CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Technical Report · July 2020

DOI: 10.13140/RG.2.2.29810.73925

CITATION
1

READS
811

1 author:

Emanuel Ortiz
Red de Investigación Academica en Ciberseguridad
22 PUBLICATIONS **21** CITATIONS

SEE PROFILE

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Presentación de la Red de investigación Académica

La Red de Investigación en Cibercrimen y Ciberseguridad "RedCiber" realiza un trabajo colaborativo a través de sus nodos de cooperación académica, los cuales trabajan en diferentes líneas de investigación y apoyan el trabajo de los otros nodos construyendo datos de alta importancia para investigadores de las ciencias forenses y áreas afines a la informática, Ciberseguridad, Cibercrimen y la Cibercriminologia.

El concepto y creación de la Red de Investigación en Ciberseguridad y Cibercrimen “RedCiber” en alianza de la Asociación Internacional de Informática Forense, tiene como objeto difundir, ampliar y reconocer a los expertos en estas áreas fundamentales para la Seguridad Digital, sin desconocer la interdisciplinariedad o multidisciplinariedad que debe responder a las necesidades actuales de la seguridad de forma integral.

Abstract

La adopción de buenas prácticas para la administración, tratamiento y gestión de los incidentes informáticos es una de las practicas más necesitadas en todos los sectores de la economía; con ella, junto a la integridad, disponibilidad y confidencialidad de los datos. Por esta razón, para que sea de fundamental valor poder unificar una metodología que permita afianzar la creación de equipos en seguridad cibernética, debe tener un aporte de investigación de esta fenomenología, la cual facilita y orienta la dinámica constante de la Ciberseguridad, teniendo en cuenta un enfoque técnico desarrollado hacia los distintos escenarios que se pueden presentar en materia de Cibercrimen.

Palabras Clave: *Ciberseguridad, Seguridad en la Información, Cibercrimen, Seguridad Cibernética, Ciberataques, Estrategia en Ciberseguridad, transformación digital.*

Antecedentes

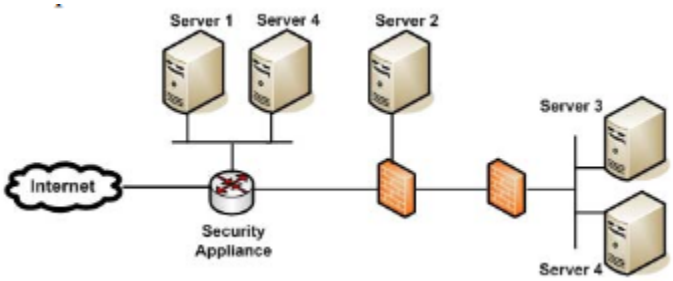
Los hechos por medio del tiempo han sido evidentemente complejos en materia de Ciberseguridad; algunos de ellos los señala (Ortiz Ruiz, 2019) en los orígenes del Cibercrimen, sin embargo es importante elevar estas connotaciones y divisiones a través de los avances tecnológicos de la humanidad; si bien es cierto el Cibercrimen hace parte de un título grande y contextualizado en todo, estas afectaciones a la ciberseguridad y Seguridad Digital tuvieron nacimiento mucho más antes de lo que imaginamos; por ende la importancia siempre de los sectores de la Economía en brindar unos aspectos centrales y estandarizados para poder focalizar los puntos de acción e instrumentalizar todos los enfoques que la industria requiere en esta materia.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

De la misma manera como lo cita (Rohmeyer & Bayuk , 2019) es sus páginas iniciales, en donde indica que debemos conocer nuestro adversario en cada una de sus facetas de la economía; por ello es importante enfocar los esfuerzos en desarrollar tecnología que posea esos estándares que la industria merece a partir de las amenazas que pueden afectar el mundo y sus consumidores. Es a partir de ese dialogo en que las ciberamenazas cobran un gran valor a partir del impacto que pueden causar; y sobre estas lo significativo que se considera, la creación de equipos de investigación cibernética en ciberseguridad y añadir componentes esenciales para su desarrollo.

Una de las características esenciales de estos equipos interdisciplinarios en Ciberseguridad, deben enfocarse en las acciones de "*Core Bussiness*" y de la idea del negocio, aspectos esenciales como su orientación en materia teórica y práctica, pueden desarrollar aún más su eficiencia o efectividad en el momento de permitir afianzar su infraestructura, el enfoque del recurso técnico, humano y especializado que este le merece. A partir de esto, también es importante mencionar sus capacidades de enrolamiento estratégico con el conocimiento de su adversario, razón que involucra mucho más la sinergia de la parte técnica, con la jurídica, legal y tecnológica.

NIST involucra estos aspectos, en su documento (NIST & SP 800 61) involucra y detalla varios aspectos de base técnica para poder orientar la infraestructura técnica como se implementaría en para sus atributos en materia de infraestructura, (ver Imagen).



Tomado de: (Penedo, 2005)

En este sentido hay varios aspectos a tener en cuenta para la creación y desarrollo escalado de un Equipo de Investigación Cibernética, y es primer hacer una distinción de los **Equipos de Respuesta a Incidentes Informáticos**, llamados CSIRT´s por sus siglas en ingles Computer Incident Response Teams, esta características enfocada en es los equipos para la respuesta a incidentes, está enfocada en sus atributos esenciales, como lo documenta el Foro de Equipos de Respuesta a Incidentes, por sus siglas en inglés FIRST (Forum Incident Response Teams (FIRST, s.f.)), el cual desde 1989 se viene

desarrollando como una organización cerrada para compartir información de intereses propios de los equipos de respuesta incidentes a nivel global. Asimismo, a partir de los años 90`s ha venido creciendo esta comunidad, en la cual se comparte información sobre incidentes de seguridad relacionados con la seguridad informática y la Ciberseguridad en todos los sectores.

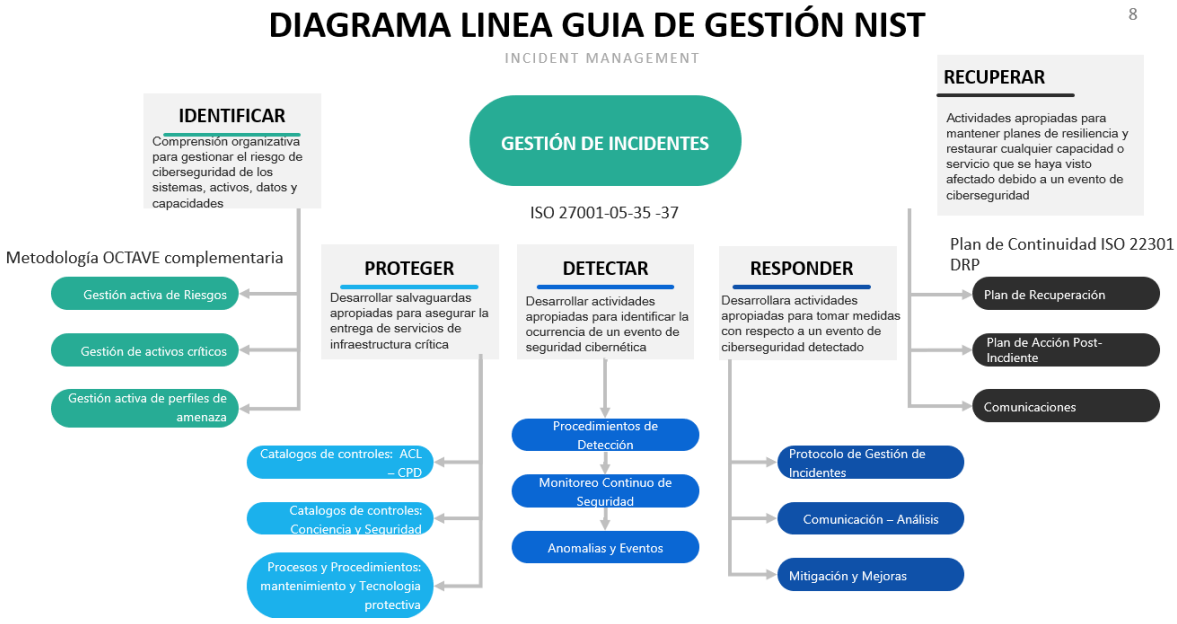
Con la explotación del internet y los problemas de seguridad en las redes de comunicación, en el año 1988; y por causa de un incidente denominado "Internet Worm", el concepto CSIRT (*Computer Incident Repsonse Team*) proviene de una historia relacionado con un evento histórico que transformó el pensamiento de la seguridad en cuanto a la creación de los equipos de seguridad, por cuanto, solamente se tenían pensados para fortalecer la seguridad en las redes (RFC 2196, 1997) y estaba destinado apara administradores locales de redes e infraestructuras asociadas a las políticas de seguridad de aquellas infraestructuras; en ese mismo sentido, el primer coordinador o CERT/CC (Computer Emergency Response Team), el cual se crea en 1997 con la finalidad de coordinar a los diferentes sectores de la industria y la economía para la creación de una analogía, denominada CSIRT.

Los CSIRT`s bajo esta denominación, son aquellos que permiten dinamizar bajo una línea base estándar de gestión, los diferentes aspectos de esas emergencias y buenas prácticas para prevenir situaciones que afecten los tres pilares de la seguridad en la información en determinado sector o "core business" asociado a un riesgo cibernético determinado o definido; el cual permite no solo llevar a buena optimización su labor, sino permite, ser escalativo, según sus focos de atención y preocupación en la industria.

El libro de mano "Handbook for Computer Security Incident Response Teams (CSIRT`s) en su segunda edición (Moira J. , Don , & Klaus, 2003) menciona la importancia de los Equipos de Respuesta a Incidentes para las diferentes necesidades de la industria tecnológica. En ese sentido muchas de las capacidades de un equipo de seguridad cibernética, las cuales poseen atributos esenciales, como: procedimientos, activos, estratégicos y operacionales, están enfocados en esos mecanismos de estructura; así como lo relaciona en primera medida las características de responder ante un incidente ó incidente handling, lo cual permite, establecer unas bases focalizadas hacia el personal que debe ser parte del equipo en este aspecto técnico.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Es en este sentido que es primordial desarrollar la operación enfocada en crear, operar y desplegar actividades de gestión de incidentes; y a partir de ello se poseen varias líneas base para poder enfocar las acciones que permitan este tipo de objetivos:



Elaboración Propia: Metodología de gestión de Incidentes: Línea base NIST CSF

La línea base a destacar para este inicio de creación de un CSIRT está enfocada en la participación de un modelo de ciberseguridad ya aplicado ante una dinámica del negocio en particular, así mismo en el desarrollo de este mismo artículo se puede ir visualizando cuales son las ubicaciones en la grilla de partida para crear un Equipo de Respuesta a Incidentes, teniendo en cuenta el marco de trabajo NIST (Cybersecurity, 2018) creado y modificado para poder orientar a la industria tecnológica en este tipo de mecanismos.

De tal manera que NIST responde a estas particularidades, dentro del cual se puede afianzar la importancia de crear equipos de seguridad cibernética basados en esta metodología, asimismo poder enfocar las tareas que poseen muchos de los equipos interdisciplinares en la gestión y tratamiento de incidentes.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Línea base y guía fundamental para interoperabilizar la Metodología

NIST mediante su modelo CSF (Cybersecurity Security Framework) define la orientación de tres aspectos esenciales: el "Core bussiness", los tiers de riesgo y el perfil del marco de trabajo, distribuido en la siguiente gráfica:

Table 1: Frameworks Comparison

Framework	Control Categories	Control Objectives	Activities
NIST CSF [1]	Functions (5)	Categories (22)	Subcategories (98)
ISF [3]	Categories (4)	Areas (26)	Topics (118)
ISO27001 (2013) [4]	Clauses (14)	Control objective (35)	Controls (114)
COBIT5 (2013) [5]	Domains (5)	Processes (37)	Practices (210)

Tomado de: (Sultan & Majeed , 2014)

En ese mismo sentido permite orientar las necesidades en tres aspectos fundamentales, las categorías de las categorías de control, objetivos de control y actividades, clasificadas mediante las necesidades de la organización o los componentes diagramados y categorizados, poseen un valor fundamental para garantizar la triada de la seguridad en la Información.

La Norma ISO 27037 (ISO, 2014), la cual indica las buenas prácticas para la gestión de la evidencia digital de un incidente informático o de ciberseguridad recoge los aspectos fundamentales de una tarea que cubren los CSIRT´s y equipos de investigación Cibernética, por ende, es importante que a partir lo que se indica por (Sultan & Majeed , 2014) cada una de estas categorías se deben abordar a partir de lo siguiente:

- **Cubrimiento del marco de trabajo** (Cybersecurity, 2018) **CSF (Cybersecurity Framework) el cual promueve las diferentes líneas base.**
- **El marco de trabajo ISF (Information Security Framework)** (Framework & Security, 2020)
- **Marco de trabajo ISO 27001 (2013)**
- **COBIT 5 (2013)**

En ese orden de ideas, existen 5 marcos de trabajo que poseen la categoría esencial para estructurar un equipo de investigación en seguridad cibernética; en este caso se selecciona el marco de trabajo NIST que cubre comparativamente una estructura más abierta y adecuada para la formación de estos equipos de seguridad cibernética. Actualmente la Universidad Carnegie Mellon por medio de su paper *"Coordinated Cybersecurity Incident Handling*" (Osorno, Millar, & Rager, 2020), en el que


CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

se menciona de qué manera poder formalizar un equipo de respuesta a incidentes cibernéticos dirigidos a la Ciberseguridad; en este mismo se relaciona y enmarca un proceso mediante el cual conlleva entender cuáles son los ciclos de información involucrados en la creación de estos tipos de equipos de seguridad. Cada uno de estos ciclos permite aislar o focalizar las acciones dirigidas a procesos alternos, como lo es, la "Respuesta y Gestión a Incidentes de Seguridad", los cuales permiten que por medio de los ciclos o fases se cumplan su preparación, detección y análisis, contingencia, erradicación y recuperación y actividad post-incidente.

Para ello, también se vincula una actividad que tiene como finalidad entender el ciclo de gestión del incidente, las taxonomías, el flujo de información sistematizada, y la generación de marcas de tiempo a los ciclos de respuesta dirigida a los *"Stakeholders"* o partes interesadas de esa información. Estos incidentes de seguridad cibernética tienen un propósito encargado de poder desplegar este tipo de acciones, y las mismas están distribuidas en la conformación del equipo de respuesta a incidentes cibernéticos.

Por ende, las mejores practicas están asociadas a las categorías previamente establecidas y relacionadas mencionadas con un estándar inicial para poder comprender el enfoque de inicio de este equipo de respuesta; de tal manera que los roles asignados a cada uno de los perfiles puedan aportar al flujo de la información del equipo de seguridad cibernética. Del mismo modo, esta estandarización como lo define (Cybersecurity, 2018) posee diferentes características que se ajusten a los tipos de entradas de información que garanticen su tratamiento y efectividad en las tareas.

En este orden de ideas es importante apoyarse del documento especial SP (800-61), el cual se trata de la vinculación de todas las buenas prácticas enfocadas en la creación de equipos y comunidades de colaboración en ciberseguridad llamados (ISACS) *Information Sharing and Analysis Centers*. Mediante esta metodología, se vinculan a otras terceras partes que permiten orientar el ciclo de comunicación, a saber:

- Los proveedores de servicio de internet
- Administradores de IP[1] de los atacantes
- Proveedores de software
- Otros equipos de respuesta a Incidentes
- Partes externas afectadas

De otro modo, para poder explicar cada una de estas categorías, dependen del alcance del equipo o grupo de personas que van a organizarse para poder estructurar ese CSIRT o CERT, para lo cual es

[1] Internet Protocol

importante definir su objetivo principal y aquellos elementos dentro del cual debe enfocarse su estructuración, de la siguiente manera:

Figura elaborada por el autor y complementada según los estándares de la División CERT – Universidad Carnegie Mellon

Analistas TRIAGE 1: Son los enfocados en clasificar e investigar inicialmente el incidente bajo el marco de conducta de la guía NIST Special Publication **800-61 pág. 21** donde se establece el ciclo para la gestión de un incidente, descrito de la siguiente manera:

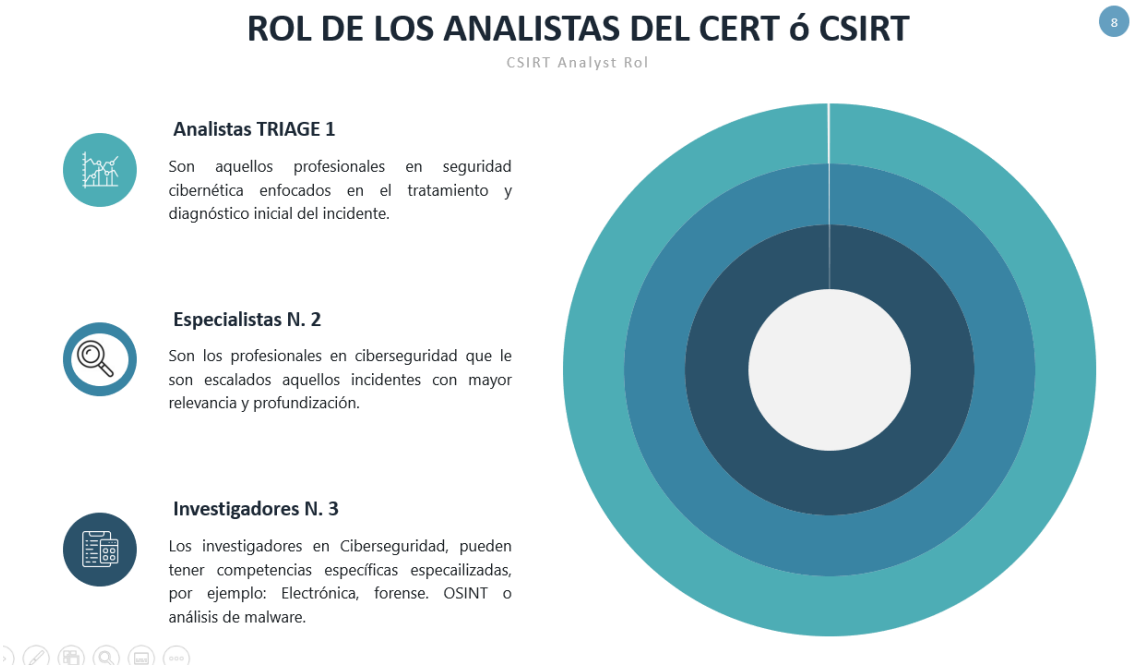
CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Figura tomada y mejorada para ilustrar el ciclo de la gestión de un incidente NIST **Special Publication 800-61 Revision 2**

Es importante tener en cuenta La importancia por parte del equipo de conocer cual es su estructura de actuación, la podemos claramente revisar frente a la guía de atención y gestión de incidentes de NIST.

Dentro del ciclo de la gestión de un incidente se define el primer rol específico para la primera línea de atención, en este caso los *"Analistas TRIAGE (Clasificación de urgencias) 1"*, en este sentido se persigue determinar en la etapa de respuesta ante la gestión comunicada (o) por parte de los clientes, organizaciones, academia, industria o economía. Sobre ese incidente, se le atribuye una priorización del mismo y posteriormente la identificación de la etapa o escalamiento debido determinado por sus roles, así:

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA



Los especialistas No. 2, son aquellos a los que le son escalados los incidentes para la investigación avanzada sobre posibles herramientas para su investigación por medio de los procesos de apoyo interno que posee el equipo de seguridad cibernética, a partir de ello, poder enfocar esfuerzos hacia la evidencia documentada por los analistas TRIAGE, revisando su clasificación del incidente y los aspectos a destacar sobre este. Esta actividad se determina a partir de la casuística y la taxonomía del incidente, que para efectos prácticos tiene que ver con determinar si el incidente tiene efectos de *pivote, de lateralidad o de propagación* frente a un activo crítico posterior o determinado en el momento de la gestión.

Estos tres aspectos subrayados están asociados a la taxonomía del incidente para lo cual es necesaria una capacidad que poder orientar lo señalado en la página 15 del reporte técnico "**CIBERSEGURIDAD**: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA" (Ortiz Ruiz, 2020), a partir del conocimiento de la estructura del incidente y su aplicabilidad, si fue ocasionado en la capa de red/enlace, transporte, sesión, presentación o aplicación.

Sin embargo para poder enfocar esta estructura de actividades y roles de los integrantes del equipo técnico en ciberseguridad, es importante definir los aspectos a determinar sobre la importancia y

relevancia de la información relacionada en el incidente; así lo documenta (Gartner, 2018), en donde define la importancia de 10 aspectos de relevancia en materia de *respuesta y detección*, y en razón a este, el criterio de poder definir posturas de análisis para la protección de los sistemas vinculados. Estos aspectos se enmarcan en el supuesto de que el especialista que hace parte del CSIRT, defina para el análisis de criticidad vs impacto. Para medir estas consecuencias que pueden afectar la operación, y posteriormente generar el impacto negativo hacia la recuperación del negocio, también se puede citar la publicación especial de (NIST, Contigency Planning Guide;, 2010), el cual permite establecer el *"Cyber Incident Response Plan",* el cual permite visibilizar por parte del especialista del CERT o CSIRT cuales son las estrategias tácticas y operativas para poder recomendar acciones de mitigación, erradicación, contención y recuperabilidad de los activos críticos afectados.

En cuanto al investigador *No. 3* referido en la gráfica de los roles, la persona debe tener un alto conocimiento en actividades especiales a desarrollar, a partir de estas capacidades específicas se pretende elaborar una tarea post- incidente que guarde los mínimos requeridos para poder afianzar lo que el especialista No. 2 ha suministrado (*incident notification*) a la parte interesada.

Dado este conocimiento previo, el investigador dentro de esta capacidad especial, podrá ejecutar análisis sobre malware especializado en el campo forense, determinar circunstancias que faciliten orientar una investigación cibernética aplicada en OSINT, darkweb, estándares, regulaciones o mediante una temática especializada como "threat hunting" traducido al español como cacería de amenazas.

Esta figura puede ser flexible a las necesidades de la organización, de tal manera que permita viabilizar una escalabilidad y crecer dentro de la respuesta y gestión a incidentes, también un enfoque de inteligencia de amenazas cibernética, inteligencia cibernética aplicada o investigación digital al cibercrimen. Estos escenarios pueden nacer del alcance del CSIRT, siempre y cuando se adopte un eje transversal que facilite la interacción entre sus componentes. Uno de estos enfoques es NIST y su marco de trabajo, el cual, a partir de distintos aspectos se desarrollan con base de cinco fases fundamentales de ciberseguridad a saber:

- **Identificar**
- **Detectar**
- **Proteger**
- **Responder**
- **Y recuperar**

Estas cinco categorías permiten equilibrar el marco de orientación a la distribución antes planteada, y facilita el Inter relacionamiento entre cada uno de estos atributos desarrollados por los roles, permitiendo con esto, que otras normativas establezcan su interacción rápida y efectiva por ejemplo la ISO 27035 como buenas prácticas para la gestión de incidentes, como se menciona en la página 4 de este artículo.

Además, como se menciona en el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon (Software & Carnegie , 2020) para poder integrar un CSIRT en la capa de concienciación y tomar conciencia en materia de ciberseguridad se requieren unas herramientas, desde la construcción de un programa de colaboración para compartir información y que identifique el contexto o *situational awareness*; después de ello, cumplir lo con los siguientes requerimientos:

- ***Gap Analysis of Current Services – Análisis de los servicios actuales:*** que brinda un CSIRT enfocado en poder entender y reconocer el entorno en el cual participen los proveedores de las herramientas que se requieren para poder soportar la información que se genera por parte del CSIRT o CERT, asimismo enfocar los esfuerzos en que ese grupo de personas o partes interesadas observen ese resultado como propio para su misma naturaleza.

- ***Stablish a Resource Library Portal with Knowledge Management Document Searching Capability - Establecer un portal de biblioteca de recursos con la búsqueda de documentos de gestión del conocimiento:*** esta capacidad está orientada a poder establecer un repositorio de información que efectivice la obtención de datos y resúmenes de los reportes relacionados (alertas, informes o inteligencia de amenazas).

- ***Customizable Feeds and Alerts Related to Your Region, Infrastructure, and Internal Environment– Fuentes y alertas personalizables y relacionadas con su región, infraestructura de carácter interno:*** esto permite que se identifique los datos de interés sobre sistemas operativos afectados, vulnerabilidades, filtrado de información relevante en gráficas y particulares a la información que se requiera en este sentido.

- ***Ability to Integrate Organizational Information and Correlate with Provided Feeds - Capacidad para integrar la información de la organización y correlacionarla con las fuentes proporcionadas*:** de la misma manera que debe permitir que se tomen datos privados y no se comparta con nadie, esto garantizará la confidencialidad de la información y que ejerza sus funciones únicas de CSIRT.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

- ***Ability to Automate Actions for the CSIRTs Internal Environment - Capacidad para automatizar acciones para el entorno interno de los CSIRT*:** permitirá de igual manera estructurar el servicio y facilitará que se puedan agregar IP, dominios o sitios a las listas negras, agregar firmas para la detección en [2]IDS, o análisis de malware, obtener reportes y establecer nomenclaturas asociadas a las necesidades de las partes interesadas.

- ***Secure Information Sharing Between Vetted CSIRTs – Capacidad para compartir información entre CSIRT´s:*** esencialmente está compuesta por Aunque la información pública puede ser muy útil para los CSIRT para información general sobre tendencias e indicadores, a menudo debe haber una discusión más detallada de la actividad real, análisis, causa raíz y remediación de lo que es posible en un entorno público. Debe haber una manera de tener discusiones seguras e intercambio de información, a través de canales protegidos y solo para CSIRT investigados. También sería útil tener alguna identificación de los demás. que tienen experiencia en diversas técnicas y herramientas de análisis, detección o mitigación a las que un CSIRT podría acceder por ayuda o consejo.

- ***Ability to Get Feed of Known Fixes – Capacidad para obtener información sobre soluciones: conocidas:*** está vinculada con una biblioteca de recursos que facilitarán la obtención de información para dar solución a necesidades.

- ***Real-World News – Noticias que involucran Seguridad Cibernética:*** esta información estaría específicamente relacionada con las actividades de infraestructura crítica en curso, donde se reúnen organizaciones internacionales, donde los tomadores de decisiones se reúnen para conferencias, cumbres, actividades deportivas o culturales, e información similar que se puede utilizar para proporcionar contexto a las actividades de redes y sistemas que se están presentando.

- ***Continuous Information Collection, Correlation, and Analysis – Información de continua recolección, correlación y análisis:*** tiene la capacidad de medir el impacto de las amenazas, su propio entorno, las fuentes de confianza de su detección, las estrategias para su mitigación y la evolución de análisis frente estos aspectos.

[2] *Sistema de Detección de Intrusos: IDS (Intrusion Detection System)*

- ***Assistance in Performing Impact Analysis – Asistencia en el mejoramiento del análisis de impacto:*** define aspectos que involucre la definición de actores de la amenaza, procurar entender donde ocurren los ataques a la infraestructura, generar conciencia situacional para comprender en donde ocurren estas vulnerabilidades, o la causa raíz para generar defensas, y realizar inversiones en ciberseguridad.

- ***Include Information on Emerging Trends – Incluir información de amenazas Emergentes:*** establece una biblioteca o repositorio de tecnologías, para probar acciones para mitigar y compartir información recolectada establecer simuaciones frente a escenarios para la predicición y análisis de amenazas que permitan medir su impacto frente a un *Common Vulnerability Scoring System (CVSS)*, que puede ser desarrollado para ayudar a medir y entender el impacto de estas amenazas dentro de la entidad u organización. Esto permitirá evaluar los records temporales priorizados y las actualizaciones que requieren estos CVSS.

- ***Include Visualization of Trends and Other Situational Awareness Information – Incluir visualización de tendencias y otra información de conciencia situacional:*** esta capacidad permitirá entender rápidamente la actividad maliciosa, su curso y su impacto para reducir el tiempo de respuesta como lo argumenta (Marc, Grégory) sobre los tipos de procesos cognitivos para analizar la información presentada. Por lo tanto, estos procesos (percepciones, comprensiones, proyecciones, resoluciones) y contextos (gestión, seguridad, operaciones) son las que se deben ajustar para la toma de decisiones.

- ***Include Different Levels of Information – Inlcuir diferentes niveles de información:*** estos niveles de información que se comparten deben ser insumo para la generación de tendencia para el aprovechamiento de esta información. Algunos indicadores para la generación de análisis y poder aprovechar efectivamente esta data asociada, que permita personalizar los intereses de análisis.

Como se describe en estas *14 funciones* que debe tener un CERT o CSIRT, ajustado a las buenas practicas que obedecen a su alcance y propósito. Los equipos de Seguridad Cibernética deben propender por establecer los mecanismos necesarios para fortalecer de manera escalada, según las necesidades que posea la organización, o las que se vayan a presentar en un futuro. Estas funciones están sujetas a la visión de transformación digital que posea la entidad frente a sus retos más cercanos.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Posterior a esto, mediante el presente articulo se define diferentes complementos a los requerimientos y funciones que un CERT o CSIRT deberá contener para poder facilitar y orientar su operación. A partir de ello, es importante ir adhiriendo o estableciendo conductos naturales de flujo interdependientes para poder mejorar la investigación cibernética y sus componentes.

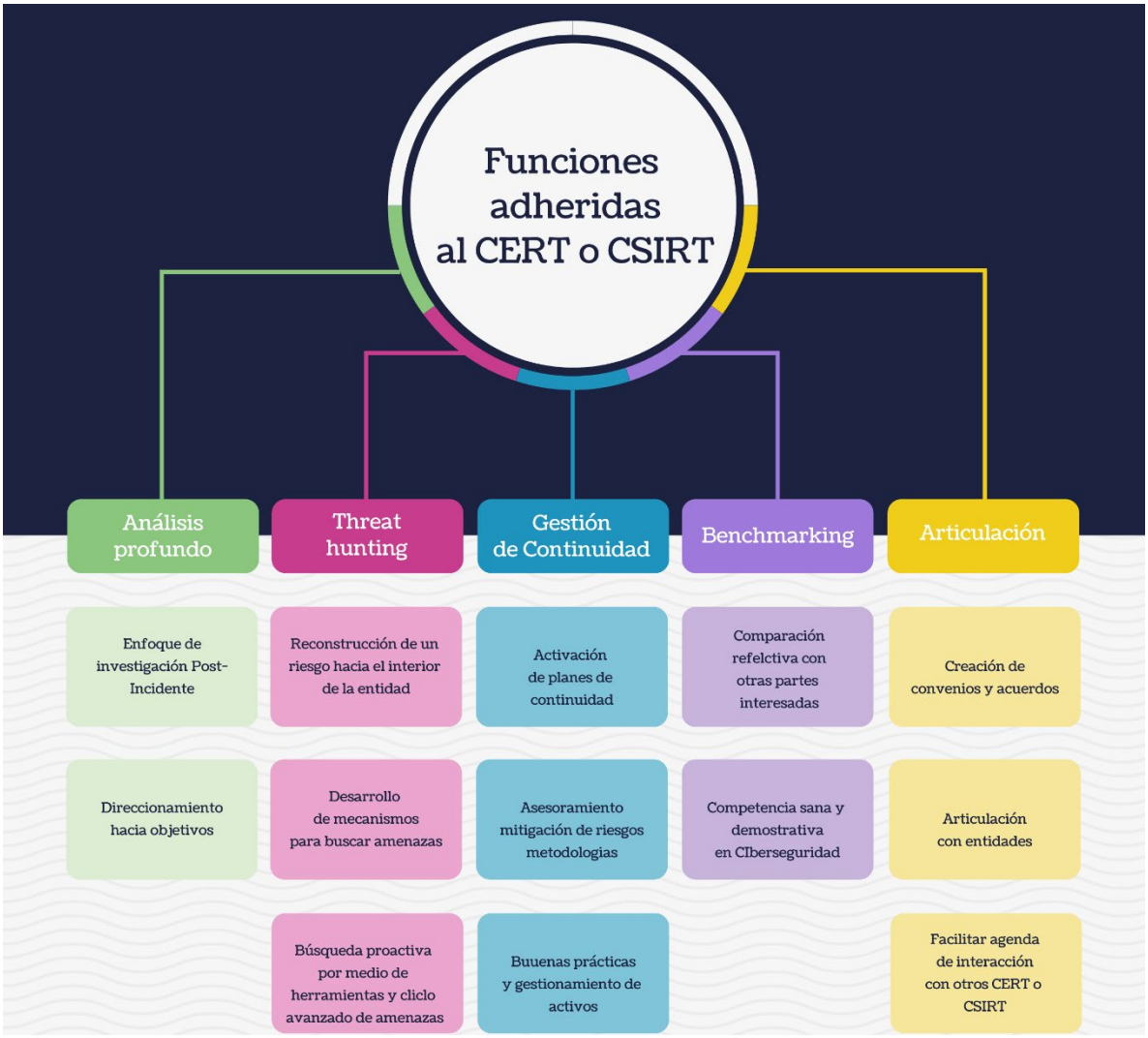
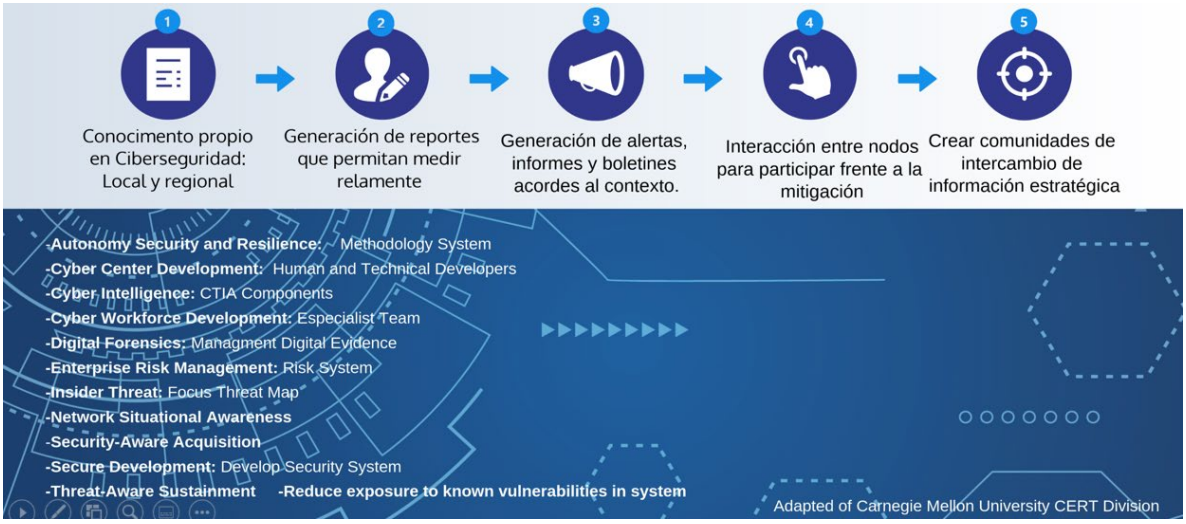


Figura elaborada por el autor en el fortalecimiento de las funciones del CERT o CSIRT

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Estas funciones adheridas al CERT o CSIRT están estructuradas en obtención de información mediante *Indicadores de Compromiso (IoC),* para ayudar a crear contenidos que permitan llevar a un nivel de madurez como lo señala la (Carnegie, Mellon University, s.f.) a partir de 12 características



esenciales:

Figura elaborada por el autor para ilustrar los 12 componentes de un CERT
(https://www.sei.cmu.edu/about/divisions/cert/index.cfm#CERTRecentlyPublishedVulnerabilityNotes)

- **Seguridad autónoma y resiliencia:** Desarrollar y mantener las mejores prácticas en seguridad y resiliencia y garantía en el desarrollo, construcción, y empleo de sistemas de aprendizaje automático.
- **Centro de Desarrollo Cyber:** Desarrollar practicas medibles y repetibles para preparar a las organizaciones en Seguridad Operativa.
- **Ciber Inteligencia:** Estudiar y describir los comportamientos y capacidades de los ciber atacantes e identificar las propiedades de sus métodos.
- **Grupo de Desarrollo de tarea Cyber:** Mantener una fuerza de trabajo cibernética bien equipada para poder respaldar con las necesidades de seguridad Cibernética.
- **Digital Forensics:** Administración de la evidencia Digital bajo las buenas prácticas para la respuesta y análisis a incidentes utilizadas por las organizaciones a medida que evoluciona el panorama tecnológico y la sofisticación de los adversarios.
- **Gestión de Riesgos Empresariales:** Desarrollar practicas medibles que permitan a las organizaciones medir y mitigar riesgos.
- **Amenazas internas:** Detectar y mitigar el impacto de las amenazas internas y reducir su ocurrencia en las organizaciones.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

- **Conciencia situacional de la Red:** Analice el terreno a medida que evolucionan los activos de riesgo, medir la actividad del adversario y priorizar la respuesta de las amenazas.
- **Adquisición de Seguridad:** Aborde las vulnerabilidades y planifique las amenazas antes, y de manera más efectiva en el ciclo de vida de la adquisición.
- **Desarrollo Seguro:** Evaluar las plataformas a través del análisis del Código fuente para asegurar que se adhieran a las mejores prácticas de seguridad.
- **Evaluación del Sistema y plataformas:** Evaluar el software, dispositivos y sistemas de diseño y origen desconocido para encontrar vulnerabilidades y estrategias para defenderse de posibles ataques.
- **Sostenibilidad consciente de la amenaza:** Reducción de la exposición a las vulnerabilidades.

Estos elementos están debidamente orientados bajo un ciclo de información documentado como: Crear, Almacenar, Usar, Compartir, Archivar y Destruir, lo que permite elaborar planes continuos de aprendizaje y entrenamiento enfocados en las necesidades de las partes interesadas, por ende, es importante determinar la visión del equipo de seguridad cibernética. En la creación de estos grupos de seguridad el 70% de organizaciones consideran la promoción del entrenamiento, permitiendo con este reforzar los conocimientos que se deben adquirir, según (Study, ISC Cybersecurity Workforce) el 81% de los encuestados manifestó que manifiestan que requieren alguna certificación para prepararse para estos futuros roles. Sin embargo, con el derecho de la información actualmente, muchas de estas están asociadas a un estudio individual y enfocado en sus necesidades.

Para la creación de un CERT o CSIRT, es importante definir sí los estudios complementarios son los suficientes para lograr ocupara estas expectativas para su funcionamiento y correcto análisis. Características relacionadas con el *Cloud Computing Security, Security Engineering and Administration, Risk Assessment, analysis, and management, Goverannce, risk management and compliance (GRC), Security and threat intelligence analysis, Penetration testing, Intrusion detection y Network monitoring*.

Estos escenarios están asociados a la creación de habilidades para el fortalecimiento de un grupo de tareas cibernéticas caracterizado por su evolución y los parámetros esenciales, enfocados de la siguiente manera:

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Habilidades y competencias

Figura elaborada con el fin de evidenciar la evolución de un CERT o CSIRT de acuerdo a sus habilidades y competencias

La categoría especial señalada como *skills* especiales, están enfocados en el tratamiento de investigaciones cibernéticas profundas que más adelante se tocarán en el presente artículo.

Tareas generales realizadas por un CERT o CSIRT

Checklist del incidente (*Fase Detección y Análisis*):

- **Determinar cuando ocurrió el incidente**
  - Identificar y analizar los indicadores o precursores.
  - Mirar y revisar su correlación
  - Realizar investigación
  - Empezar la documentación *(Obtención de Evidencia)*
- **Priorizar el incidente basado en los siguientes factores *(impacto funcional, impacto sobre la información, esfuerzo de recuperabilidad)***
- **Reporte a la persona o parte interesada *(Externa o Interna)***

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

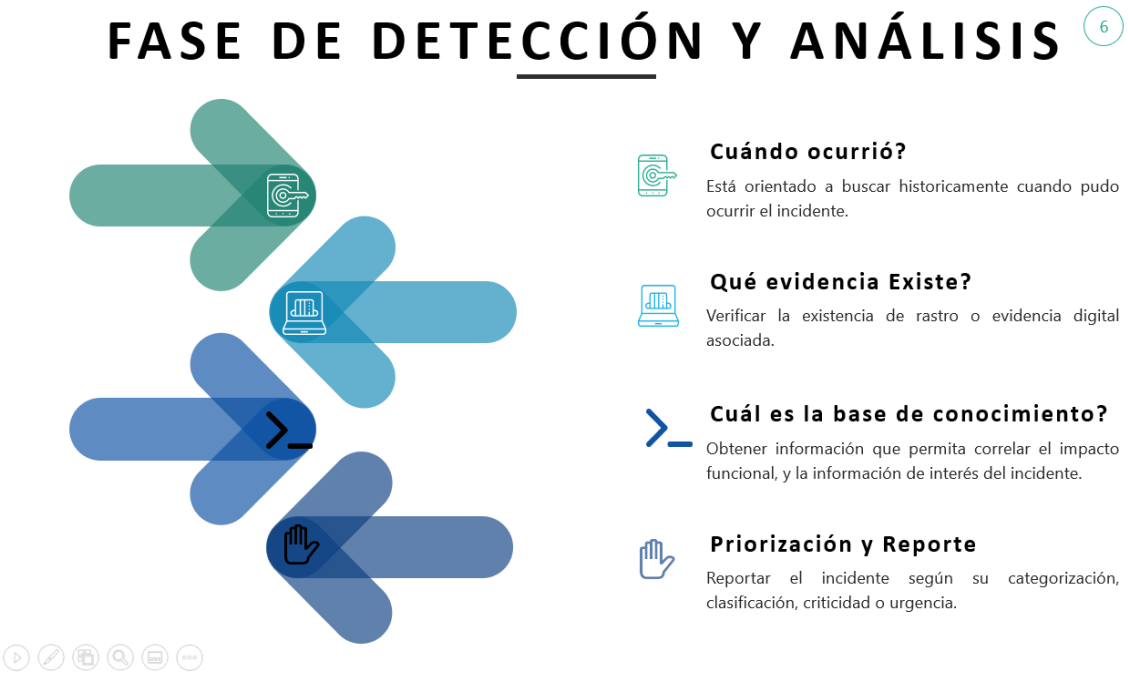


Figura elaborada con la finalidad de explicar la primera fase de la gestión de Incidentes

Es importante en esta etapa definir en la sección de análisis y Triage (Pág. 8-9) establecer la criticidad y la urgencia de comunicación a las partes interesadas, permitiendo, por medio de esta, la facilitación del conocimiento de una tabla que permita medir la probabilidad y el impacto ocurrido por un ciberataque. Dentro de esta misma metodología implementada en este artículo, es conveniente realizar constantes ejercicios de casuística enfocados en estas dos variables (Probabilidad e Impacto).

Espacio dejado a propósito

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Esta tabla de probabilidad tiene como finalidad ilustrar los posibles eventos que se pueden materializer mediante una línea de ***ocurrencia, catalogada del 4-7***, lo cual es efectiva dentro de los numerals 8-9 y 10 en sus categorias alto y crítico.

Figura elaborada y sugerida para medir la probabilidad basado en tres niveles (medio, medio alto, alto y crítico)

Posteriormente se sugiere, cruzar la Tabla de probabilidad (ilustración anterior), con la tabla de impacto sugerida para la comunicación a las partes interesadas, de la siguiente manera:

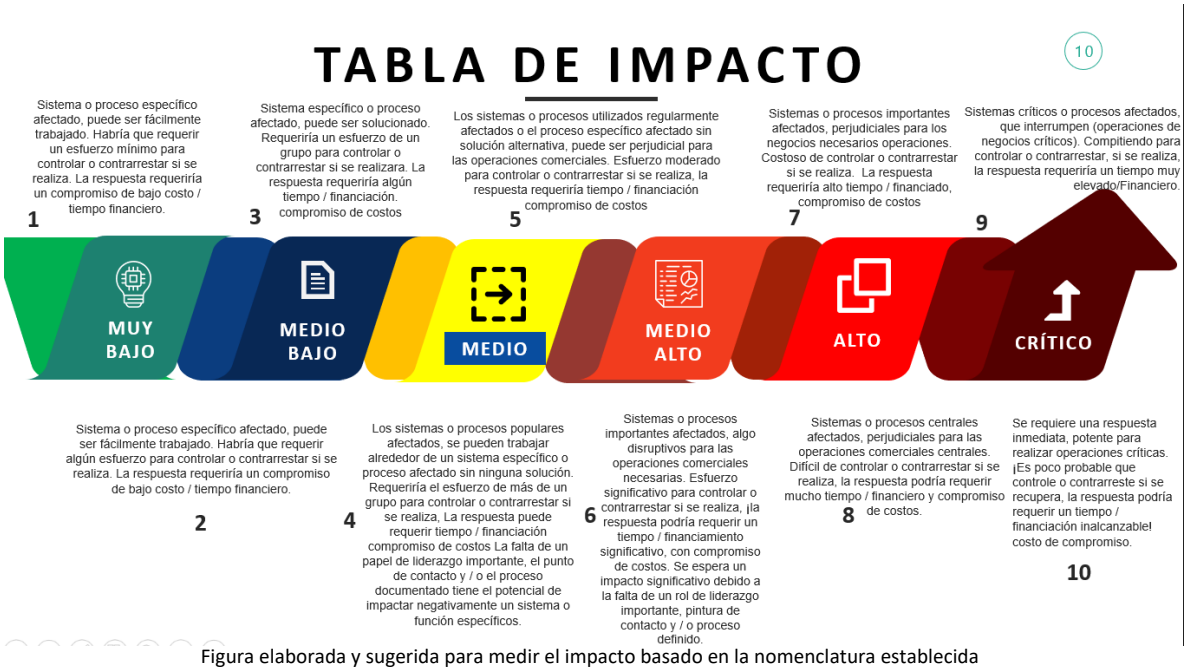


Figura elaborada y sugerida para medir el impacto basado en la nomenclatura establecida

Por medio de esta relación probabilidad vs impacto se podrá correlacionar los aspectos que debe tener en cuenta el analista con funciones en el CERT o CSIRT. Posteriormente es recomendable relacionar en una tabla los aspectos determinantes en la etapa de detección y análisis.

De tal manera que se tienen dos labores involucradas en estas tareas que desempeña un equipo de seguridad cibernética, lo cual complementa lo comentado en la pagina 8 y 9 de este articulo y que permite orientar la siguiente fase, así:

Checklist del incidente (*Fase Contingencia, Erradicación y Recuperación*):

- **Adquirir, preservar, asegurar y documentar evidencia**
- **Contener el incidente**
- **Erradicar el incidente**
  - Identificar y mitigar todas las vulnerabilidades que fueron explotadas
  - Remover [3]malware, materiales inapropiados y otros componentes
  - Si se descubren más [4]hosts afectados (por ejemplo, nuevas infecciones de malware), repita los pasos de Detección y Análisis para identificar a todos los otros hosts afectados, luego contenga y erradique el incidente para ellos.
- **Recuperarse del incidente**
  - Regresar a los sistemas afectados a su estado operativo
  - Confirme que los sistemas afectados funcionan normalmente
  - Si es necesario, implemente un monitoreo adicional para buscar actividades relacionadas en el futuro.

Espacio dejado a propósito

[3] Software Malicioso

[4] **Host:** Anfitrión se usa en informática para referirse a las computadoras u otros dispositivos (tabletas, móviles, portátiles) conectados a una red que proveen y utilizan servicios de ella. Tomado de internet

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

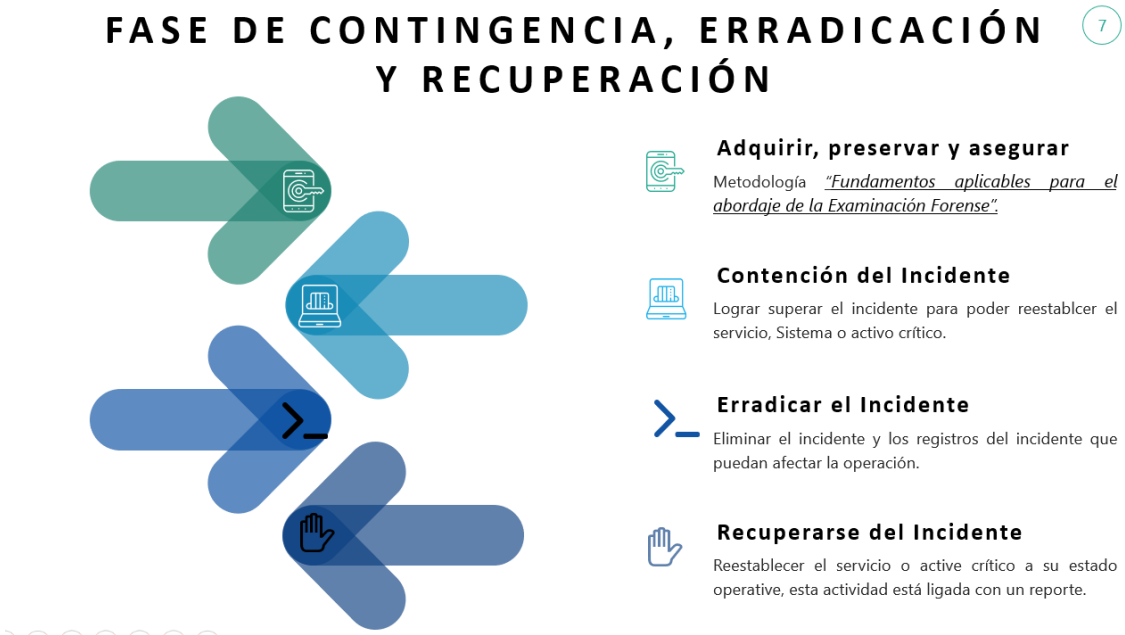


Figura elaborada por el autor para reflejar la segunda fase

- **Actividad Post- Incidente**
  - Crear un informe de seguimiento
  - Establezca una reunión de lecciones aprendidas *(obligatoria para incidentes mayores, opcional de lo contrario)*

Espacio dejado a propósito

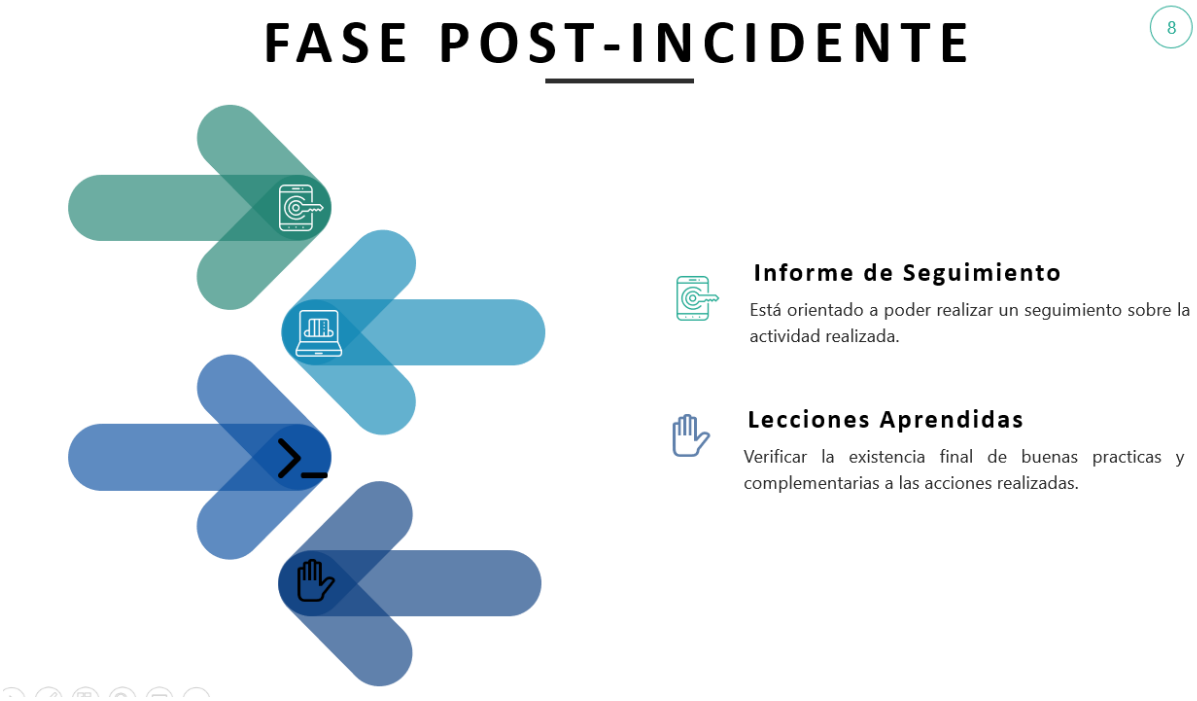


Figura elaborada por el autor para reflejar la tercera fase

Este conjunto de fases se deben tener en cuenta, en el momento de evaluar la respuesta a un incidente, sin embargo las buenas prácticas relacionadas en la Guía *Computer Security Incident Handling Guide* (800-61) relacionada por NIST, es complementaria a todas las actividades que perfeccionen la técnica elaborada por los analistas, especialistas e investigadores que hacen parte del equipo de seguridad cibernética. Aquellas características referenciadas anteriormente, permiten incrementar los niveles de madurez en el momento de realizar algún escenario que involucre una crisis o en lo relacionado con un incidente.

Por otra parte, también se encuentra relacionado en estas buenas practicas lo referente a la coordinación y la información que comparte un CERT o CSIRT; para ello, debe enfocar sus esfuerzos a mantener los canales de seguridad cibernética sobre la información de una forma segura; (FIRST, s.f.), el Foro de Intercambio de Experiencias en materia de Equipos de Respuesta a Incidentes permite elaborar una metodología que garantiza el desarrollo formal de información bajo un esquema colaborativo. Este protocolo, clasificado en cuatro niveles de confidencialidad, garantiza los elementos de confidencialidad dispuestos por el originador del mensaje.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

El protocolo *Traffic Light* o semáforo, concibe tres elementos fundamentales y uno accesorio: *Luz Roja*, tiene que ver con la información de un único destinatario y que posee características esenciales para salvaguardar esa confidencialidad única. *Luz Amber*, tiene que ver con información directa a la parte interesada, pero con ciertas limitaciones para compartir a los equipos de seguridad internos o a un proveedor en riesgo o tercera parte. Por último, la *luz verde*, la cual tiene que ver con una información que no guarda un aspecto de confidencialidad mayor, y se podrá compartir entre los miembros del equipo de la parte interesada y proveedores de riesgo, la limitación consiste en entregar esta información en manos de otras entidades o proveedores que no tengan que ver con el tratamiento o gestión de esta notificación.

Otros conceptos liberados recientemente que se utilizan en los equipos de seguridad implementados recientemente a nivel global se encuentran relacionada la luz blanca o TLP White, y es la que tiene relacionada acciones que involucran actividades globales en seguridad; esta función de confidencialidad no aplica para información que deba solamente ser transferida a un único destinatario.

Coordinación con Autoridades y externos a su organización CERT o CSIRT

La coordinación de un Equipo de Respuesta a Incidentes (CERT o CSIRT) debe involucrar, además de un protocolo, el poder organizar actividades independientes de aprovechamiento dentro de la estrategia que desee involucrar; por ejemplo, un CSIRT que involucre actividades técnicas o de articulación con proveedores y terceras partes de alto riesgo para sus partes interesadas. Por otro lado, se encuentra relacionado en el catalogo de entidades que deben involucrar alguna interacción, ya sea técnica, operativa o técnica. Además de eso, la información sometida a intercambio o a entrega por parte del equipo de seguridad cibernética, deberá contener todos los aspectos de seguridad y confidencialidad reconocidos por ambas organizaciones.

La Coordinación del Equipo está facilitada por un coordinador que permite realizar la actividad de sinergia actual, con los diferentes entes, organizaciones o instituciones que deba tener contacto; con una debida orientación y facilitación de este escenario, por parte de un director de proyecto CO-CSIRT (*Chief Operation of CSIRT*) o Director de Operaciones que a sus veces coordinará las acciones pertinentes con otros ISAC´S o comunidades de intercambio.

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Las relaciones que pueden existir son:

- *Técnicas:*

  Equipo con Equipo; aquellas que van orientadas a facilitar espacios de intercambio técnico, administrativo y logístico que permiten fortalecer la capa de colaboración en procedimientos en las diferentes etapas de preparación (Análisis TRIAGE).

- *Estratégicas:*

  CO – CSIRT con CO – CERT o CSIRT; son aquellas las establecidas con los directores de operación de ambos equipos técnicos, para poder abordar escenarios que involucren acciones dirigidas hacia la toma de decisiones sobre una amenaza cibernética, crisis o incidente cibernético, y poder determinar el alcance sobre la misma, y sobre las partes interesadas.

- *Operativas:*

  Involucran acciones desplegadas en virtud de poder adelantarse a distintas formalidades en intercambio de información, como las enfocadas en una temática específica, ej: Ciberejercicio o simulación cibernética.

- *Administrativas:*

  Son las enfocadas en actividades de índole administrativo o logístico, donde se respetarán la autonomía de cada equipo de ciberseguridad.

Figura elaborada por el autor, orientada al relacionamiento y articulación de Equipo de Seguridad Cibernética

Dentro de este relacionamiento también se pueden suscribir acuerdos o convenios que faciliten el intercambio de información de manera segura, que estructuren la razón de ser de cada uno de los equipos de seguridad, también que involucre partes o terceras en riesgo cibernético u otras.

La Universidad Carnegie Mellon estableció como principio establecer las principales formas de determinar la creación de un CERT o CSIRT con base a una generación escalada de aspectos técnicos que involucran el crecimiento de cada una de sus áreas.

Cada equipo de seguridad cibernética está relacionado con una misión, unos objetivos a perseguir, la disposición del *expertise* de sus miembros, la composición y estructuración de los recursos de este, y su fundación. Estos atributos están orientados a poder conocer esos recursos mínimos que debe tener este equipo de respuesta y gestión a incidentes, por lo mínimo deberá contener:

- Una respuesta mediante correo electrónico para los incidentes
- Documentación sobre eventos o reportes de incidentes que contengan vulnerabilidades y otra información técnica.
- Notificaciones sobre líneas básicas o guías
- Desarrollo de políticas y procedimientos
- Comunicaciones internas y externas para las partes interesadas


CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Integridad: Dentro de esta misma estructura propuesta por la División CERT de la Universidad Carnegie Mellon se encuentra enfocada en los miembros que trabajan para el equipo de respuesta a incidentes, el cual debe ir enfocado en evitar impactar negativamente a las partes interesadas, y que esto pueda afectar la operación, por lo tanto es importante que los miembros de este Equipo comprendan la importancia de la diferencia en el servicio y la suscripción que tenga el miembro frente a la información relacionada con alguna investigación que afecte la imagen del CSIRT y del equipo.

Resolución de problemas con la comunicación: Del mismo modo es importante destacar que la importancia de la información que se suministra a sus miembros, la cual puede determinar su relevancia, de esta manera radica la importancia de definir claramente dentro del público objetivo, la respectiva finalidad de esa información, teniendo en cuenta lo siguiente:

- Distribución limitada de la información
- Resolución de problemas *(Entre los miembros del equipo para poder determinar si la información debe ser difundida)*
- Información técnica adicional
- Verificar la información por medio de enfoques
- Sintetizar información y determinar relaciones que existen con otros incidentes.

Dentro de las múltiples tareas del equipo de respuesta a incidentes de seguridad cibernética, es importante también definir las tareas que complementan el trabajo de los miembros, como conferencias, presentaciones, trabajos en grupo, y acciones que fortalezcan las actividades diarias realizadas.

Las habilidades técnicas del equipo y su naturaleza deben ser elementos focalizados por el CERT o CSIRT, cuando se involucran a partir de este las mejoras evolutivas en asistencia técnica dirigida a las partes interesadas, por ende, la importancia del nivel de profundidad, respuestas apropiadas, el nivel de autoridad y las acciones específicas a aplicar por parte de cada uno de los miembros del equipo.

Los miembros del CERT o CSIRT deben tener en cuenta una política de confidencialidad de la información, sobre todo, cuando se habla de los elementos que fundan y caracterízan cada uno de los atributos de la información suministrada a las partes interesadas. De tal manera que esta política debe ir enfocada en respetar lo siguiente:

- Confidencialidad
- Disponibilidad
- Integridad

- Autenticación
- Control de acceso a la información
- Privacidad
- No repudio

Riesgo: El Equipo CERT o CSIRT deberá comprender la importancia de que existe un riesgo involucrado en su infraestructura y sus componentes; de tal manera que, le permita tener una política de aseguramiento de esos activos de la información.

Conocimiento sobre las técnicas utilizadas para las intrusiones: Dentro de este mismo conocimiento, es importante definir las habilidades especiales que se citaron en la página 17 de este artículo, en donde se citan las capacidades que deberá tener los miembros del equipo:

- Identificar una nueva vulnerabilidad
- Realizar análisis técnicos a intrusiones
- Reconocer nuevas técnicas de intrusiones basadas en sus huellas y efectos
- Documentar el análisis de artefactos y su estudio de los nuevos métodos asociados a esos riesgos y su prevención.

Caso de estudio relacionado con la creación de un CERT o CSIRT Financiero

Dentro de los documentos de estudio que posee la (Carnegie, Mellon University, s.f.) en cuanto a los ambientes desarrollados por (SANS Institute), para diseñar un equipo de Respuestas a Incidentes, además de tener en cuenta la metodología presentada; cuando se creó este caso de estudio dirigido a congregar a las instituciones financieras de los Estados Unidos se tuvo en cuenta los siguientes aspectos:

- Definir y determinar la estructura de los informes del CSIRT (Autoridad y modelo)
- Determinar el rango de los niveles de servicio
- Identificación del personal a contratar
- Políticas y procedimientos relacionados
- Identificar puntos de contacto

A partir de ello se propuso adelantar y enfocar los esfuerzos en desarrollar argumentos esenciales para poder entender el alcance, los objetivos, la población a impactar y los niveles de confidencialidad dispuestos para cada una de sus actividades. Sin embargo, crear o desarrollar un CSIRT o CERT no están sencillo o fácil, en esta misma dinámica. Deben existir elementos de peso legal, técnico y tecnológico para desarrollarlo. Además, determinar la estrategia de seguridad digital que posea el país en concreto o la política de gobernanza que exista a nivel del sector que se quiera impactar; como ejemplo particular en Colombia existe el (CSIRT de Asobancaria) el cual ha sido

focalizado en esas políticas, reconociendo que hace parte del ecosistema de las infraestructuras críticas, basado en una experiencia internacional para poder estructurar su aprobación, bajo una dinámica colaborativa que permite a cualquier entidad que haga parte del proceso, llevar acabo los objetivos y búsqueda constante de mejoras desarrolladas para su comprensión y el desarrollo de la transformación digital.

Actualmente es importante destacar este referente como ejemplo adoptado bajo un esquema de las mejores prácticas desarrolladas en esta metodología. Asimismo, las tendencias que tenga un país en esta vía son fundamentales para desarrollar un proyecto que tenga una evolución escalada, la cual se demuestra ante los nuevos retos que antepone el cibercrimen.

Dados estos aspectos se construye un nivel de conocimiento en la materia, desarrollada así por los nuevos fenómenos que exige cada vez más los componentes de los servicios digitales enfocados en la industria (economía, social, política y tecnológica).

Para culminar la primera parte de esta metodología es bueno determinar cuál debe ser el recorrido de un CSIRT o CERT, por ello, es importante dar alcance a todos estos factores antes enunciados para permitir realizar una consultoría confiable y certera sobre los retos [5](CSIRT Financiero de Asobancaria, 2020). Este paso radica en la apropiación y pertinencia de cada uno de los actores desarrollados entre sí, para poder orientar las necesidades en cada uno de los eslabones de la cadena de la ciberseguridad.

[5] Url de acceso a la memoria anual: https://www.asobancaria.com/wp-content/uploads/2020/06/CRT-MA_2020_compressed.pdf

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

REFERENCIAS BIBLIOGRÁFICAS

800-61, N. S. (s.f.). *Computer Security Incident Handling Guide.* doi:http://dx.doi.org/10.6028/NIST.SP.800-61r2

Carnegie, Mellon University. (s.f.). Obtenido de https://web-search.andrew.cmu.edu/search?q=CERT&proxystylesheet=default_frontend

CSIRT de Asobancaria. (s.f.).

CSIRT Financiero de Asobancaria. (2020). *Memoria Anual Operación CSIRT FInanciero.* Bogotá: Asobancaria.

Cybersecurity, N. (2018). NIST Cybersecurity Framework.

EC3, I. (2019). *Internet Organised Crime Threat Assessment (IOCTA).* The Hague: European Union Agency for Law Enforcement Cooperation 2019.

FIRST. (s.f.). *https://www.first.org/about/*. Obtenido de https://www.first.org/about/: https://www.first.org/about/

Framework, I. S., & Security, I. (2020). *http://www.alntechnology.com/sites/default/files/isfpdf%20%28rombus%29.pdf.* Obtenido de http://www.alntechnology.com/sites/default/files/isfpdf%20%28rombus%29.pdf: http://www.alntechnology.com/sites/default/files/isfpdf%20%28rombus%29.pdf

Gartner, C. (2018). *https://www.gartner.com/*. Obtenido de https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/

ICONTEC. (s.f.). ISO . *DIRECTRICES ISO 27001*.

ISO, 2. I. (2014). Guidelines for identification, collection, acquisition and preservation of digital evidence" ISO/IEC 27037:2012.

Marc, Grégory. (s.f.). *Visualisation for network situational awareness in computer network defence.*

Mellon, C. U. (Junio de 1999). *https://resources.sei.cmu.edu/.* Obtenido de https://resources.sei.cmu.edu/asset_files/: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1999_005_001_16769.pdf

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

MITRE, C. (s.f.). Malware . *Captalogación del Malware*.

Moira J. , W.-B., Don , S., & Klaus, P. (2003). *Handbook for Computer Security Incident Repsonse .* National Science Foundation.

NIST, Contigency Planning Guide;. (2010). *Contingency Planning Guide for Federal Information Systems.* Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

NIST, S., & SP 800 61. (s.f.). *https://www.csirt.org/publications/.* Obtenido de CSIRT: https://www.csirt.org/publications/sp800-61.pdf

Ortiz Ruiz, E. E. (2020). *CIBERSEGURIDAD: METODOLOGÍA APROXIMADA PARA REALIZAR INVESTIGACIÓN EN INTELIGENCIA CIBERNÉTICA.* Bogotá: Reporte Técnico. doi:10.13140/RG.2.2.25127.37289/2

Ortiz Ruiz, E. E. (Agosto de 2018). Blockchain: Conceptos básicos aplicables para reducir la brecha del Fraude. *Blockchain: Conceptos básicos aplicables para reducir la brecha del Fraude*.

Ortiz Ruiz, E. E. (2019). Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación. *Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación*.

Ortiz Ruiz, E. E. (02 de Abril de 2019). Evidencia Digital: Principios metodológicos para el análisis de Código Malicioso. *Evidencia Digital: Principios metodológicos para el análisis de Código Malicioso*. Bogotá: ResearchGate.

Ortiz, E. E. (2020). APROXIMACIÓN METODOLÓGICA DEL CIBERCRIMEN EN COLOMBIA. *Seguridad*, 20.

Osorno, M., Millar, T., & Rager, D. (28 de 04 de 2020). *Coordinated Cybersecurity Incident Handling.* Obtenido de Sematics schoolar : https://pdfs.semanticscholar.org/3e83/19d3f150866dc70f550aaf7897efcd2b5c8b.pdf

Penedo, D. (2005). Technical Infraestructure of a CSIRT.

RFC 2196, B. (1997). *Site Security handbook.* IETF.

Rohmeyer , p., & Bayuk , J. (2019). *Financial Cybersecurity Risk Manangement.* Hoboken NJ, USA: Springer. Recuperado el 17 de Marzo de 2020

SANS Institute. (s.f.).

CIBERSEGURIDAD: METODOLOGÍA PARA LA CREACIÓN DE EQUIPOS DE INVESTIGACIÓN EN SEGURIDAD CIBERNÉTICA

Software, E. I., & Carnegie , M. U. (2020). *apps.dtic.mil.* Obtenido de Carnegie Mellon University: https://apps.dtic.mil/dtic/tr/fulltext/u2/a596848.pdf

Study, ISC Cybersecurity Workforce. (s.f.).

Sultan , A., & Majeed , A. (2014). *Information Security Maturity Model For NIST CSF.* Arabia Saudita: College of Computer Sciences and Engineering. Obtenido de https://s3.amazonaws.com/academia.edu.documents/52007982/csit76505.pdf?response-content-disposition=inline%3B%20filename%3DINFORMATION_SECURITY_MATURITY_MODEL_FOR.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20200317%2Fus-e

Toro, M. M., Ortiz, E. E., & Parada, W. (2018). *Fundamentos de la investigación forense en ambientes informáticos.*