa de la pandemia del COVID-19. El panorama general de seguridad se ha visto modificado en gran medida, debido a esta contingencia, lo que generó nuevos retos a las organizaciones para continuar con su funcionamiento, situación que involucra la apropiación de nuevas estrategias laborales y cambios en los mecanismos de funcionamiento, como en el caso del teletrabajo. Esta migración de entornos laborales físicos a entornos virtuales, ha generado que se maximice la alerta situacional sobre los riesgos que conlleva la utilización de entornos virtuales por parte del sector empresarial. De acuerdo con el Security Report "Latino América 2020" generado por ESET[16], aproximadamente el 45% de los usuarios de entornos digitales recibieron intentos de phishing y más del 50% asegura que las organizaciones no brindaron las herramientas de seguridad necesarias para migrar a entornos virtuales de trabajo. De acuerdo con lo anterior, queda en evidencia la brecha digital existente, debido a la obligatoria implementación de la virtualidad generada por la contingencia del COVID-19, lo que obliga a las organizaciones y a la sociedad en general a una aceleración en los procesos de transformación digital, algo para lo cual las organizaciones y los usuarios no estaban preparados.

A raíz del impacto causado por la pandemia, las organizaciones se vieron en la necesidad de efectuar cambios en las estrategias de negocios, así mismo en la implementación de planes de contingencia y planes de continuidad, esto obligó a acelerar los procesos de implementación de maniobras virtuales para garantizar el funcionamiento de todos los procesos. La premura en mantener la operatividad durante la pandemia generó una brecha de seguridad, quizá la vulnerabilidad más peligrosa y fácil de explotar por parte de los atacantes son los usuarios con desconocimiento de los diferentes tipos de amenazas que pueden encontrar, propensos a ataques de ingeniería social, configuraciones inseguras en las estaciones de trabajo, robo de información, uso indebido de la infraestructura, entre otras, lo que puede desencadenar una disminución de la productividad e incluso en un cese de operaciones temporal o definitivo por parte de las organizaciones.

Aunque la capacitación y concientización de uso seguro enfocado a los usuarios, sin lugar a duda genera entornos más seguros, no solo basta con enfocarse en un solo lado del panorama, también hay que fortalecer los procesos de seguridad en las organizaciones, en palabras de Juan Carlos Puentes Manager de Fortinet Colombia: "La ciberseguridad pasó de ser un elemento complementario a una necesidad crítica para toda empresa en su proceso de transformación digital (...)". Una manera de fortalecer las organizaciones es mediante la aplicación de estándares de seguridad, ya que estos crean ambientes seguros y generan políticas de gobernanza confiables en relación a las tecnologías de la información, uno de los estándares de seguridad de la información más conocido es el estándar ISO/IEC 27001.

Este estándar se enfoca principalmente en la implementación de un Sistema de Gestión de seguridad de la información, el cual tiene como principal objetivo garantizar la integridad, confidencialidad e integridad de la información en toda la arquitectura de información de una organización. La implementación de esta estándar abarca los siguientes aspectos: liderazgo, planeación, soporte, operaciones, autoevaluación y mejora, contexto organizacional, entre otros. Uno de los fuertes de este estándar es el proceso de evaluación

[16] Compañía de software especializada en ciberseguridad

de rendimiento y mejora, ya que en su metodología de implementación y funcionamiento el estándar incorpora el ciclo PHVA (Planificar, hacer, verifica y actuar), lo cual garantiza la mejora continua mediante procesos de autoevaluación de los procesos y controles de seguridad.

Surge entonces, la necesidad de implementar los Centro de Respuesta a incidentes Cibernéticos, los cuales están conformados por un equipo de personas especializadas y entrenadas para afrontar y resolver los retos que conlleva dar respuesta a un ataque o incidente informático. Hoy en día, dichos especialistas deben contar con capacidades de coordinación, trabajo en equipo, manejo de situaciones de crisis, y lo más importante ser aptos para prevenir, detectar y brindar una respuesta ágil y efectiva con el fin de disminuir los impactos que pueda generar un incidente en la ciberseguridad en la organización.

Un Centro de Respuesta a incidentes Cibernéticos no solamente cumple con responder con rapidez ante los riesgos materializados, de acuerdo con welivesecurity.com, un CSIRT también debe garantizar que después de un incidente se pueda operar con normalidad en el menor tiempo posible y con el menor impacto tolerable; de igual manera, prevenir eventos similares que puedan ocurrir en el futuro; es decir, un CSIRT no solo actúa al momento de la ocurrencia de un incidente si no también antes y después de estos.

Un factor para tener en cuenta a la hora de definir las funciones del Centro de Respuesta a incidentes Cibernéticos es el plan de gestión de seguridad y respuestas a incidentes, este plan de acuerdo con Álvaro Gómez debe contemplar los siguientes aspectos:

- Constitución de un equipo de respuesta a incidentes
- Detección y manejo de los incidentes de seguridad
- Implementación del ciclo de vida de la gestión de incidentes (contención, erradicación, recuperación y actividades post incidente)
- Comunicados y relaciones publicas[17]

Mediante el seguimiento de los aspectos mencionados y la implementación en el plan de gestión y respuesta a incidentes se garantiza que el equipo de respuesta a incidentes cibernéticos actúe de manera efectiva ante los incidentes de seguridad, de esta manera se minimizaran los daños ocasionados y sus efectos colaterales.

El estado de los Centros de Respuesta a Incidentes Informáticos a pesar de lo que indica el índice de Ciber seguridad nacional, ha presentado una buena evolución e implementación, de acuerdo con el reporte de equipos de respuesta a incidentes generado por FIRST[18], en Colombia actualmente existen 17 Centros de Respuesta, resaltando entre ellos CSIRT Asobancaria, CSIRT-ETB, CSIRT-PONAL, SOC-CCOC (Centro de Operaciones de Seguridad de las Fuerzas Militares), COLCERT, entre otros.

4.5. MARCO TECNOLÓGICO

[17] GOMEZ, ALVARO. Gestión de incidentes de seguridad informática. RA-MA Editorial. 2014.
[18] FIRST. Forum of Incident Response and Security Teams [sitio web]. [Consultado: 25 de abril de 2021]. Disponible en: https://www.first.org/members/teams/#colombia

Para dar soporte de un funcionamiento al CSIRT, se requiere una infraestructura tecnológica que sea capaz de garantizar el cumplimiento de las funciones propias de estos equipos de respuesta. Con el fin de permitir un correcto funcionamiento y disminuir los costos de implementación se buscará que toda la infraestructura tecnología este soportada en software gratuito y de código abierto. Una buena referencia en cuanto a tecnología y software es la guía de ENISA "Como crear un CSIRT paso a paso"[19], en donde se establecen una serie de herramientas tecnologías que usan los CSIRT, entre ellas se encuentran:

I. Software de encriptación

II. Herramientas de gestión de incidentes.

III. Herramientas de CRM, las herramientas CRM (Customer Relationship Managemet), es un software de gestión empresa-clientes que permite manejar una gran cantidad de operaciones comerciales e interacciones con los clientes, por lo general este tipo de herramientas son usadas cuando se tiene una gran cantidad de clientes a atender.

IV. Herramientas de verificación de la información, para facilitar el monitoreo de cambios en un entorno web determinado

V. Sistema de detección de intrusos IPS/IDS, El sistema de detección de intrusos (IDS) y el sistema de prevención de intrusos (IPS), son dos mecanismos de seguridad usados para prevenir accesos no autorizados a los sistemas informáticos de una organización, protegiendo así las redes de la organización de amenazas externas provenientes de internet o de terceros, esto se logra mediante la vigilancia de puertos de red y el constante monitoreo del tráfico de la red, de esta manera se logra dar una alerta temprana en caso de un intento de ataque y poner en marcha los mecanismos de defensa informáticos, generalmente estos sistemas funcionan en tiempo real, consideradas herramientas muy útiles para la seguridad de una organización; las que funcionan de la mano con los firewall los cuales bloquean el tráfico no autorizado a los sistemas informáticos

4.6. MARCO LEGAL

El Documento CONPES 3995 del año 2020 denominado Política nacional de confianza y seguridad digital, además de emitir las políticas de seguridad informática y la ruta a seguir en este ámbito se enfoca también en afianzar los ambientes digitales en Colombia, producto de la Cuarta Revolución Industrial y promover el uso de las tecnologías y entornos digitales mediante el aumento de los índices de confianza y seguridad digital.
Resolución 093 del 11 de febrero de 2019. "Por la cual se delegan unas funciones, se conforman unos comités y se dictan otras disposiciones". Capítulo Tercero: Equipo de respuesta a incidentes de seguridad de la Información. Art. 77. Se establece como órgano consultivo del Comité de Seguridad de la información, el CSIRT, sus miembros son: la

[19] ENISA. Como crear un CSIRT paso a paso. En: Herramientas disponible para CSIRT. ENISA, 2006. p. 55.

jefatura para la protección presidencial del Departamento Administrativo de la Presidencia de la Republica

Ley 1928 del 24 de julio de 2018. “Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest”. El delito electrónico, se ha expandido, en todo el mundo, a tal punto, que, en el año 2001, en la comunidad europea (UE), se reunieron varios Estados miembros, en la ciudad de Budapest (Hungría), con el fin de crear una herramienta jurídica, contra este comportamiento ilegal. Así, nace, “El Convenio de Budapest sobre la Cibercriminalidad de 2001.” Desde luego, este, ha sido, ratificado, por varios Estados, entre ellos, Colombia, en el año 2018, mediante la ley 1928

Documento CONPES 3854 de 2016. “Política Nacional de Seguridad Digital”, mediante el cual se incorpora la gestión de riesgo como uno de los pilares fundamentales de la seguridad digital en Colombia. Cuyo fin, es que la Dirección de Seguridad de la Presidencia de la República asuma las actividades de coordinación y articulación de las políticas de seguridad en el país, de conformidad con las funciones propias de la citada dependencia.

Documento CONPES 3701 de 2011. “Lineamientos de política para ciberseguridad y ciberdefensa”, mediante el cual se asigna el presupuesto para la creación de estrategias para contrarrestar las amenazas informáticas en Colombia. Documento que define un plan de acción para la ejecución de la política en ciberseguridad y ciberdefensa, el cual estará a cargo de las entidades involucradas. cibernética contra la población, el territorio y la organización política del Estado.

Ley Estatutaria 1581 de 2012 de protección de datos personales que hace referencia a aspectos clave como la recolección, uso, transferencia, divulgación no autorizada, actualización, confirmación de la veracidad y eliminación de datos personales

LEY 1273 DE 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de los tipos penales.

5. DISEÑO METODOLÓGICO

Para el desarrollo de este proyecto se utilizará una metodología de tipo documental-descriptiva, se desarrollará en la descripción del diseño de un CSRIT en el que se incluyen procedimientos, métodos, técnicas y estructuras necesarias para el funcionamiento; de igual, manera se usará la investigación documental o bibliográfica, tomando las publicaciones existentes y realizadas por INCIBE, ENISA y FIRST los cuales son referentes mundiales sobre la implementación y funcionamiento de los CSIRT.

La metodología usada para este proyecto (documental-descriptiva), tendrá un enfoque cuantitativo, ya que, mediante la recopilación de estadísticas, mediciones y datos recolectados sobre incidentes, amenazas, riesgos en las organizaciones tanto regionales como a nivel mundial, se efectuará un estudio para determinar la mejor manera de documental el diseño de un CSIRT.

Como técnica de recolección y principal fuente de información se hará uso de la revisión documental, ya que, a partir de los estudios previamente realizados por diferentes organizaciones y autores a nivel mundial, se determinará las necesidades y procedimientos para elaborar el marco de trabajo objeto de este proyecto y poder brindar como producto final un marco de trabajo con políticas y procedimientos alineados al panorama tecnológico y de seguridad informática actual.

Así mismo, se vincularan los procesos metodológicos con la norma ISO 27001, teniendo en cuenta que es uno de los estándares del ámbito de la seguridad de la información más conocidos a nivel mundial, la que ha sido homologado por el ICONTEC y adoptado como una norma técnica colombiana; la pertinencia radica en que es un estándar enfocado en seguridad de la información y se encuentra relacionado con una de las finalidades de este trabajo de grado, la cual es, mejorar las arquitecturas de seguridad en las instituciones y lograr la protección y seguridad de los activos de información.

6. DESARROLLO DE LOS OBJETIVOS

6.1. ESTABLECER LOS PROCEDIMIENTOS Y POLÍTICAS DE SEGURIDAD NECESARIAS PARA LA IMPLEMENTACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES INFORMATIVOS

Con el fin de efectuar una implementación optima de un CSIRT, es necesario comprender y conocer el marco de trabajo básico de un CSIRT. La especificación del entorno busca dar respuesta a una serie de preguntas básicas: qué, para quién, en dónde y con quienes, las cuales traducidas a un nivel organizacional nos permite establecer que el marco de trabajo del CSIRT está conformado por:

- Misión: establece las metas objetivos y prioridades.
- Alcance: establece la comunidad objetivo y los modelos de relación.
- Lugar en la organización: establece niveles de jerarquía y prioridades dentro de un esquema organizacional.
- Relación con otros CSIRT: relaciones de cooperación y coordinación con otros CSIRT.

6.1.1 Misión

La misión del CSIRT, es uno de los aspectos más importantes a definir, ya que es el punto de partida; es donde se establece el propósito y hacia donde está enfocado el funcionamiento del CSIRT. Una misión definida y fundamentada, permitirá a la organización del CSIRT un desarrollo óptimo del marco de trabajo mediante la definición clara metas y objetivos, por ejemplo, recuperación de sistemas, análisis de ataques, punto de coordinación e información, entre otras.

Una definición clara y precisa de la misión del CSIRT permitirá establecer también la comunidad objetivo y los servicios necesarios para cumplir con el objetivo funcional del equipo, así como también la naturaleza y el enfoque del CSIRT.

Un ejemplo claro de misión es la definida por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT, en donde se establece lo siguiente:

Cuadro 1. Misión ColCERT

Misión ColCERT	El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.[20]

Fuente: ColCERT. Acerca de [sitio web]. [Consultado: 05 de mayo de 2021]. Disponible en: http://www.colcert.gov.co/?q=acerca-de

[20] ColCERT. Acerca de: Nuestra Misión [sitio web]. [Consultado: 05 de mayo de 2021]. Disponible en: http://www.colcert.gov.co/?q=acerca-de

En esta misión se pueden establecer factores como responsabilidad principal (Ciberseguridad y Ciberdefensa Nacional), propósito (coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado), y se puede inferir el tipo de CSIRT (CSIRT de infraestructura critica), también se pueden evidenciar otros factores como el marco legal (Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional).

6.1.2 Alcance

Dentro de esta etapa se definirá la comunidad objetivo y el tipo de CSIRT a implementar con base a la misión ya definida. Cuando se habla de comunidad objetivo, se refiere a la organización o institución a la cual el CSIRT prestará los servicios, en otras pablaras esta comunidad corresponde al sector o población hacia la cual están orientados los servicios del CSIRT.

Es necesario definir con exactitud la comunidad objetivo, ya que dependiendo del enfoque de las organizaciones y su ámbito de desempeño (académico, militar, comercial, etc.) se definirá que tipo de CSIRT se implementará y que servicios serán necesarios implementar, con el fin de garantizar la protección y seguridad de las infraestructuras tecnologías de la organización.

De acuerdo con ENISA[21], se establecen los siguientes tipos de CSIRT clasificados por sectores:

- CSIRT del sector académico, clientes atendidos: estudiantes
- CSIRT comercial, clientes atendidos: clientes que pagan por ello
- CSIRT del sector de la protección de la información vital y de la información y las infraestructuras vitales (CIP/CIIP), clientes atendidos: empresas de TI
- CSIRT del sector público, clientes atendidos: organizaciones gubernamentales
- CSIRT interno, clientes atendidos: personal de TI que pertenece a la empresa propietaria del CSIRT
- CSIRT del sector militar, clientes atendidos: instituciones militares
- CSIRT nacional, clientes atendidos: país en el que se encuentra ubicado, cumple funciones de coordinación y de punto de contacto a nivel internacional en asuntos de ciberseguridad
- CSIRT del sector de la pequeña y mediana empresa (PYME), clientes atendidos: Pymes y su personal
- CSIRT de soporte, clientes atendidos: propietarios de productos o fabricantes de productos específicos, por ejemplo, HP CSIRT y Adobe PSIRT.

Una vez definido el alcance del CSIRT de acuerdo con la naturaleza de la comunidad objetivo, se debe determinar con base a ello el modelo de relación y autoridad con la comunidad, de esta forma se establecerá el nivel de autonomía con respecto a la aplicación de procedimientos y servicios, es decir, si los servicios del CSIRT entrarán en funcionamiento de forma autónoma o por decisión de la comunidad objetivo. De acuerdo

[21] ENISA, Óp. cit., p. 8.

con el Centro Criptológico Nacional[22] los modelos de autoridad se clasifican de la siguiente manera:

- Autoridad completa: el CSIRT efectuará todas las acciones y procedimientos con respecto a gestión de incidentes de manera autónoma.
- Autoridad compartida: la gestión de incidentes y la toma de decisiones se hace de manera conjunta entre el CSIRT y el equipo de TI de la organización.
- Autoridad nula: el CSIRT actúa únicamente como asesor y fuente de información, no cuenta con atribuciones al momento de toma de decisiones.
- Autoridad indirecta: el CSIRT no tiene autoridad sobre la comunidad, pero tiene la posibilidad de influenciar sobre la toma de decisiones.

6.1.3 Lugar en la organización

Al momento de hablar del lugar en la organización que tomará el CSIRT, no solamente se habla de en qué lugar físico estará ubicado, sino también de a que dependencias estará ligado y que papel desempeñará en la seguridad de la organización.

Uno de los factores decisivos al determinar el lugar en la organización del CSIRT será la misión y el alcance, por ejemplo, un CSIRT que tenga como misión velar por la seguridad y protección de toda la infraestructura tecnológica de la compañía, teniendo como eje fundamental la respuesta a incidentes y la mejora e implementación de sistemas de seguridad que permitan la mitigación de riesgos y reducción de los daños colaterales causados por un incidente de seguridad, tendrá un lugar principal en la estructura organizacional, en donde estará a cargo de todo el sistema de seguridad informático que disponga la compañía o el cliente a atender.

Otro factor que ayuda a determinar el lugar en la organización del CSIRT es el alcance, este servirá como criterio para determinar otros factores tales como si dependerá de otra departamento o si será autónomo, por ejemplo, si se determina que el modelo a adoptar por el CSIRT es un modelo de autoridad completa; se recomienda que el CSIRT sea estructurado en una dependencia totalmente independiente, lo cual permitirá autonomía total en las decisiones, por otro lado, si se determina que el CSIRT tiene una autonomía compartida o más aún si el alcance determina que el equipo será de soporte o interno, se podría establecer que hará parte de otra dependencia afín al alcance, por ejemplo el departamento de TI.

Es importante aclarar que sin importar el lugar donde se desarrollara la organización del CSIRT, este debe trabajar en cooperación con las demás dependencias, en especial con la sección encargada de las tecnologías de la información, de esta manera se podrán establecer relaciones de cooperación y soporte mutuo, e incluso establecer parámetros de atención, por ejemplo, si se trata de un evento de seguridad aislado, tal como un malware que afecte solo una terminal, se puede determinar que el departamento de TI atienda este tipo de eventos y establecer que el CSIRT se hará cargo de eventos de mayor escala, como afectaciones a sistemas críticos de la organización.

[22] CENTRO CRIPTOLÓGICO NACIONAL. Guía de Creación de un CERT/CSIRT. España: Editor y Centro Criptológico Nacional. 2011. p. 23.

6.1.4 Relaciones con otros CSIRT

Las relaciones de cooperación y coordinación con otros CSIRT, juegan un papel muy importante en el funcionamiento de estos centros, ya que, una adecuada coordinación entre equipos puede ayudar a mitigar y a manejar un incidente de manera eficaz, adicionalmente una relación de cooperación y coordinación ayuda a complementar el trabajo de un CSIRT mediante el fortalecimiento de los canales de comunicación, lo que nos permitirá conocer el ecosistema de los CSIRT que los rodean. Por ejemplo, en Colombia existe el CSIRT financiero liderado por Asobancaria el cual es el encargado de todo el sector financiero, por tal motivo, los CSIRT de entidades financieras tendrán como primer punto de contacto el CSIRT liderado por Asobancaria, de igual manera los CSIRT de las Fuerzas Militares tienen como primer punto de contacto el Centro de Operaciones de Seguridad de las Fuerzas Militares.

De lo observado en los ejemplos mencionados anteriormente, se puede concluir que hay CSIRT que funcionan como puntos de contacto, los cuales a su vez puede funcionar como centros de coordinación entre CSIRT. Este tipo de relaciones CSIRT-Centro de coordinación, no significa que los CSIRT estén restringidos a comunicarse con otros centros mediante el centro de coordinación, también se puede establecer comunicación de manera directa, en especial cuando se trate de temas que requieran solución en poco tiempo o asesoría directa, sin embargo, se debe informar los centros de coordinación con el fin de que hagan un seguimiento al incidente que se esté tratando y si es el caso generar alertas a otros centros de coordinación y CSIRT.

6.1.5 Estructuras organizacionales

De acuerdo con la Organización de los Estados Americanos[23] la organización de un CSIRT está clasificada en cuatro estructuras principales, Equipo de seguridad localizada, Equipos de respuesta a incidentes distribuidos, Equipo de respuesta a incidentes centralizado y Equipo coordinador.

6.1.5.1 Equipo de seguridad localizada

Es la estructura CSIRT más sencilla, en donde los eventos de seguridad son resueltos por el personal de las organizaciones, los cuales no necesariamente son expertos en respuesta a incidentes o gestión de riesgos, pero cuentan con el conocimiento de la infraestructura TI de la organización, lo que les permite resolver un incidente, mas no, determinar la naturaleza y origen de este mismo, lo que causa una brecha de seguridad, puesto que el desconocimiento de la causa del evento no permite la aplicación de soluciones oportunas ni la aplicación de buenas prácticas de seguridad por lo que la vulnerabilidad queda expuesta a ser explotada por un atacante. Por lo general este tipo de estructura se usa en organizaciones pequeñas en donde el capital no es suficiente, no para implementar una estructura más robusta, sino para crear un sistema de respuesta de incidentes informáticos que sea exclusivo para esto.

[23] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSRIT nacional. Washington D.C: Secretaría General de la Organización de los Estados Americanos (OEA). 2016. P. 45

6.1.5.2 Equipo de respuesta a incidentes centralizado

En este tipo de estructura CSIRT, el equipo de respuesta cuenta con su propio personal y estos se encuentran especializados en el manejo de eventos e incidentes de seguridad informática; en este tipo de estructura solo existe un equipo encargado de la gestión y respuesta de todos los incidentes de seguridad, por lo general este tipo de configuración organizacional es usada en las grandes corporaciones cuya infraestructura TI se encuentra centralizada en una sola locación.

6.1.5.3 Equipo de respuesta a incidentes distribuidos

Este es el tipo de estructura CSIRT aplicable a grandes organizaciones cuya infraestructura tecnológica se encuentra distribuida en diferentes locaciones, este tipo de estructura se conforma de varios CSIRT en donde uno de estos hace las veces de centro de coordinación, el alcance del CSIRT dependerá de la locación en donde se encuentre y el sector de la organización al que le ofrecerá sus servicios, permitiendo de esta forma la creación de CSIRTs especializados en una misma organización.

6.1.5.4 Equipo coordinador

Cumple funciones similares a las del Equipo de respuesta distribuido, la diferencia radica en que el Equipo coordinador no efectuará funciones de coordinación dentro de una misma organización, sino que es el encargado de efectuar labores de coordinación entre diferentes centros de respuesta de organizaciones diferentes.

Ahora bien, teniendo en cuenta los diferentes tipos de estructura CSIRT propuestos por la Organización de Estados Americanos, se debe elegir un tipo de estructura acorde al tamaño de la organización en la cual se implementará el CSIRT, para ello se deben tener en cuenta ciertos aspectos como:

1. Ubicación.
2. Tamaño de la comunidad objetivo.
3. Distribución geográfica.
4. Servicios para ofrecer[24].

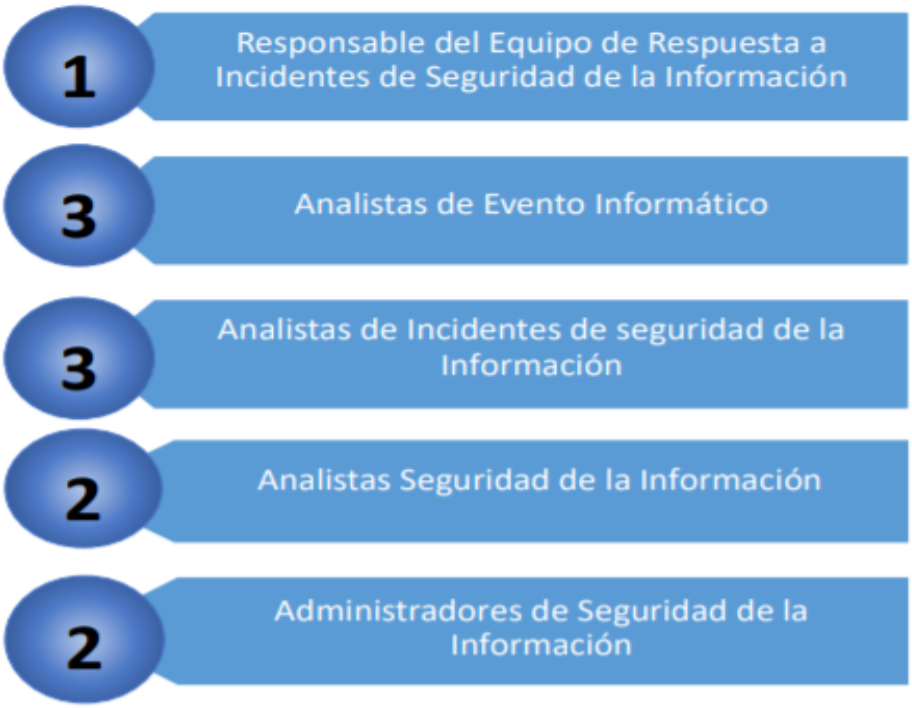
6.1.6 Equipo de trabajo

En la Figura 1 se puede identificar la composición ideal del equipo de un CSIRT el cual es encuentra alineado con las recomendaciones gubernamentales en Colombia sobre los lineamientos del equipo de repuesta a incidentes de seguridad de la información[25]

[24] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSRIT nacional. En: Tamaño de la organización. Washington D.C: Secretaría General de la Organización de los Estados Americanos (OEA). 2016. p. 47

[25] PRESIDENCIA DE LA REPUBLICA. Lineamientos Del Equipo De Respuesta A Incidentes De Seguridad De La Información. En: Cantidad ideal de personas para la conformación del equipo. Colombia. 2019. p. 7

Figura 1. Cantidad ideal de personas para la conformación del equipo.



Fuente: PRESIDENCIA DE LA REPUBLICA. Lineamientos Del Equipo De Respuesta A Incidentes De Seguridad De La Información. En: Cantidad ideal de personas para la conformación del equipo. Colombia. 2019

6.1.7 Estructura Organizacional Mínima del CSIRT

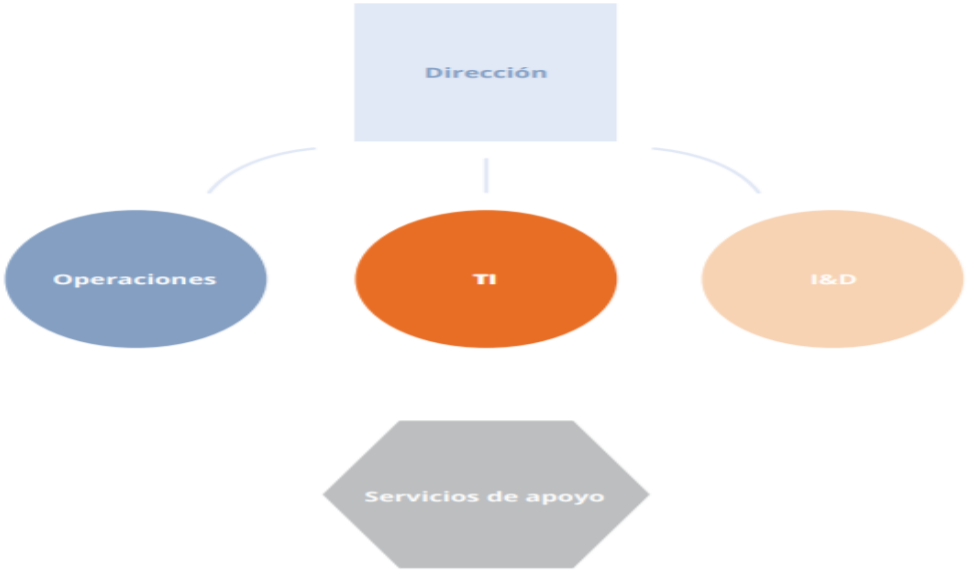
Un buen punto de partida para determinar la estructura mínima organizacional de un CSIRT es la definida por la Organización de los Estados Americanos[26], la cual plantea una estructura organizacional que permite la expansión de la organización conforme avanza el tiempo y la organización crece, en este modelo cada sección es la encargada de ciertas tareas específicas.

Como se puede apreciar en la Figura 2, el CSIRT estaría encabezado por la dirección, quienes son los encargados de la administración estratégica del equipo, así como también de todas las tareas de supervisión, gestión financiera y coordinación con otros CSIRT, el área de operaciones se podría decir que es el corazón del CSIRT, es aquí donde se realiza todo lo relacionado con monitoreo, análisis, gestión de incidentes, etc., la sección de TI es la encargada de implementar y gestionar todos los sistemas (hardware y software) necesarios para el funcionamiento de la infraestructura tecnológica de la organización y el funcionamiento del CSIRT y por último, la sección de Investigación y Desarrollo (I&D), es el área del CSIRT encargada de desarrollo de herramientas que permitan un mejor funcionamiento del CSIRT, desarrollo de cursos de capacitación, investigación de

[26] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Óp. cit. p. 51

tendencias, amenazas, ataques y demás estudios relacionados con el área de seguridad informática.

Figura 2. Estructura Mínima Organizacional



Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas Prácticas para establecer un CSRIT nacional. En: Tamaño de la organización. Washington D.C: secretaria general de la Organización de los Estados Americanos (OEA). 2016. P. 51

6.1.8 Políticas y procedimientos

Una vez establecida la misión, el alcance y los servicios necesarios de acuerdo con la naturaleza del CSIRT y las necesidades del cliente, se cuenta con los aspectos más básicos para poder determinar una idea sobre el funcionamiento y el enfoque del equipo, el siguiente paso es establecer las políticas y procedimientos para la operación del CSIRT, estas describirán más a fondo las directrices en las que tienen que estar enmarcadas todas las operaciones que efectúen el CSIRT.

Al momento de definir las políticas de seguridad, es necesario tener en cuenta ciertos aspectos, con el fin de encontrarse alineados con la misión, objetivos y metas de la organización, entre estos aspectos se encuentra:

1. Alcance
2. Objetivos y prioridades en tema de seguridad
3. Compromiso y apoyo de la alta gerencia
4. Clasificación de los activos de información
5. Análisis y gestión de riesgos e incidentes
6. Roles y responsabilidades de seguridad
7. Normas y procedimientos de seguridad a implementar
8. Plan de continuidad de negocio

Una buena referencia para establecer las políticas y procedimientos de un CSIRT, la establece FIRST[27], el cual establece un requisito de políticas obligatorias mínimas que garantizan una estandarización con los parámetros establecidos por FIRST como ente de referencia mundial para los CSIRT que desean ser miembros de dicha organización, estas políticas mínimas obligatorias son:

1. Política de clasificación de información: en esta política se debe detallar la categorización o clasificación de la información.
2. Política de protección de datos: esta política debe describir como diferente información clasificada es protegida en su almacenamiento, transito, acceso, entre otras.
3. Política de destrucción de información: esta política detalla como la información es destruida de acuerdo con su clasificación.
4. Política de divulgación de información: esta política establece que información puede ser divulgada en grupos internos y externos.
5. Política sobre el acceso a la información: esta política establece que tipo y clasificación de la información puede ser accedida por los miembros del CSIRT, clientes o entidades externas.
6. Políticas de uso apropiado de los sistemas CSIRT: establece como el grupo de trabajo del CSIRT debe usar el equipamiento y sistemas del CSIRT en el uso diario.
7. Definición de incidentes de seguridad y política de eventos: determina los criterios de como evaluar un reporte y determinar si es un incidente y su categoría.
8. Gestión de incidentes: define quien tiene la responsabilidad de la gestión del incidente y la forma en que será gestionado.
9. Política de cooperación: define el proceso de como el CSIRT contribuye con otros equipos de respuesta a incidentes informáticos.

De acuerdo con Moira West-Brown[28], las políticas no son un conjunto detallado de procedimientos, si no, son un conjunto de directrices que establecen ciertos parámetros a cumplir al momento de efectuar en relación a determinada actividad

6.1.8.1 Política de clasificación de información

Con el fin poder efectuar una adecuada clasificación de la información y poder brindar seguridad y protección, la organización debe tener pleno conocimiento de todos los activos de información con los que cuenta o el grupo objetivo que atenderá el CSIRT, para ello se debe efectuar un inventario de los activos de información, esto no solo permitirá al CSIRT tener el conocimiento de los activos de la organización, si no que permitirá clasificar e identificar aquellos activos que requieren un mayor enfoque debido a sus características y roles al interior de la organización, esto a su vez permitirá la identificación de prioridades de atención en caso de un incidente informático.

[27] FIRST. FIRST Site Visit Requirements and Assessment. rev 3.1. 2020. p. 5.
[28] WEST-BROWN, Moira, et al. Handbook for Computer Security Incident Response Teams (CSIRTs). 2 ed. Pittsburgh, PA: Carnegie Mellon University. 2003. p. 38.

Una buena guía para efectuar la identificación e inventario de activos es la Guía para la Gestión y Clasificación de Activos de Información[29] propuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia en donde el inventario se hace de la siguiente manera:

1. El primer paso es definir los activos de información que harán parte del inventario para ello se debe obtener la información básica de los activos mediante la descripción de características como identificador, nombre del activo, clasificación, descripción, tipo (información, software, servicio, etc.), ubicación, criticidad, propiedad, entre otros
2. Posteriormente se debe efectuar una revisión de los activos de información con el fin de determinar si estos han tenido algún cambio o si ya no hacen parte del inventario, este procedimiento puede ser efectuado cada vez que sea requerido
3. En caso de que sean necesario hacer cambios, se debe hacer la actualización del inventario de activos de información
4. Una vez efectuados los cambios requeridos e identificados los activos de información se debe hacer la publicación del inventario como documento confidencial, de manera que solo se permita el acceso a usuarios autorizados

Uno de los aspectos para tener en cuenta al momento de efectuar el inventario de activos de información es la clasificación de estos, esta distribución se hace con el fin de garantizar los niveles de protección y acceso necesarios basado en el valor y la importancia del activo en la organización. Al momento de efectuar la clasificación de los activos de información se deben tener en cuenta tres aspectos fundamentales de la seguridad de la información, confidencialidad, integridad y disponibilidad.

Cuando se habla de confidencialidad se refiere a que la información esté protegida con respecto al acceso de todos los usuarios no autorizados; la integridad, se refiere a que los activos permanezcan inalterados e inmutables ante intentos de modificación no autorizados, por último, la disponibilidad, hace referencia a que los activos estén siempre accesibles cuando sean requeridos por una persona autorizad. Basado en estos tres aspectos y alineado con la gestión de activos mencionada en la ISO27001:2013, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia[30] propone la siguiente clasificación de los activos de información:

Cuadro 2. Esquema de clasificación por confidencialidad

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma.

[29] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Activos de Información. 2016.
[30] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Óp. cit. p. 16

Cuadro 2. Continuación

INFORMACION PUBLICA CLASIFICADA	Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Activos de Información. 2016. p. 16.

Cuadro 3. Esquema de clasificación por integridad

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Activos de Información. 2016. p. 17.

Cuadro 4. Esquema de clasificación por disponibilidad

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Activos de Información. 2016. p. 17.

6.1.8.2 Política de protección de datos

El CSIRT, se hará responsable por el tratamiento y protección de los datos personales a los cuales tenga acceso durante el desarrollo de todas las actividades propias de su funcionamiento; así mismo, esta información será usada, procesada y distribuida únicamente a los entes involucrados en el proceso de protección y seguridad informática que cuenten con los permisos de acceso; en ningún caso, esta información será difundida a terceros. Por lo anterior, se tomarán todas las medidas necesarias para garantizar una adecuada confidencialidad y preservación de la información de acuerdo con lo establecido en la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.”.

El CSIRT tendrá autorización para tratar, manipular, procesar, almacenar y transmitir según se requiera los datos, siempre actuando bajo el marco de lo establecido en la ley 1581 de 2012, por tal motivo se autoriza al CSIRT proveer los datos personales y demás datos procesados a terceros siempre y cuando se cumpla con uno de estos fines:

A. Dar repuestas a peticiones, quejas y recursos
B. Dar respuesta a organismos de control y autoridades competentes
C. Dar respuesta a requerimientos a terceros con los cuales el CSIRT haya suscrito acuerdos de cooperación mutua
D. Brindar asistencias a incidentes, eventos y cualquier situación en donde se vea comprometida la seguridad de los activos de información

De igual manera como titular de los datos personales, se tiene derecho a:

A. Conocer la información que ha sido objeto de tratamiento, procesamiento o manipulación
B. Actualizar información frente a los datos personales que se encuentre incorrecta o que induzca al error a cualquier ente.
C. Solicitar la eliminación de datos cuando no se hayan cumplido los derechos legales y constitucionales, así como lo establecido en la normatividad vigente.
D. Identificar el responsable por el tratamiento de sus datos

6.1.8.3 Política de destrucción de la información

Esta política tiene como fin garantizar que toda la información almacenada en los equipos, medios digitales y físicos sea destruida de forma correcta al final de su ciclo de vida, para ello se deben emplear ciertos procedimientos de destrucción con el fin de evitar que la información caiga en manos de terceros, en especial si se trata de información crítica.

Una vez se determine la información a destruir se debe efectuar un registro que permita identificar la información almacenada y el responsable de este, con el fin de efectuar un debido control del ciclo de vida y adecuada destrucción de la información, así como también para tener un registro histórico de la información destruida en caso de llegar a necesitarse.

Entre los medios de destrucción más usados se encuentran:

A. Desmagnetización: mecanismo que consiste en aplicar un campo magnético sobre medios de almacenamiento como discos duros, disquetes, cintas magnéticas, etc., lo cual elimina de forma permanente los datos eliminados en el dispositivo.
B. Destrucción física: consiste en el uso de diferentes mecanismos tales como trituración, incineración, desintegración, etc., para efectuar la destrucción física de los medios de almacenamiento, de esta forma se efectúa una destrucción permanente que inutiliza el medio de almacenamiento, es útil para destruir información alojada en CD y papel
C. Sobre escritura: consiste en la escritura de nuevos datos sobre los datos almacenados en el dispositivo de almacenamiento, para ello se debe efectuar una sobreescritura total del dispositivo de almacenamiento, se usa para destrucción de información alojada en discos duros y unidades de almacenamiento extraíbles

6.1.8.4 Política de divulgación de la información

La política de divulgación de la información, tiene como objetivo permitir la divulgación de la información pública a los entes que lo requieran de manera oportuna, clara y amplia, así como también garantiza que la información que tenga un nivel de clasificación superior a publica permanezca de forma confidencial y sin divulgación.

La divulgación de la información estará a cargo por parte del vocero de la organización y toda la información que se vaya a divulgar debe estar bajo la autorización del comité de divulgación, el cual estará conformado por el gerente de la organización, el equipo de seguridad de la información de la organización y el CSIRT.

Todas las solicitudes tramitadas por terceros, deben centralizarse y ser tramitadas por la oficina de comunicaciones o quien haga sus veces en la organización, y se debe informar inmediatamente a la gerencia y al CSIRT con el fin de verificar los niveles de clasificación y que tan oportuno es la divulgación de la información solicitada.

Siempre que se requiera divulgar una información ya sea por iniciativa propia, solicitud de terceros o requerimientos de las autoridades pertinentes se debe cumplir con los siguientes puntos de control:

A. Identificación de la normativa aplicable en cuanto a divulgación de información
B. Únicamente puede ser divulgada a terceros la información con nivel de público, salvo casos en donde se requiera el acceso a información reservada o clasificada debido al adelantamiento de procesos legales y cuando la ley así lo estipule
C. Identificación de los responsables de recopilar y preparar los comunicados
D. Verificar que el comité de divulgación apruebe la solicitud de divulgación de la información
E. Difundir información únicamente por medios y por personas autorizadas

De igual manera se deben tener en cuenta los siguientes aspectos:

- Está prohibida la difusión, divulgación o publicación de información confidencial o propiedad de la organización.

- Se deben establecer unos medios de información oficiales ya sea blogs, páginas webs, chats, redes sociales, etc.
- Cada vez que se difunda una información o se efectúe alguna publicación esta debe contar con los logotipos de identificación de la organización, un numero de control, autor de la publicación y firma del vocero de la organización o quien haga sus veces.
- Se debe verificar cual es el nivel máximo de clasificación de la información que se puede divulgar, en caso de que la organización sea de tipo publica se debe regir por lo estipulado en la ley 1715 de 2014.
- No discutir asuntos confidenciales por medios no oficiales o en lugares donde terceros puedan acceder a la información.
- No enviar información reservada o clasificada por medios electrónicos no seguros
- Se deben crear niveles del manejo de la información con el fin de que al interior de la organización la información reservada o clasificada sea manejada únicamente por personal autorizado

En caso de que se determine que se emitió un comunicado o publicación con información errónea o falsa, el comité de divulgación debe tomar acciones inmediatas con el fin de efectuar la respectiva rectificación y notificar inmediatamente a la gerencia de la organización. En el caso de que haya autoridades competentes involucradas se les debe notificar a estas mismas, con el fin de evitar inducir al error en algún tipo de proceso y que se genere alguna acción legal contra la organización.

Otro aspecto a tener en cuenta son los rumores, la organización debe tomar una postura respecto a estos y determinar si se efectuará una aclaración de estos o si hará caso omiso a las especulaciones, de igual manera, será el comité de divulgación quien defina la política en cuanto a estas situaciones

6.1.8.5 Política sobre el acceso a la información

La organización/CSIRT es la dueña de todos los sistemas informáticos y la información que estos procesan, almacenan, modifican y generan, por tal motivo se debe garantizar unos adecuados controles de acceso a todos los sistemas informáticos de la organización, esto con el fin de evitar accesos no autorizados a los sistemas y por ende a la información contenida. Para ello la organización/CSIRT debe implementar sistemas o controles de seguridad de acceso para los usuarios que, mediante mecanismos de identificación y control, garanticen que un usuario solo podrá acceder a la información de acuerdo a los niveles de autorización que tenga, de igual manera este proceso debe ir acompañado de campañas o planes de concientización con el fin de que los usuarios comprendan la importancia de la información y la responsabilidad que se debe tener frente al manejo de esta misma.

El responsable de esta política será el oficial de seguridad de la información de la organización o quien haga sus veces, este debe velar por el cumplimiento de todos los procedimientos, mecanismos y medidas que se tomen con el fin de controlar el acceso a los sistemas informáticos de la organización, tales como bases de datos, sistemas de almacenamiento, computadores, acceso a redes, etc. Asimismo, el oficial de seguridad de la información debe efectuar controles de calidad o auditorías a los mecanismos

implementados con el fin de evaluar la efectividad de los controles de acceso implementados.

Con el fin de contribuir a un fácil desarrollo de los procedimientos que apoyaran esta política se debe tener en cuenta lo siguiente:

- Efectuar un adecuado inventario y clasificación de la información
- Determinar que controles, procedimientos y medidas para controlar el acceso a la información se implementaran en la organización
- Diseñar e implementar un sistema de control de privilegios de usuarios
- Efectuar controles periódicos a los privilegios de usuarios

6.1.8.6 Políticas de uso apropiado de los sistemas CSIRT

Esta política es de obligatorio cumplimiento para todos los usuarios de la organización, así como también para todas las entidades o terceros que interactúen o hagan uso de los servicios ofrecidos por el CSIRT. Esta política se desarrolla con el fin de optimizar y mejorar la calidad de los servicios brindador por el CSIRT y conseguir una mejora en todos los procesos internos e implementación de todos los mecanismos necesarios para brindar servicios de calidad y garantizar en todo momento la seguridad y protección de la información alojada en los sistemas del CSIRT.

Para tal fin se hace necesario establecer políticas de uso apropiado de los sistemas del CSIRT, las cuales tendrán como objetivo el uso seguro y eficaz de todos los sistemas y herramientas disponibles.

Las políticas de uso apropiado de los sistemas CSIRT son:

- Se hará uso de los sistemas CSIRT únicamente para actividades relacionadas con la gestión de incidentes o la prestación de alguno de los servicios brindados por el CSIRT, ya sean reactivos, proactivos o de gestión de la calidad
- Los sistemas CSIRT serán usados únicamente por personal debidamente calificado y autorizado para su uso
- Se deben respetar los derechos de autor en todos los aplicativos, información y demás accedidas mediante los sistemas CSIRT
- Se deben cumplir con todas las normas de seguridad informática establecidas por la organización
- Está prohibido el uso de los sistemas CSIRT utilizando una cuenta de un tercero o ejecutando cualquier mecanismo de modificación de privilegios de acceso
- La violación de las normas de seguridad informáticas y las establecidas por esta política constituye una violación de los parámetros de seguridad de la organización, lo cual conllevara a la cancelación de cuentas, terminación inmediata del vínculo laboral y se aplicara lo establecido por las leyes en Colombia
- El acceso a internet está permitido siempre y cuando sea para el cumplimiento de la misión del CSIRT y las tareas derivadas de ello y no para actividades personales
- El uso de cuentas debidamente autenticadas no exime de ser auditado por personal de seguridad

- Todo software en uso debe tener sus respectivas licencias vigentes, de igual manera el único personal autorizado para efectuar instalación de software serán los administradores de los sistemas de información
- El CSIRT es el responsable de establecer los mecanismos de asignación de cuentas, administración de contraseñas, permisos de acceso, etc.
- El CSIRT podrá auditar cualquier actividad desarrollada en los sistemas de este mismo

6.1.8.7 Definición de incidentes de seguridad y política de eventos

De acuerdo al glosario de definiciones de NIST, un incidente de seguridad se define como un evento que pone en peligro la confidencialidad, integridad o disponibilidad de la información o de un sistema de información, o bien un evento que constituye una violación o amenaza inminente de violación de la ley, políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

Como se puede observar, en la definición de incidentes de seguridad no se establece un alcance o una clasificación, lo cual se hace necesario al momento de determinar si es un incidente o no, y como se clasificaría. Para ello el CSIRT[31] desarrolló una taxonomía de clasificación de los incidentes, el cual será útil en el proceso de gestión y atención de incidentes informáticos, tal como se observa en el cuadro 5.

Cuadro 5. Clasificación de incidentes

Incident Class*ification*	**Incident *Examples***	**Description / *Explanation***
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a *functionally comparable* content.
	Harmful Speech	Discreditation or discrimination of somebody (e.g., cyber stalking, *racism and threats against one or more individuals*)
Abusive Content	Child/Sexual/ Violence/...	Child Pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
	Rootkit	

[31] eCSIRT es un proyecto fundado por la comunidad europea de CSIRT, se enfoca en el desarrollo e implementación de nuevas técnicas y prácticas para mejorar la cooperación entre equipos de respuesta.

Cuadro 5. Continuación.

Incident Class*ification*	**Incident *Examples***	**Description / *Explanation***
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingered, DNS querying, ICMP, SMTP (EXPN, RCPT, …), *port scanning*.
	Sniffing	Observing and recording of network traffic (wiretapping).
Information Gathering	Social Engineering	Gathering information from a human being in a non--technical way (e.g., lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting of known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardized identifier such as CVE name (e.g., buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged Account Compromise	A successful compromise of a system or application (service). This can have been caused remot*ely* by a known or new vulnerability, but also by an unauthorized local access. *Also includes being part of a botnet.*
	Unprivileged Account Compromise	
	Application Compromise	
	Bot	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. *DoS examples are ICMP and SYN floods, Teardrop attacks and mail--bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks.* However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) *– or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.*
	DDoS	
	Sabotage	
Information *Content* Security	Unauthorized access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). *Human/configuration/software error can also be the cause.*
	Unauthorized modification of information	

Cuadro 5. Continuación.

Incident Class*ification*	**Incident *Examples***	**Description / *Explanation***
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit--making ventures (E.g., the use of e--mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	*Offering* or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
Fraud	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	*Masquerading as another entity in order to persuade the user to reveal a private credential.*
Vulnerable	*Open for abuse*	*Open resolvers, world readable printers, vulnerability apparent from Nessus etc. scans, virus signatures not up--to--date, etc.*
Other	All incidents which don't fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	*Meant for testing*	*Meant for testing*

Fuente: STIKVOORT, Don. Incident Classification / Incident Taxonomy according to eCSIRT.net – adapted.2015.

6.1.8.8 Gestión de incidentes

El CSIRT será el encargado de todo el proceso de gestión de incidentes, para ello hará uso de todos los recursos disponibles en el momento, siendo prioridad en todas las operaciones de protección y seguridad efectuadas, teniendo como fin salvaguardar los sistemas informáticos y los activos de información que estos almacenan, procesan y producen, para ello el CSIRT dará cubrimiento a todas las fases del ciclo de vida de gestión y respuesta a un incidente de seguridad tal como se observa en la Figura 3.

Figura 3. Ciclo de vida de la gestión y respuesta a un incidente de seguridad

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.2016.

6.1.8.9 Política de cooperación

El CSIRT, tendrá como eje fundamental dentro de sus políticas de trabajo la cooperación con otros CSRIT y grupos de seguridad, con el fin de facilitar las coordinaciones y cooperaciones entre equipos de seguridad.

Entre los CSIRT con los que cooperará inicialmente, será con los equipos establecidos a nivel regional, entre ellos se encuentren:

- ColCERT
- CSIRT-PONAL
- CSIRT financiero
- CSIRT Gobierno
- Comando Conjunto Cibernético

Es de aclarar que las cooperaciones con otros equipos no se limitarán únicamente a los mencionados anteriormente, el CSIRT puede establecer acuerdos de cooperación con todas las organizaciones que se requiera con el fin de dar apoyo a la misión principal del CSIRT, la gestión y respuesta a incidentes.

6.2. EVALUAR LOS DIFERENTES RECURSOS TECNOLÓGICOS (HARDWARE Y SOFTWARE) JUNTO CON SERVICIOS NECESARIOS PARA EL FUNCIONAMIENTO DEL CSIRT

Una vez establecido los aspectos generales de las políticas, procedimientos, naturaleza y objetivo del CSIRT los cuales son necesarios para poder determinar los requisitos y el enfoque, se procede a evaluar los diferentes recursos tecnológicos y físicos necesarios para funcionamiento del CSIRT, para ello, primero se debe tener conocimiento de los servicios que ofrece un CSIRT con el fin de determinar los requerimientos de software y hardware necesarios para dar soporte a estos.

6.2.1 Servicios

De acuerdo con el manual para equipos de respuesta a incidentes de seguridad informática, de la definición de la misión se derivan tres componentes a saber entre los que se encuentran las políticas y los aspectos relacionados con la calidad de servicios que se prestan.

Con el fin de determinar los servicios, se debe analizar las necesidades y capacidades del cliente, para esto existen herramientas que facilitan el análisis y permiten una óptima planeación y obtención de los requisitos, por ejemplo, a través de un análisis DOFA se pueden evaluar las debilidades, oportunidades, fortalezas y amenazas, esta información permitirá a las empresas y en este caso al equipo trabajo tomar decisiones acertadas en cuanto a los servicios requeridos, a la par de esta herramienta también se requieren canales de comunicación efectivos entre el CSIRT y el cliente o comunidad objetivo, estos canales pueden ser presenciales como reuniones o visitas locativas, de igual manera o se pueden llevar a cabo encuentros virtuales mediante el uso de los recursos tecnológicos disponibles como sitios web, correos electrónicos, llamadas telefónicas, video llamadas, etc.

Una vez efectuado el análisis de las necesidades y capacidades del cliente, es posible determinar los servicios a implementar, los cuales deben estar alineados con la misión, con la naturaleza del CSIRT y con la capacidad de talento humano, ya que dependiendo el recurso humano del CSIRT y de la organización se determinará si se implementaran todos los servicios o si se tercerizará algunos de ellos con el fin de dar satisfacción a las necesidades del cliente.

De acuerdo con la Organización de los Estados Americanos[32], los servicios prestados por un CSIRT se agrupan en tres tipos: servicios reactivos, servicios proactivos y servicios de valor agregado o servicios de gestión de la calidad de la seguridad tal como se observa en el Cuadro 6**Error! Reference source not found.**.

[32] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. Washington, D, C: Secretaria General de la Organización de los Estados Americanos (OEA). 2016. p. 21.

Cuadro 6. Lista de servicios tradicionales de un CSIRT

Servicios Reactivos	Servicios Proactivos	Servicios de Gestión de la Calidad de la Seguridad
• Alertas y Advertencias • Manejo de incidentes • Manejo de vulnerabilidades • Manejo de artefactos Maliciosos	• Anuncios • Observatorio de tecnología • Evaluaciones o auditorias de la seguridad • Configuración y mantenimiento de herramientas de seguridad, aplicaciones y estructuras • Desarrollo de herramientas de seguridad • Servicios de detección de intrusos • Difusión de información relacionada con seguridad	• Análisis de riesgos • Continuidad del negocio y recuperación ante desastres • Consultoría de seguridad • creación de conciencia • Educación/formación • Evaluación o certificación de productos

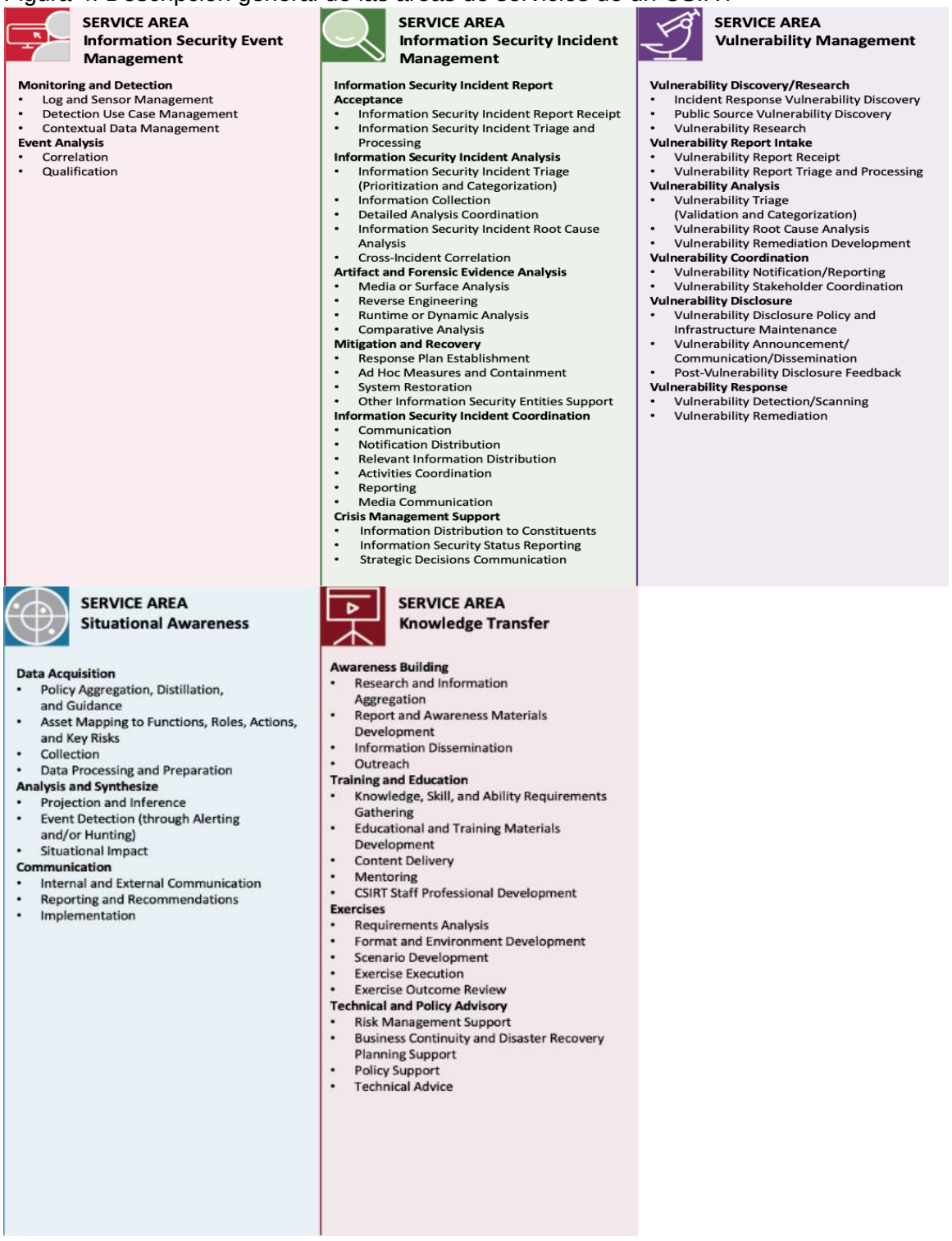
Fuente: WEST-BROWN, Moira, et al. Handbook for Computer Security Incident Response Teams (CSIRTs). 2 ed. Pittsburgh, PA: Carnegie Mellon University.

Los servicios reactivos son aquellos que se ponen en marcha una vez se detecte un evento o incidente de seguridad informática o por petición de algún miembro del equipo, este tipo de servicios conforman el núcleo del CSIRT y son esenciales para su funcionamiento. Los servicios proactivos, son los que se especializan en ayudar a la organización a proteger y asegurar los activos de información mediante la preparación de un sistema de seguridad que pueda hacer frente a ataques, eventos e incidentes de seguridad, se enfocan en reducir los incidentes a futuro.

Por último, los servicios de gestión de la calidad de seguridad se enfocan en mejorar los servicios existentes, por lo general son realizados por dependencias externas al CSIRT, tales como departamentos de tecnología, equipos de auditoría, equipos de capacitación externos, entre otros; generalmente son clasificados como servicios proactivos ya que ayudaran a la reducción de incidentes mediante el aumento de la calidad y eficiencia de los procesos existentes.

La finalidad de estos servicios es brindar cobertura a ciertas áreas que deben estar cubiertas por un CSIRT, según FIRST dichas áreas están divididas en 5 secciones tal como se observa en la Figura 4.

Figura 4. Descripción general de las áreas de servicios de un CSIRT



Fuente: FIRST. FIRST CSIRT Services Framework. [sitio web]. [Consultado: 28 de marzo de 2022]. Disponible en: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

6.2.2 Software

Con el fin de garantizar el funcionamiento del CSIRT es necesario implementar ciertas herramientas tecnológicas que estén acordes a la infraestructura tecnológica de la organización y las cuales garanticen el soporte de los servicios primordiales de estos centros, es decir los servicios reactivos, principalmente el servicio de manejo de incidentes y otros servicios necesarios que apoyan el manejo de incidentes y la misión principal del CSIRT.

Es de tener en cuenta que actualmente existen diferentes herramientas tecnológicas que pueden brindar soporte a estos servicios las cuales varían en licenciamiento, enfoque, casa desarrolladora, precio, curva de aprendizaje, entre otras, por lo tanto, la elección e implementación de las herramientas dependerá de las necesidades y capacidades de la organización.

En el Cuadro 7 se puede observar un listado de servicios, área y el software correspondiente para dar soporte a este mismo.

Cuadro 7. Software para un CSIRT

Servicio	Área	Enfoque	Nombre
Alertas y Advertencias / Manejo de incidentes	Gestión de incidentes de seguridad de la información / Informe de incidentes de seguridad de la información	Alertas y reportes	Request Tracker for Incident Response (RTIR)
			Open Technology Real Services (OTRS)
	Gestión de eventos de seguridad de la información / Monitoreo y detección	Alertas e informes / Monitoreo activo	The Hive
			NfSen
			Elastic
			Wazuh
			PackertBeat
Difusión de información relacionada con seguridad / Analisis de riesgos	Conciencia situacional / Adquisición de datos	Fuentes de información	Website watcher
			watch that page
			http://www.zone-h.org/archive/special=1
			https://www.phishtank.com/asn_search.php
			https://www.malwaredomainlist.com/mdl.php
			https://zeustracker.abuse.ch/monitor.php
			http://www.netcraft.com/anti-phishing/phishing-site-feed
			https://www.cyveillance.com/home/security-solutions/data
			https://www.team-cymru.com/reputation-feed.html
			https://www.proofpoint.com/us/solutions/products/threat-intelligence
			cve-search

Cuadro 7. Continuación

Servicio	Área	Enfoque	Nombre
Manejo de artefactos maliciosos	Gestión de vulnerabilidades / Descubrimiento e investigación	Herramientas forenses digitales	Cuckoo Sandbox
			Malwr
			VirusTotal
Manejo de artefactos Maliciosos / Manejo de vulnerabilidades	Conciencia situacional / Análisis y síntesis	Honeypots	Nepenthes
			Dionaea
			Glastopf
			Conpot
			Thug
			HoneyViz
			Kippo-graph
			T-Pot
Manejo de incidentes	Gestión de incidentes de seguridad de la información / Análisis de eventos de seguridad de la información	Recolección y procesamiento de información	IntelMQ
		Análisis de amenazas e Información de amenazas y taxonomías.	Malware Information Sharing Platform
		Log management	Graylog
Manejo de incidentes / Manejo de vulnerabilidades	Gestión de incidentes de seguridad de la información / análisis de artefactos y pruebas forenses	Herramientas forenses digitales	REMnux
			Volatility
			Interactive Disassembler
			Volatility
	Gestión de vulnerabilidades / Descubrimiento e investigación	Herramientas de evaluación de seguridad	Kali Linux
			Nessus
Servicios de detección de intrusos	Gestión/monitoreo y detección de eventos de seguridad de la información	Monitoreo activo	Snort
			Suricata
			BroIDS
			OSSEC
Servicios de detección de intrusos	Gestión/monitoreo y detección de eventos de seguridad de la información	Monitoreo activo	Security Onion

Fuente: Elaboración Propia.

Así mismo, se recomienda la implementación de herramientas adicionales que permitirán elevar los estándares de seguridad al interior de la organización

1. Software de cifrado de correos electrónicos: GnuPG, software de cifrado gratuito y de código abierto, permite la encriptación de datos y comunicaciones

2. Herramientas de Búsqueda de información de un contacto, estas herramientas permiten optimizar la gestión de contactos para comunicación de incidentes y cooperación entre equipos de respuesta, algunas herramientas que se pueden usar son:

    a. RIPE
    b. IRT-object
    c. TI

3. Software de virtualización, es un software que permite la instalación de sistemas adicionales dentro de un sistema operativo anfitrión mediante la implementación de ambientes virtuales, existen 2 herramientas que son las más usadas: VMware (herramienta de pago) y VirtualBox (software libre). Este tipo de herramientas se hace necesarias para la implementación de copias de respaldo, sandbox, honeynets, entre otros. Se recomienda que un CSIRT tenga al menos 2 servidores de virtualización con el fin de garantizar disponibilidad y redundancia de la información.

4. Sistemas operativos, se recomienda el uso de sistemas operativos que sean basados en GNU/Linux, ya que es un sistema operativo de uso libre, estable y rápido, soportado por la comunidad lo que permite el desarrollo de parches de seguridad para arreglar vulnerabilidades detectadas, así como también cada distribución se especializa en ciertas funciones, por ejemplo, Kali Linux especializada en seguridad de red, Ubuntu orientado a la experiencia de usuario y accesibilidad, cuenta con 2 versiones una de escritorio y una especializada para servidores.

5. Antivirus, es necesario el uso de herramientas que garanticen una capa de seguridad extra en los ordenadores de la organización, herramientas como los antivirus son una excelente elección, ya que con el avance de la tecnología muchos de ellos incorporan firewalls virtuales, copias de seguridad automáticas, alertas, protección contra Advanced Persistent Threats, ramsonware, entre otros. En el mercado se encuentran diferentes soluciones, entre las más conocidas están Kaspersky, Norton Antivirus y Nod32.

6. Licenciamiento, es importante tener en cuenta el licenciamiento de todo el software que adquiera la empresa, esto con el fin de cumplir con todos los requerimientos de ley respecto al uso de software licenciado y también para poder contar con el soporte técnico y de usuario final que ofrecen las empresas, entre las licencias más comunes a adquirir se encuentran:

    a. Sistemas operativos: Windows
    b. Suite Empresarial Office 365

c. Software de Virtualización: Vmware
d. Antivirus (Kaspersky, Norton, Nod32, etc.)

Las herramientas por implementar no deben limitarse a las mencionadas anteriormente, se pueden implementar todas las herramientas que la organización tenga a bien adquirir para cumplir con los objetivos organizacionales, garantizar la seguridad de la información y dar soporte al CSIRT.

6.2.3 Hardware

Los recursos físicos (Hardware) estarán condicionados a la estructura organizacional del CSIRT y al tamaño de la infraestructura tecnológica de la organización, así como también al presupuesto de la organización. No existe norma general para determinar las referencias del equipamiento necesario, estos pueden variar en marca, referencia y capacidad dependiendo del tamaño del CSIRT, su estructura y la estructura tecnológica de la organización. De manera general se puede decir que los recursos de Hardware necesarios para dar soporte al CSIRT son los siguientes:

Cuadro 8. Recursos físicos (Hardware) de un CSIRT

DISPOSITIVO	MARCA DE REFERENCIA	CARACTERISTICAS
Firewall	Firewall Fortinet FortiGate 7040E.	• Alto rendimiento • Inspección SSL • Protección contra APT • Filtrado de paquetes • Prevención de intrusos
Routers	Cisco Catalyst 8500 Series.	• Criptografía acelerada por hardware • Alto rendimiento • Automatización
Switchs	Cisco Catalyst 9300 Series.	• Diseñado para IOT • Interfaz simple y Segura • Gestión de red avanzada
Access-point	Wireless AC1750 Wave 2 Dual-Band PoE Access Point. D-LINK	• Band Steering • Varios modos de funcionamiento • Alta velocidad, eficiencia y seguridad
Servidor DNS y DHCP	Dell PowerEdge FC430 Server	• Ideal para servidores Web, virtualización, host dedicado entre otros
Servidor Web	Cisco UCS® C220 M5 Rack Server. Cisco	• Servidor escalable • Ideal para infraestructura web, ti, virtualización, bases de datos, etc. • Alto rendimiento y eficiencia

Cuadro 8. Continuación

DISPOSITIVO	MARCA DE REFERENCIA	CARACTERISTICAS
Servidor de Virtualización	SYNOLOGY RS3621RPxs	• Servidor NAS con 12 bahías • Potente y rentable • Óptimo para sistemas de virtualización, gestión de datos y copias de seguridad
Storage	Western Digital My Cloud Expert Series EX2 Ultra	• Almacenamiento de alto rendimiento • Alta velocidad de procesamiento y transmisión • Cifrado de volúmenes
WAF	FortiWeb 1000E	• Aprendizaje automático • Mitigación avanzada de bots • Protección para las API • Herramientas de análisis visual
Analizador de eventos	Fortianalyzer FAZ-150G	• Detección y correlación de eventos en tiempo real • Integración con firewall y equipos FortiGate • Copias de seguridad automáticas • Automatización de seguridad
Servidor Sandbox	FortiSandbox-1000D	• Automatización inteligente • Implementación flexible • Machine Learning y Deep Learning integrados
Computadores	ThinkStation P340 Tower (Intel)	• Seguro y ampliable • Memoria y almacenamiento de vanguardia • Alto rendimiento

Fuente: Elaboración propia.

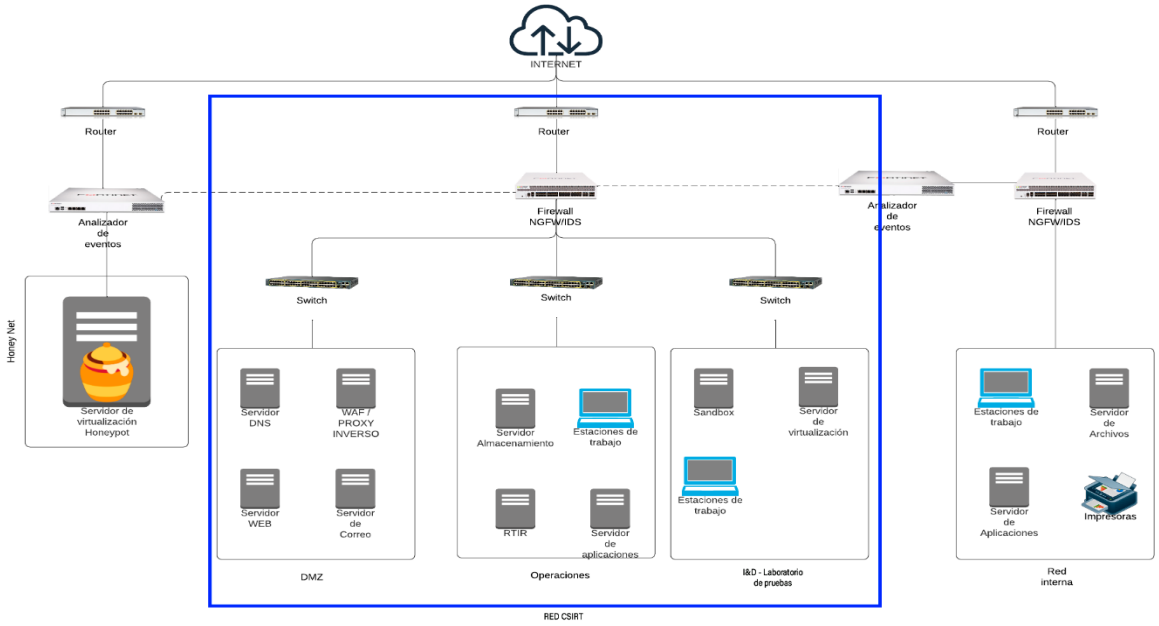
Adicionalmente se debe tener en cuenta la adquisición de otros equipos de uso básico en las tareas diarias de la organización tales como:

1. Servicio de correo institucional
2. Computadores
3. Teléfonos
4. Trituradores
5. Unidades de almacenamiento lógico portátil
6. Impresoras
7. Equipo de oficina (escritorios y sillas ergonómicas)

6.2.4 Diagrama de red

La red con la que trabajara el CSIRT debe contar con mecanismos que garanticen la seguridad de la información ya que como se dijo anteriormente, en los diferentes dispositivos del CSIRT reposa y se procesa información sensible de la organización lo cual en caso de caer en manos inescrupulosas puede ocasionar graves daños a la organización. Entre estos dispositivos encontramos Firewalls, IDS/IPS, WAF, Honeypots, etc.; de igual manera, en la arquitectura de red se tendrá en cuenta la segmentación de esta misma a fin de evitar que un ataque o incidente informático pueda diseminarse y afectar toda la red

Figura 5. Diagrama de Red de la Organización



Fuente: Elaboración propia

6.2.5 Instalaciones del CSIRT

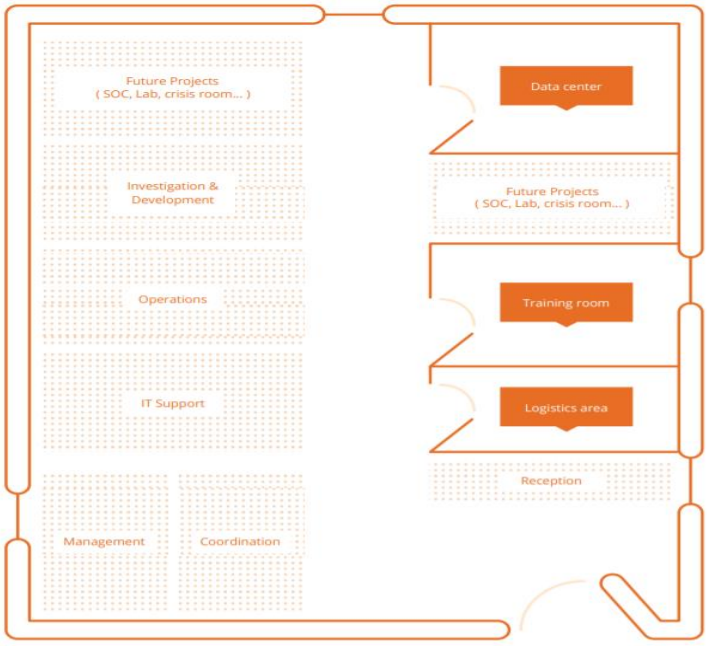
Cuando se planean y diseñan las instalaciones del CSIRT se debe tener en cuenta la sensibilidad de la información con la que se trabaja por lo tanto se deben diseñar y planear teniendo en cuenta la seguridad tanto de la información como de los empleados y el staff del CSIRT por lo tanto se debe garantizar en todo momento la seguridad de la información e infraestructura alojada; esto se logra mediante la implementación de controles de seguridad físicos los cuales serán los encargados de gestionar, garantizar y mantener el acceso únicamente al personal autorizado y a los miembros del CSIRT. El cuarto de datos en donde se encontrará alojada toda la infraestructura tecnológica del CSIRT debe contar con controles físicos de acceso y con mecanismos de seguridad ambiental que garanticen las condiciones ambientales óptimas para el funcionamiento de los equipos que se encuentren alojados.

Entre otros aspectos a tener en cuenta resaltan la implementación de sistemas de detección y extinción de incendios, sistemas redundantes (UPS, aires acondicionados, etc.), salidas de emergencia y lockers para el personal del CSIRT; también se recomienda la instalación de sistemas de vigilancia (CCTV) al interior y exterior de las instalaciones

Es pertinente que como mínimo las instalaciones del CSIRT contengan:

1. Cuarto de datos
2. Oficinas del personal del CSIRT
3. Sala de reuniones (Salón de crisis)

Figura 6. Plano Básico de las instalaciones del CSIRT



Fuente: ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. Washington, D, C: secretaria general de la Organización de los Estados Americanos (OEA). 2016.

Una buena aproximación de las instalaciones de un CSIRT es la que se observa en la 6, en donde se puede apreciar la distribución de las instalaciones y en donde se cuenta con un data center, cuarto de entrenamiento, área logística, así como también espacio para futuros proyectos

6.3. EXAMINAR LOS DIFERENTES ESTÁNDARES, MODELOS Y RECOMENDACIONES DE SEGURIDAD INFORMÁTICA APLICABLES A UN CSIRT

Para el obtener un desempeño destacable y garantizar un correcto funcionamiento de un CSIRT, es necesario contar con un marco de referencia que permita al personal del CSIRT establecer parámetros y estándares con el fin de medir la calidad y seguridad de todos los procedimientos efectuados, por ejemplo al momento de elaborar políticas o definir los servicios a ofrecer estos deben elaborarse bajo ciertos estándares y parámetros con el fin de implementar todas las buenas prácticas y recomendaciones de seguridad que emiten las organizaciones a nivel nacional e internacional, de esta manera se garantiza que los profesionales de seguridad encargados de la implementación del CSIRT cumplan con criterios de alta calidad al momento de cumplir un trabajo deseado. Es por ello por lo que existen diversas organizaciones especializadas en seguridad informática y en respuesta a incidentes tales como el National Institute of Standars and Technology (NIST), Internet Engineering Task Force (IETF), Forum of Incident Response and Security Teams (FIRST), entre otras, las cuales con el fin de garantizar la existencia de estos parámetros han elaborado estándares, guías y buenas prácticas aplicables a un CSIRT entre los cuales se encuentran:

1. NIST
    a. Computer Security Incident Handling Guide[33]: esta publicación de NIST, establece una guía para ayudar a las organizaciones a implementar las capacidades de respuesta y manejo de incidentes de formar efectiva y eficaz, provee lineamientos de manejo de incidente enfocados en el análisis de información y la elección de métodos apropiados para respuesta a cada incidente.

2. Carniege Mellon Software Engineering Institute
    a. Organizational Models for Computer Security Incident Response Teams (CSIRTs)[34]: esta guía ayuda a los CSIRT a gestionar un modelo organización que permita la implementación de todos los procesos de manejo y respuesta a incidentes, se incluyen ventajas y desventajas de diferentes modelos, así como también que tipo de servicios funcionan mejor con determinado modelo organizacional.
    b. Defining Incident Management Processes for CSIRTs: A Work in Progress[35]: este reporte ayuda a la definición del proceso de manejo de incidentes mediante el análisis de cinco fases, preparación/sostenimiento-mejora, protección de infraestructura, detección de eventos, triage y respuesta

[33] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST-SP 800-61. a. Computer Security Incident Handling Guide. Gaithersburg, MD: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2012. rev.2.

[34] KILLCRECE, Georgia, et al. Organizational Models for Computer Security Incident Response Teams (CSIRTs). Pittsburgh, PA: Carnegie Mellon University. 2003.

[35] ALBERTS, Chris, et al. Defining Incident Management Processes for CSIRTs: A Work in Progress. Pittsburgh, PA: Carnegie Mellon University. 2004

c. Action List for Developing a Computer Security Incident Response Team (CSIRT)[36]: provee una lista de chequeo con temas y diferentes aspectos a verificar al momento establecer un CSIRT, toca aspectos como planeación, problemas comunes, entrenamiento y capacitación, definición de la misión y constitución del CSIRT, identificación de recursos, roles y responsabilidades, etc.
d. Handbook for Computer Security Incident Response Teams (CSIRTs)[37]: se podría decir que es una de las guías maestras al momento de implementar un CSIRT, este manual provee todas las directrices y guías necesarias para establecer y operar un CSIRT, se enfoca en ayudar a las organizaciones a definir el enfoque y naturaleza del CSIRT mediante el desarrollo del servicio de manejo de incidentes. Esta guía es una de las que más tuvo relevancia al momento de desarrollar este trabajo puesto que representa una gran fuente de información detallada sobre el funcionamiento, organización, políticas y servicios de un equipo de respuesta a incidentes.

3. FIRST
    a. CSIRT Services Framework[38]: este marco de trabajo presenta un conjunto de servicios de ciberseguridad aplicables a un CSIRT para ayudar al funcionamiento del servicio de manejo y respuesta de incidentes, así como también a facilitar y mejorar todas las operaciones propias del CSIRT

4. ENISA
    a. How to set up CSIRT and SOC[39]: otra de las guías maestras para la implementación de CSIRT, provee directrices para establecer tanto un CSIRT como un centro de operaciones de seguridad (SOC), se enfoca en 5 pilares fundamentales alistamiento, diseño, implementación, operaciones y mejora.
    b. Reference Incident Classification Taxonomy[40]: provee un marco de referencia para la clasificación de incidentes de seguridad informáticos, que ayudan a establecer parámetros para una fácil identificación de los incidentes, así como también provee las fuentes más comunes de ataque, comportamientos, activos de información afectados, etc.
    c. A good practice guide of using taxonomies in incident prevention and detection[41]: establece buenas prácticas para el uso de taxonomías para la clasificación, detección y prevención de incidentes de seguridad informáticos.

[36] CARNEGIE MELLON UNIVERSITY. Action List for Developing a Computer Security Incident Response Team (CSIRT). Pittsburgh, PA: Carnegie Mellon University. 2006
[37] WEST-BROWN, Moira, et al. Handbook for Computer Security Incident Response Teams (CSIRTs). 2 ed. Pittsburgh, PA: Carnegie Mellon University. 2003.
[38] FIRST. Computer Security Incident Response Team (CSIRT) Services Framework. Ver. 2.1. 2019
[39] ENISA. HOW TO SETUP CSIRT AND SOC. ENISA, 2020.
[40] ENISA. Reference Incident Classification Taxonomy. ENISA. 2018.
[41] ENISA. A good practice guide of using taxonomies in incident prevention and detection. ENISA. 2016.

d. Good Practice Guide for Incident Management[42]: establece un marco de trabajo con buenas prácticas y provee directrices sobre incidentes de seguridad de la información enfocándose en el manejo de incidentes.

[42] ENISA. Good Practice Guide for Incident Management. ENISA. 2010.

6.4. PROPONER UN FLUJO DE PROCESOS PARA EL DESARROLLO DE LAS ACTIVIDADES AL INTERIOR DEL CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Una vez abordados los aspectos necesarios para el funcionamiento de un CSIRT tales como alcance, servicios, estructura organizacional, recursos, buenas prácticas, entre otros, se procede a establecer un flujo de procesos que permita la puesta en marcha del CSIRT.

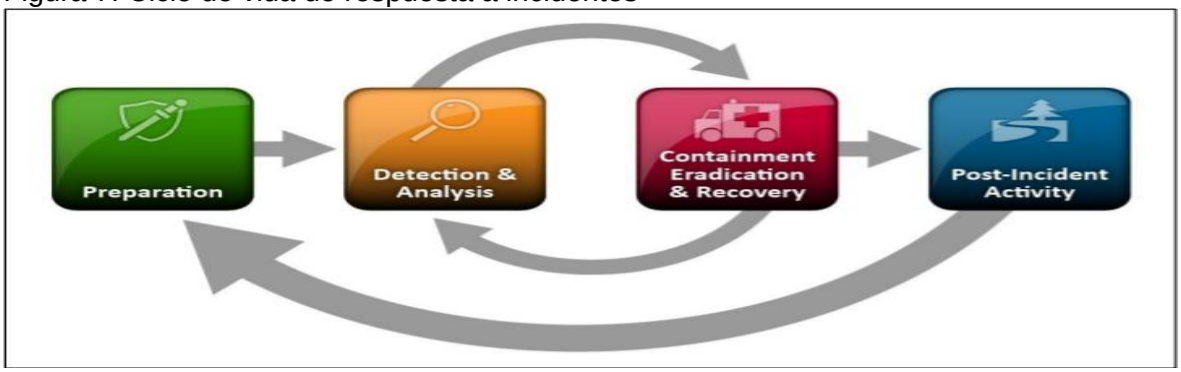
Como se dijo anteriormente el servicio más importante y fundamental de un CSIRT es el servicio de manejo de incidentes, esta operación es el núcleo fundamental del funcionamiento del centro.

6.4.1 Servicio de manejo de incidentes

Un correcto procedimiento del manejo de accidentes es logrado mediante la definición de un flujo lógico que permita al CSIRT establecer un plan de acción y generar una respuesta oportuna que permita reducir el impacto de un incidente en los activos de información de la organización.

El National Institute of Standars and Technology ha desarrollado un ciclo de vida de respuestas a incidentes el cual puede ser observado en la Figura 7, en dicho ciclo se plantea un flujo de procesos que permiten un correcto manejo de los incidentes, este flujo comprende cuatro etapas, preparación, detección y análisis, contención, erradicación y recuperación y por último actividades post-incidentes.

Figura 7. Ciclo de vida de respuesta a incidentes



Fuente: National Institute of Standards and Technology. NIST-SP 800-61 Computer Security Incident Handling Guide. Gaithersburg, MD: National Institute of Standards and Technology. 2012. Rev. 2

6.4.1.1 Procedimiento de preparación para el manejo de incidentes

Esta fase consiste en brindar las herramientas necesarias para que el equipo sea capaz de responder a incidentes de seguridad, así como también se enfoca en la prevención de accidentes mediante el aseguramiento de todos los activos de información con los que cuenta la organización. Esta fase debe estar apoyada por los equipos encargados de tecnologías de la información o similares con los que cuente la organización, de esta

manera no solo se logra que el CSIRT cuente con las herramientas tecnológicas, sino que también permitirá la implementación de buenas prácticas de seguridad lo que contribuirá al aseguramiento de los sistemas. Adicionalmente se recomienda que el CSIRT tenga a disposición los siguientes recursos:

- Comunicaciones: el CSIRT debe contar con los recursos necesarios para establecer comunicación entre los miembros de la organización, autoridades competentes y otros equipos CSIRT para ello se debe contar con un listado de contactos que incluya información como correos, teléfono principal y backup adicionalmente se debe contar también con mecanismos que faciliten el reporte de incidentes y medios de comunicación seguros.
- Hardware y software: se debe contar con herramientas tecnológicas que permita desarrollar funciones del CSIRT como obtención de información, análisis forense, recolección de evidencias, análisis de vulnerabilidades, así como también recursos físicos como estaciones de trabajo, computadores portátiles, discos de almacenamiento, dispositivos de backup, etc.
- Análisis de incidentes: se debe tener documentado configuraciones de red, activos críticos, diagramas de red y listado de puertos usados con el fin de agilizar el proceso de análisis de incidentes mediante la identificación de anomalías y diferencias entre la información proporcionada y la información recolectada en el momento del incidente
- Mitigación de incidentes: comprende todos los recursos necesarios que permiten recuperar el funcionamiento de un sistema, copias de seguridad, imágenes de instalación, servidores de backup, etc.

También se deben tener en cuenta las siguientes buenas prácticas de seguridad para la prevención de incidentes:

- Evaluaciones de riesgo de manera periódica con el fin de determinar posibles nuevos riesgos, amenazas y vulnerabilidades en la organización, esto no solo contribuye a la identificación de un panorama de riesgos, sino que también permite identificar la infraestructura y activos de información críticos los cuales serán prioridad en caso de un incidente informático
- Seguridad de Dispositivos, esta debe seguir el principio de menor privilegio, es decir proveer a los usuarios únicamente los privilegios necesarios para el cumplimiento de sus tareas diarias, también es recomendable que se haga un seguimiento de la actividad de todos los dispositivos mediante auditorias y logs de registros de eventos, una buena práctica es la implementación de software automatizado que permita un monitoreo de configuraciones de seguridad y software ejecutándose en los dispositivos
- Seguridad en redes, la red de la organización debe estar configurada para denegar todo el tráfico que no sea permitido, esto se logra mediante la implementación de reglas de seguridad en los firewalls de la red
- Prevención de malware, uno de los principales aspectos al momento de hablar de seguridad informática, la prevención de malware es crucial al momento de asegurar los activos de información esto puede ser logrado mediante la implementación de software que detecte y elimine este tipo de aplicaciones malignas no solo a nivel de dispositivos sino también a nivel de servidores, clientes, mensajería, etc.

- Sensibilización y entrenamiento de usuarios, se debe prestar especial atención a este punto ya que los usuarios son el eslabón más débil en la cadena se la seguridad, se deben crear programas de sensibilización y entrenamiento que permita a los usuarios comprender las políticas de seguridad de la información de la organización, uso correcto de medios tecnológicos, buenas prácticas de seguridad, entre otros. Se debe tener también en cuenta el entrenamiento no solo de los usuarios regulares sino también del personal del CSIRT y de encargado de tecnologías de la información de la organización, para ello puede ser usado como referente la Guía de programas de prueba, capacitación y ejercicios para planes y capacidades de TI elaborada por el NIST[43]

6.4.1.2 Procedimiento de detección y análisis

La detección de incidentes de seguridad puede convertirse en un proceso complejo debido a la combinación de diferentes factores tales como tipo de incidente, magnitud, saber si ya ocurrió o si está ocurriendo el incidente e incluso situaciones básicas tales como saber detectar un incidente de seguridad.

Los incidentes de seguridad pueden ser detectados por diversos medios como sistemas automatizados, antivirus, detección manual, reportes de usuarios, todos estos medios varían en nivel de confiabilidad y detalle de la información proporcionada, es por ello que existen ciertas señales que permiten la identificación y detección de incidentes de seguridad y saber si están ocurriendo o si ya ocurrieron, por ejemplo, alertas de seguridad, fallas de funcionamiento normal, caídas de servidores, logs de servidores donde se evidencie uso de escáneres de vulnerabilidad e incluso redes sociales en donde hackers anuncian el ataque a las organizaciones.

Este conjunto de señales puede ser clasificada en dos categorías, precursores, es decir señales que dan indicio de un posible incidente en el futuro, o indicadores, los cuales son señales que dan indicio de que un incidente ya ocurrió o está ocurriendo en este mismo momento. Los precursores e indicadores pueden ser detectados por diferentes medios, con el fin de facilitar la tarea NIST de poner a disposición una lista de las fuentes más comunes de detección tal como se observa en la Cuadro 9.

Cuadro 9. Fuentes más comunes de precursores e indicadores

Source	Description
Alerts	
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces false positives—alerts that indicate

[43] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST-SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, MD: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2006.

Cuadro 9. Continuación.

Source	Description
Alerts	
IDPSs	malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service, and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by
	correlating event information. Depending on the event information, an alert can be generated to indicate an incident. Section 3.2.4 discusses the value of centralized logging
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.
Network flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities.32 Organizations such as US-CERT33 and CERT® /CC periodically provide threat update information through briefings, web postings, and mailing lists.

Cuadro 9. Continuación.

Source	Description
Alerts	
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

Fuente: National Institute of Standards and Technology. NIST-SP 800-61 Computer Security Incident Handling Guide. Gaithersburg, MD: National Institute of Standards and Technology. 2012. Rev. 2

Una vez sea identificado un posible precursor o indicador, se debe verificar la veracidad de este ya que en muchas ocasiones puede resultar que la señal detectada sea un posible falso positivo y que la causa sea algo diferente a un incidente de seguridad por ejemplo la caída de un servidor debió a un corte del suministro eléctrico, es por ello por lo que cada señal debe ser evaluada y analizada por el CSIRT.

Con el fin de facilitar la compleja tarea de detección y análisis se debe tener un conocimiento de las características de operación normal de toda la infraestructura de sistemas, la información que permita la detección de incidentes debe encontrarse centralizada y al alcance del CSIRT, se debe tener conocimiento de nuevas vulnerabilidades, información de los servicios que se encuentran funcionando, sistemas operativos, software implementado, se debe llevar un registro histórico de incidentes de seguridad así como también documentarse sobre incidentes en infraestructuras tecnológicas similares y crear planes de diagnóstico periódico de los sistemas con el fin de encontrar posibles anomalías en el comportamiento que permita detectar un incidente de seguridad, de igual manera debe evaluarse la pertinencia del incidente con el fin de determinar si el incidente debe ser atendido por el CSIRT, por ejemplo si el CSIRT presta servicios a una organización privada y llega un reporte de un usuario que indica que una página gubernamental esta caída o hay algún fallo en la infraestructura critica cibernética de un país corresponde al CSIRT Nacional.

Una vez se determine la confiabilidad de la señal y se establezca la ocurrencia de un incidente de seguridad se recomienda efectuar un registro de los incidentes con el fin de facilitar el seguimiento y la gestión de este, para ello se recomienda el uso de sistemas automatizados que facilitan la tarea de registro y control, entre los sistemas de registro más usados por los CSIRT se encuentran RTIR (Request Tracker for Incident Response) y OTRS (Open Technology Real Services).

Posterior al registro del incidente de seguridad se le debe asignar una clasificación, esto ayuda a determinar la gravedad, una referencia del tipo de incidente y los recursos necesarios para manejar el incidente, una buena guía para efectuar un sistema de clasificación de incidentes es el sistema de clasificación de casos del CSIRT[44].

El sistema de clasificación y la clasificación de incidentes no solo permite determinar la gravedad del incidente, sino que también proporciona información estadística, permite determinar tendencias y reincidencias y permite hacer similitudes con reportes de incidentes generados por las diferentes organizaciones.

Una buena práctica al momento de clasificar los incidentes es el uso de taxonomías, estas permiten el uso de lenguajes estandarizados referente a seguridad informática, entre las taxonomías más usadas se encuentra Reference Incident Classification Taxonomy[45].

Una vez registrado y recibido el incidente de seguridad por parte del CSIRT se debe hacer una valoración del incidente, existe un procedimiento usado por el personal de la salud llamado triage, en el cual mediante ciertos parámetros se determina la prioridad de atención de un caso; en el caso de un incidente informático se deben evaluar parámetros como:

- Pertinencia
- Impacto
- Posibles daños colaterales
- Activo de información afectado
- Naturaleza del incidente

Estos parámetros pueden ser medidos mediante la asignación de valores numéricos tal como se efectúa en la guía de Gestión de Incidentes del MinTIC, en donde se le asignan valores numéricos al nivel de criticidad tal como se observa en la Cuadro 1010.

Cuadro 10. Niveles de Criticidad de Impacto

Nivel Criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0,50	Sistemas que apoyan más de una dependencias o proceso de la entidad
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas Críticos.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.2016.

[44] FIRST. CSIRT Case Classification. Disponible en: https://www.first.org/resources/guides/csirt_case_classification.html
[45] ENISA. Reference Incident Classification Taxonomy. 2018

De igual manera se le asignan valores numéricos a los niveles de impacto actual y futuro tal como se observa en la Cuadro 111.

Cuadro 11. Niveles de impacto Actual y Futuro

Nivel Impacto	Valor	Definición
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	1,00	Impacto alto en uno o más componentes de más de un sistema de información.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.2016.

Una vez definidos los niveles de impacto y de criticidad se puede obtener el nivel de prioridad mediante la ecuación que se observa en la Figura 8.

Figura 8. Ecuación Nivel de Prioridad

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.2016.

Una vez se tenga el valor del nivel de prioridad, a cada valor se le debe asignar un nivel cualitativo de nivel de prioridad tal como se observa en la Cuadro 122.

Cuadro 12. Niveles de Prioridad del Incidente

Nivel Prioridad	Valor
Inferior	0,00 – 2,49
Bajo	2,5 0 – 3,74
Medio	3,75 – 4,99
Alto	5,00 – 7,49
Superior	7,50 – 10,00

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.2016.

El nivel de prioridad permite determinar un tiempo de respuesta al incidente, estos tiempos pueden variar dependiendo de la naturaleza del incidente, así como también por las políticas establecidas por la organización, una buena estimación de tiempo de atención de incidentes de seguridad puede ser observada en la Cuadro 133.

Cuadro 13. Tiempos máximos de atención de incidentes

Nivel Prioridad	Valor
Inferior	3 horas
Bajo	1 hora
Medio	30 min
Alto	15 min
Superior	5 min

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.2016.

Una vez detectado, clasificado y priorizado el incidente de seguridad el CSIRT debe notificar al personal idóneo del equipo para dar tratamiento de manera sistemática al incidente de acuerdo con su naturaleza. La notificación de incidentes además de permitir un tratamiento oportuno de este, contribuye a la mitigación de impactos, reducción de daños colaterales y recuperación de sistemas y procesos involucrados, al igual que el tratamiento de incidentes, existe un flujo de notificación de incidentes de seguridad este se describe de la siguiente manera:

- El usuario de la organización que detecta o sospecha de la ocurrencia de un posible incidente informático lo reporta al punto de contacto del CSIRT por lo general conocido como mesa de soporte o atención al usuario, esta notificación puede efectuarse por los medios que la organización haya dispuesto al momento de la creación del CSIRT y debe diligenciarse el formato de reporte de incidentes el cual debe ser definido por la organización.
- Posteriormente la mesa de soporte verifica la información del incidente de seguridad y verifica la pertinencia de este, es decir si el incidente descrito realmente se debe catalogar como incidente o corresponde a un requerimiento de soporte de TI. Si se verifica que es un incidente de seguridad se procede a registrar en los sistemas de seguimiento y control con el fin de hacer la adecuada gestión hasta el cierre del caso
- Si la detección se efectúa mediante los sistemas de monitoreo y análisis con los que cuenta la organización, el caso es notificado inmediatamente al analista de incidentes de seguridad quien efectuará las gestiones necesarias para dar tratamiento al incidente, se notificará al primer punto de contacto con el fin de hacer los tramites respectivos de registro y control y efectuar el seguimiento del caso

6.4.1.3 Procedimiento de contención, erradicación y recuperación

Dependiendo de la gravedad, complejidad y naturaleza del incidente puede ser necesario la ejecución de una o varias técnicas con el fin de contener y mitigar el incidente, algunas acciones de contención y mitigación pueden ser:

- Desactivación de servicios
- Parches de seguridad
- Aislamiento de sistemas o servicios
- Apagado de sistemas
- Desconexión de la red
- Bloqueo de cuentas
- Deslogueo de usuarios
- Remoción de privilegios
- Redirección a un sandbox

Las estrategias de contención variaran dependiendo del incidente y los criterios de atención, es por ello por lo que se deben establecer estrategias de atención para facilitar y optimizar el tiempo de toma de decisiones, la elección de estas estrategias está ligada a parámetros tales como:

- *Robos y daños potenciales*
- *Necesidad de preservación de evidencia*
- *Disponibilidad de servicios*
- *Tiempo y recursos necesarios para implementar la estrategia*
- *Efectividad de la estrategia*
- *Duración de la solución*[46]

Una vez se logre la contención del incidente se hace necesario la erradicación y recuperación, esto consiste en actividades de limpieza de los daños y residuos dejados por el incidente de seguridad y posteriormente se procede a hacer una recuperación de los sistemas afectados mediante mecanismos de restauración de sistemas tales como copias de seguridad, restitución de servicios, reinstalación de copias en limpio de sistemas operativos, software, etc.

Es importante que durante esta fase se identifiquen todos los dispositivos afectados con el fin de aplicar las medidas de erradicación y recuperación necesarias, una vez se apliquen estas medidas se debe confirmar el funcionamiento normal de los sistemas y verificar que las estrategias de atención al incidente hayan sido efectivas, también se debe estudiar el incidente y aplicar medidas de prevención contra nuevos incidentes similares.

En algunos casos cuando los incidentes causan daños graves a los activos de información, la recuperación puede tardar días o meses, es por ello por lo que las organizaciones deben contar con planes de continuidad de negocios para garantizar el funcionamiento de la organización a pesar de los daños causados por un incidente.

[46] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST-SP 800-61 Computer Security Incident Handling Guide. En: Choosing a Containment Strategy. Gaithersburg, MD: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2012. Rev. 2

6.4.1.4 Actividades posts incidentes

Una vez solventado el incidente de seguridad, se debe hacer un informe sobre el incidente presentado que comprenda detalles como:

- Inicio del incidente
- Hora de reporte
- Detalle del incidente
- Acciones ejecutadas
- Activos de información involucrados
- Afectaciones y daños
- Medidas de seguridad a implementar

Este informe no solamente sirve para efectuar comunicaciones de lo sucedido sino también para establecer estrategias de mejora que permitan no solo evitar que sucedan incidentes similares si no también mejorar los procesos de atención, tiempos de respuesta, estrategias de atención, determinar capacidad del CSIRT y mantener un registro histórico de los incidentes que permita generar lecciones aprendidas.

6.4.2 Servicio de alertas y advertencias

La generación de alertas y advertencias es el servicio encargado de emitir alertas de intrusión, advertencias de vulnerabilidades y avisos de seguridad, así como también generar informes sobre nuevas tecnologías, vulnerabilidades y herramientas para la detección de vulnerabilidades; esto orientado a mantener la seguridad de toda la infraestructura y estar a la vanguardia de la seguridad informática contando con el conocimiento de vulnerabilidades que puedan ser explotadas en un futuro y afectar los sistemas de información de la organización, adicionalmente, es importante contar con este servicio ya que nos permitirá generar comunicados a las diferentes dependencias e incluso a otros CSIRT. La generación de alertas y advertencias seguirá el siguiente flujo:

6.4.2.1 Obtención de información.

Se debe obtener información que contribuya a obtener información de los sistemas, tecnologías e infraestructura en general con la que cuenta la organización, esto comprende información de vulnerabilidades, incidentes de seguridad recientes en compañías a fines al objeto de la organización y actualizaciones de seguridad. Esta información puede ser obtenida de diversas fuentes de información tanto públicas como privadas, por ejemplo, revistas, sitios web, artículos, informes de vulnerabilidades, manuales, etc., esta recopilación de información permitirá obtener conocimiento acerca de las posibles vulnerabilidades que puedan ser encontradas en los sistemas de la organización, adicionalmente también pueden ser efectuadas pruebas de vulnerabilidad al interior de la organización con el fin de recopilar la mayor cantidad de información posible.

6.4.2.2 Evaluación de la veracidad y confiabilidad de la información.

Una vez recopilada la información se debe evaluar, con el fin de determinar los aspectos anteriormente mencionados. A fin de comprobar la veracidad de la información, se debe

primero establecer si la fuente de la información es de confianza con el fin de garantizar que las alertas que se generen proveerán información necesaria, verídica y de impacto para la organización, la no corroboración de las fuentes de información puede resultar perjudicial para todos los procesos de la organización ya que generará alertas falsas, desgaste de personal y disminución de la confiabilidad del CSIRT, para ello la Universidad de Alicante propone unos criterios de evaluación para determinar la confiabilidad de la información, en donde se plantean estrategias como respuesta a una serie de interrogantes (¿De dónde?, ¿Quién?, ¿Qué?, ¿Donde?, ¿Cuándo?, ¿Cómo?), y en donde se definen criterios de evaluación dependiendo también la fuente de la información.

Figura 9. Interrogantes para evaluar la información recuperada.

Fuente: Universidad de Alicante. Como evaluar la información encontrada. 2014 p. 4.

De igual manera ENISA propone un ejemplo de procedimiento de identificación de la información, en donde resalta el uso de preguntas básicas para determinar la autenticidad de un mensaje (información).

Figura 10. Ejemplo de procedimiento de identificación de la información.

Procedimiento de identificación de la autenticidad de un mensaje y su fuente

Lista de comprobación general

1. ¿La fuente es conocida y está registrada como tal?
2. ¿La información llega por un canal regular?
3. ¿El mensaje contiene información «extraña« que «parece» errónea?
4. Si intuitivamente una información parece dudosa, antes de actuar hay que volver a verificarla.

Correo electrónico - Fuentes

1. ¿La dirección de la fuente es conocida por la organización y figura en la lista de fuentes?
2. ¿Es correcta la firma PGP?
3. Si surgen dudas con un mensaje, compruebe la cabecera completa.
4. Si surgen dudas, use «nslookup» o «dig» para comprobar el dominio del remitente[20].

WWW - Fuentes

1. Cuando conecte con un sitio web protegido, compruebe los certificados del navegador (https ://).
2. Compruebe el contenido y la validez (técnica) de la fuente.
3. Si duda, no entre en los vínculos ni descargue software.
4. Si duda, haga un «lookup» y un «dig» en el dominio, así como un «traceroute».

Teléfono

1. Escuche el nombre atentamente.
2. ¿Reconoce la voz?
3. Si tiene dudas, pida un número de teléfono y llame usted al autor de la llamada.

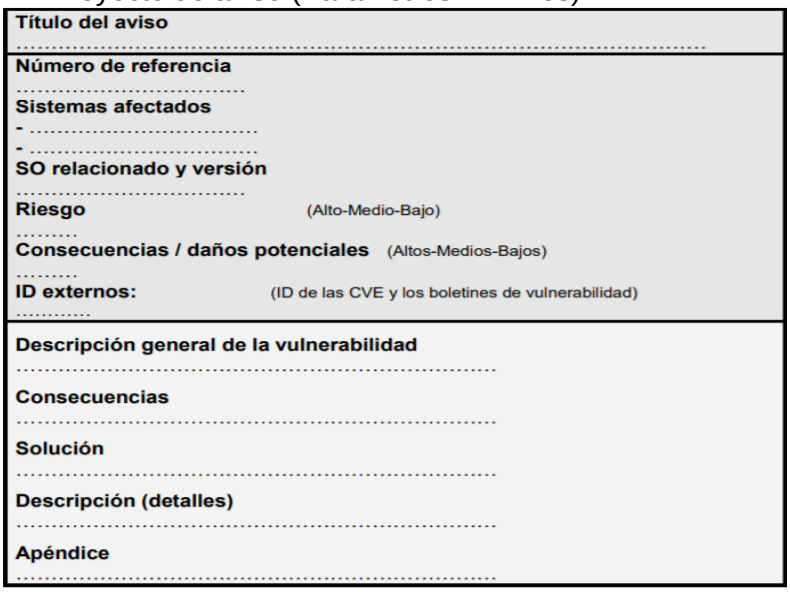
Fuente: ENISA. Como crear un CSIRT paso a paso. Agencia Europea de Seguridad de las Redes y de la Información (ENISA), 2006. p. 45

6.4.2.3 Generación de la información a distribuir.

Una vez completados los pasos anteriores se podrá hacer la generación y distribución de las alertas, estas pueden ser distribuidas por el medio de preferencia de la organización (e-mail, sitios web, etc.).

Es importante que todas las alertas mantengan la misma estructura con el fin de garantizar claridad y estandarización, un buen referente para estas comunicaciones es el formato de común aviso del EISPP (Anexo C), este es un formato elaborado por el programa de promoción de seguridad de la información europeo, el cual busca estandarizar todos los avisos de seguridad en las organizaciones en especial en los CSIRT, en caso de no ser posible la adaptación de este formato, ENISA dispone de los parámetros mínimos que debe tener un aviso informativo como se observa en la Figura 11.

Figura 11. Proyecto de aviso (Parámetros mínimos)



Fuente: ENISA. Como crear un CSIRT paso a paso. Agencia Europea de Seguridad de las Redes y de la Información (ENISA), 2006. p. 47

7. CONCLUSIONES

De acuerdo a lo desarrollado en el presente trabajo mediante la investigación documental sobre el funcionamiento y el diseño documental de procesos propios de un CSIRT se puede concluir que estos no solo se enfocan en dar atención a incidentes informáticos si no abarcan una amplia gama de procesos fundamentales para su funcionamiento tales como gestión de riesgos, atención al usuario, capacitación, investigación, entre otros.

También se puede concluir que los CSIRT son un sistema cambiante y adaptable debido a que los procesos necesarios para el correcto y adecuado funcionamiento de un CSIRT varía dependiendo de muchos factores, como se habló a lo largo del desarrollo de este trabajo, todas las organizaciones tienen factores que las diferencian unas de otras ya sea la naturaleza, la organización, su capacidad financiera, sus objetivos; todos estos factores, determinan qué servicios y procesos de un CSIRT aplicar y será esto lo que finalmente determine la naturaleza del CSIRT y su enfoque (académico, comercial, militar, entre otras).

Como se pudo observar los CSIRT varían dependiendo de la organización y por ello se hace necesario que existan ciertos parámetros para que los profesionales en seguridad puedan guiarse e implementar CSIRT bajo estándares de calidad, es por ello que el uso de buenas prácticas cumplen un papel fundamental al momento de hablar de implementación, estos estándares y buenas prácticas no solo contribuyen al diseño óptimo de procesos propios de estos centros, sino también contribuye a la ampliación de los conocimientos necesarios para la atención de incidentes de seguridad tales como flujos de procesos de comunicación, flujos de manejo de incidentes, recomendaciones de seguridad, gestión de riesgos, políticas y procedimientos de seguridad, etc., lo cual permite comprender más a fondo la naturaleza de los servicios ofrecidos, de igual forma se pudo establecer el flujo de procesos para dar cumplimiento a las funciones de un CSIRT que sirven de modelo para una implementación real.

Mediante el desarrollo de este trabajo se evidencia que el punto de partida de los proyectos es quizá el más importante en el ciclo de vida de estos, por ejemplo al momento de hablar de CSIRT se puede concluir que la definición de los aspectos más básicos tales como el alcance, misión y estructura cumplen un papel vital y determinante en la implementación de estos centros, ya que en base a estos se desarrollara el funcionamiento y naturaleza de este, esto debido a que con base al alcance definido se establecerán una serie de políticas, procedimientos y servicios que irán alineados con el programa estratégico de la organización.

8. RECOMENDACIONES

Se debe reconocer la importancia de los activos de información, ya que al hablar de activos de información no solamente se refiere a dispositivos electrónicos sino también a toda la infraestructura tecnológica y física, recursos humanos y la información en sí, lo cual mediante un correcto manejo puede ofrecer un valor agregado a todos los procesos corporativos y aumentar la eficacia y eficiencia de las rutas para alcanzar las metas y objetivos planteados por una organización.

Se recomienda que al momento de implementar un CSIRT se efectúe mediante el uso de las directrices y parámetros definidos en los estándares y buenas prácticas de los cuales se trató a lo largo del desarrollo de este trabajo, ya que esto garantiza un correcto flujo de trabajo y estándares de calidad para la implementación de estos centros, es menester que todos los miembros que participen de los servicios reactivos y proactivos que brinda el CSIRT, conozcan las políticas definidas para la actuación del mismo

Al momento de implementar servicios, políticas y procedimientos no se debe limitar a los expuestos en el desarrollo de este documento, existen una gran gama de servicios que varían dependiendo de las necesidades de la organización e incluso pueden implementarse servicios que no se encuentren listados en este trabajo siempre y cuando sea con el fin de garantizar las funciones propias de un CSIRT y cumplir con los requisitos corporativos.

Uno de los factores más importantes en el funcionamiento de un CSIRT es el entrenamiento del personal que trabaja en estos centros, es por ello que se recomienda que las organizaciones tengan un programa de entrenamiento y capacitación continuada en donde se adquieran conocimientos en fundamentos de redes, fundamentos de ciberseguridad, manejo básico y avanzado de incidentes, pentesting, arquitectura de seguridad, respuesta a incidentes, entre otros. También se debe tener en cuenta capacitar al equipo en las herramientas que el CSIRT decida implementar para dar soporte a los servicios que brindará.

Se deben establecer controles suficientes para la protección de un CSIRT según el grado de importancia que tenga en contraste con aspectos legales, de criticidad, de valor y del impacto de su divulgación o manipulación sin previa autorización, teniendo en cuenta la cantidad de recurso humano para operar el CSIRT.

Por último se recomienda que las organizaciones efectúen una adecuada identificación de activos, ya que esto permitirá al CSIRT establecer prioridades de atención con base a la sensibilidad e importancia de los activos en caso de ocurrencia de un incidente informático, una buena aproximación al procedimiento de identificación de activos es el que se presenta en el Anexo A, el cual se encuentra alineado con la Guía para la Gestión y Clasificación de Activos de Información del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

De igual manera se recomienda incorporar la gestión de riesgos dentro del marco de funcionamiento del CSIRT, ya que esto permitirá preparar al equipo mediante el conocimiento de los riesgos y vulnerabilidades de la organización y por lo tanto aumentar la eficacia al momento de dar respuesta a un incidente, un mecanismo de evaluación de

riesgos puede ser encontrado en el Anexo B, es de aclarar que lo expuesto en los anexos mencionados no representa una camisa de fuerza, simplemente es una base que puede seguir como guía al momento de implementar dichos procesos.

9. BIBLIOGRAFÍA

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. Metodología de análisis y gestión de riesgos para los sistemas de información. UNE71504:2008. Madrid: AENOR. 2008

CAROZO B., Eduardo. Centro de respuesta a incidentes informáticos... ¿Para qué? En: Revista Seguridad cultura de prevención para TI. Vol. 16. 2018. [En línea]. Recuperado en 2022-06-08. Disponible en: https://revista.seguridad.unam.mx/numero-16/centro-de-respuesta-incidentes-inform%C3%A1ticos-para-qu%C3%A9

CENTRO CRIPTOLÓGICO NACIONAL. Guía de Creación de un CERT/CSIRT. España: Editor y Centro Criptológico Nacional. 2011. p. 23.

COLCERT. Acerca de ColCERT. En: Grupo de Respuesta a Emergencias Cibernéticas de Colombia. (2022). [En línea]. Recuperado en 2022-06-08. Disponible en: http://www.colcert.gov.co/?q=acerca-de

ENISA. Como crear un CSIRT paso a paso. ENISA, 2006.

ENISA. HOW TO SETUP CSIRT AND SOC. Good Practice Guide. ENISA, 2020.

FIRST. FIRST Site Visit Requirements and Assessment. rev 3.1. 2020

FIRST. FIRST Teams. En: Forum of Incident Response and Security Teams (2022). [En línea]. Recuperado en 2022-06-08. Disponible en: https://www.first.org/members/teams/#colombia

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Minimum Security Requirements for Federal Information and Information Systems. FIPS PUB 200. Gaithersburg, MD: National Institute of Standards and Technology. 2006.

GOMEZ, Álvaro. Gestión de incidentes de seguridad informática. RA-MA Editorial. 2014.

INCIBE. Tendencias en el mercado de la Ciberseguridad. Madrid, España: INCIBE, 2016. Wout de Natris. 2014

KILLCRECE, Georgia, et al. Organizational Models for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University. 2003

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Activos de Información. 2016.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. 2016.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Incident Handling Guide. NIST-SP 800-61. rev. 2. Gaithersburg, MD: National Institute of Standards and Technology. 2012.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. NIST-SP 800-160. Gaithersburg, MD: National Institute of Standards and Technology. 2016..

National Cyber Security Index. ÍNDICE DE CIBER SEGURIDAD NACIONAL Colombia. En: NCSI (2021). [En línea]. Recuperado en 2021-04-20. Disponible en: https://ncsi.ega.ee/country/co/

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Buenas prácticas para establecer un CSIRT nacional. Washington, D, C: Secretaria General de la Organización de los Estados Americanos (OEA). 2016.

PRESIDENCIA DE LA REPUBLICA. Lineamientos Del Equipo De Respuesta A Incidentes De Seguridad De La Información. En: Cantidad ideal de personas para la conformación del equipo. Colombia. 2019.

WEST-BROWN, Moira, et al. Handbook for Computer Security Incident Response Teams (CSIRTs). 2 ed. Pittsburgh, PA: Carnegie Mellon University. 2003

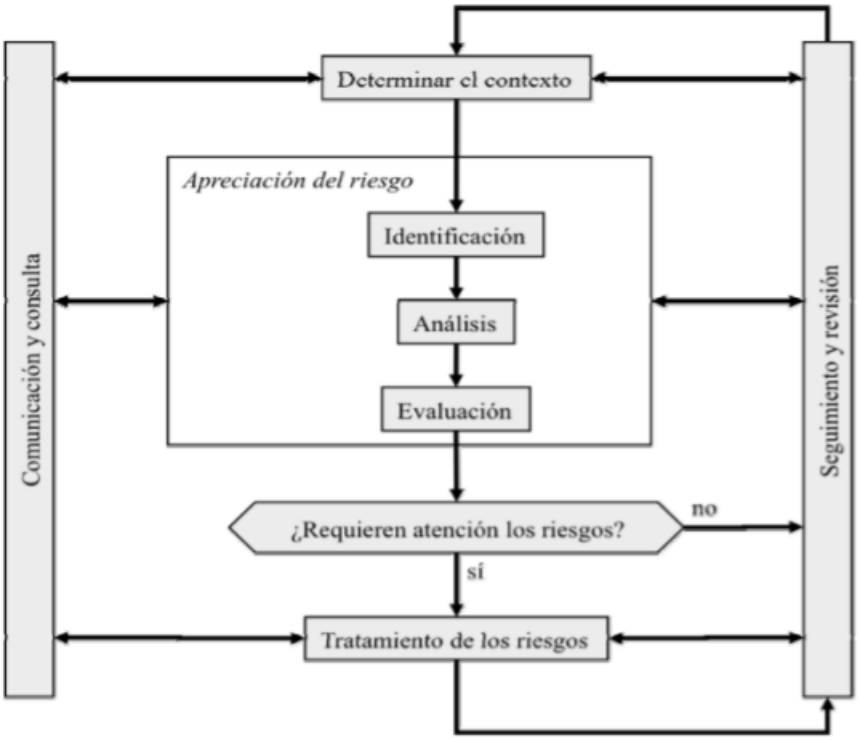
ANEXO A
(Informativo)

EVALUACIÓN DE RIESGOS PARA LA ORGANIZACIÓN

Es necesario hacer un análisis del panorama de riesgos que aporta la información recolectada, por ejemplo, en caso de recopilar información de un análisis de vulnerabilidades de la organización en donde se encuentre una vulnerabilidad que resulte en una posible materialización del riesgo, se debe efectuar un análisis y gestión de los riesgos implicados, para ello existen metodologías como MAGERIT[47], la cual se hará uso para dar desarrollo a este paso.

Un panorama general del proceso de gestión de riesgos es descrito en la norma ISO31000[48] en 7 pasos, los cuales son: determinar el contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento de riesgos, comunicación y consulta y seguimiento y revisión.

Figura 12. Proceso de gestión de riesgos ISO31000



En la metodología MAGERIT el análisis de riesgos es manejado en 4 pasos. El primero es la identificación de los activos, paso el cual ya fue realizado al inicio de este capítulo, el

[47] MAGERIT de gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica actualmente Comisión de Estrategia TIC.
[48]

segundo paso es determinar las amenazas, posteriormente estimar el impacto y por último estimar el riesgo.

Para determinar las amenazas es necesario primero entender el concepto que es una amenaza, una amenaza se puede definir como "*causa potencial de un incidente que puede causar daños a un sistema de información o a una organización*"[49]. MAGERIT en el capítulo 5 del Catálogo de elementos dispone listado de las amenazas más comunes que puedan afectar los activos de información, estas pueden ser plasmadas en una matriz que contenga el activo de información, nombre y la amenaza relacionada.

Figura 13. Matriz de análisis de riesgos MAGERIT 3.0

Activos de Informacion	Nombre del activo de información	Amenazas Metodologia Magerit
[SW] SOFTWARE	Servidor de archivos FTP	[E8] Difusión de software dañino

Fuente: El autor.

El catálogo de amenazas de MAGERIT 3.0, no solo pone a disposición un listado de las amenazas más comunes, sino que también junto con la descripción de las amenazas identifica el tipo de activo y la dimensión (disponibilidad, confidencialidad, integridad, autenticidad o trazabilidad) que puede afectar.

De igual manera en este catálogo de elementos se encuentra un listado de los tipos de activos, el cual sirve como base para efectuar una clasificación de los activos de información ya inventariados y que de esa manera se incorpore la metodología en los procesos.

Una vez determinada la amenaza que puede afectar el activo, se debe evaluar dos aspectos, la degradación o impacto, es decir el daño que causaría la amenaza el cual es evaluado de manera cualitativa y, la probabilidad de ocurrencia, evaluado como una frecuencia de ocurrencia junto con una escala numérica, tal como se propone en el cuadro 14 y 15.

[49] Asociación española de Normalización y Certificación. UNE71504:2008. Madrid: AENOR. 2008

Cuadro 14. Degradación del valor

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: MAGERIT. Metodología De Análisis Y Gestión De Riesgos De Los Sistemas De Información. Madrid: Ministerio de Hacienda y Administración Electrónica. v. 3.0.

Cuadro 15. Probabilidad de ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/100	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Fuente: MAGERIT. Metodología De Análisis Y Gestión De Riesgos De Los Sistemas De Información. Madrid: Ministerio de Hacienda y Administración Electrónica. v. 3.0.

Estos cuadros pueden ser adaptados a las necesidades de la organización e incluso se puede asignar valores numéricos con el fin de que sean más entendibles las matrices de valoración, tal como se observa en la Figura 14.

Figura 14. Matrices adaptadas

PROBABILIDAD DE OCURRENCIA

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	**Muy probable**	5
	A	**Probable**	4
	M	**Normal**	3
	B	**Poco probable**	2
	MB	**Muy poco probable**	1

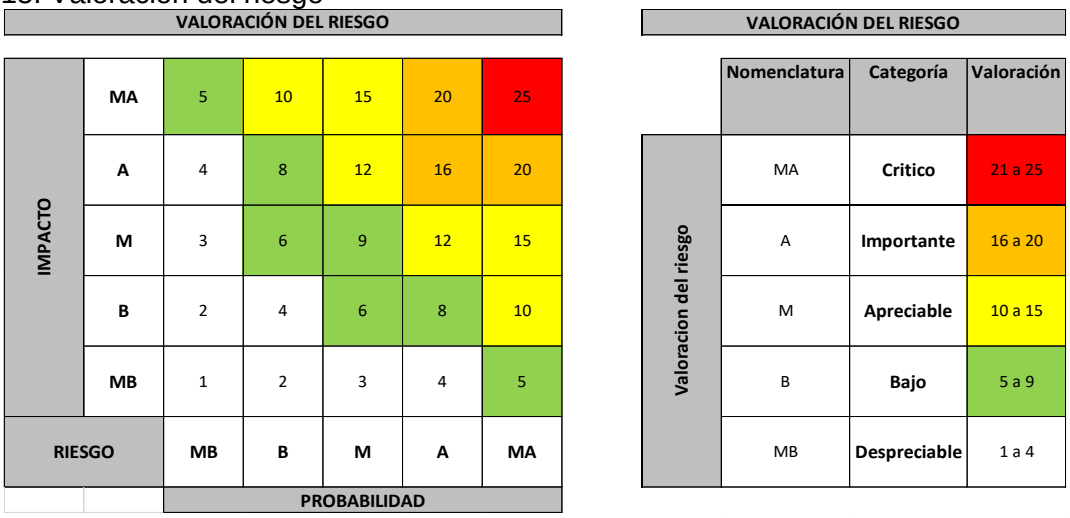
IMPACTO DE LA AMENAZA

	Nomenclatura	Categoría	Valoración
Impacto	MA	**Muy Alto**	5
	A	**Alto**	4
	M	**Medio**	3
	B	**Bajo**	2
	MB	**Muy Bajo**	1

Fuente: Elaboración propia.

Una vez se haga la medición de la probabilidad de ocurrencia y del impacto de la amenaza se puede determinar de manera más precisa el riesgo potencial que representa una amenaza, esto se puede hacer mediante un gráfico de mapa de calor cuyas variables son impacto (eje Y) y probabilidad (eje X), como se indica en la figura 15.

Figura 15. Valoración del riesgo



Fuente: Elaboración propia.

Adicionalmente MAGERIT en el capítulo 6 del catálogo de elementos pone a disposición un listado de salvaguardas las cuales sirven herramientas para reducir el riesgo, esta información puede ser ampliada mediante la consulta del Libro I – Método de la Metodología de análisis y gestión de riesgos de los sistemas de información.

ANEXO B
(Informativo)

FORMATO DE COMÚN AVISO DEL EISPP

Field		Description
Identification Data		
Issuer		Advisory Issuer
Reference Number		An advisory reference number
Date		The date on which the advisory was published
Language		Default language of the advisory
Title		The advisory's title
Abstract		A short abstract that complements the information given in the title.
History Data		
Version History		Information about the advisory's current version/revision, along with history information.
Update Information		Information about the relation of the advisory to prior/later advisories of the same issuer
Vulnerability Classification		
Vulnerability Identifiers		A list of standard identifiers such as CVE numbers, Bugtraq IDs, etc. for the vulnerability.
Confidence Level		Information about the confidence the issuer puts into the presented information.
Vulnerability Category		Description of the vulnerability's cause.
Attack Requirements		Technical requirements needed by an attacker to exploit the vulnerability.
Current Impact		Rating of vulnerability's current impact on IT security.
Immediacy		Information about how immediate the threat posed by the vulnerability is, based on:
	Vulnerability Status	Current stage of the vulnerability in the vulnerability life cycle
	Propagation Method	Level of automation that has been achieved for exploitation
Vulnerability Impact		Rating of the severity of the vulnerability's effect
	Vulnerability Effects	Effects that successful exploitation has on the attacked system
Current Impact		The current impact gives a general assessment of the threat posed by the vulnerability.
Risk		Overall assessment of the risk, taking into account also constituency-specific factors.
System Information		
The system information contains information about the affected systems. Typical fields for specifying such information are		
	Affected Platform	Information about platforms affected by the described vulnerability.
	Affected Software	Information about software affected by the described vulnerability.
	Affected System	Combined information about affected platform and software (instead of above two fields)
	Remarks	Additional remarks, e.g., information about systems that may be affected, are not affected, etc.
Description		
The description section of the advisory contains information relevant for understanding the vulnerability. Typical fields are:		
	Publication Context	Information that puts the advisory into context.
	Technical Context	Information that helps the user to understand the technical context of the advisory.
	Description	Description of the vulnerability/vulnerabilities treated by the advisory.
	Technical Info.	Detailed technical information, targeted more at security experts than the average reader.
	Diagnostic	Information to help the reader to determine whether his system is vulnerable.
Solution		
Solution Introduction		General information about possible solutions.
Solution Sections		Each section describes a possible solution. Sections may be divided by solution type (patch, workaround, etc.), affected system, or both.
Additional Resources		
Additional Resources		References to relevant material such as other advisories.

Fuente: EISPP CONSORTIUM. EISPP Common Advisory Format Description. 2003