Diseño del CSIRT para la Dirección Nacional de Inteligencia DNI

Juan Carlos Mikly Melo
Erich Siegert Cerezo

Trabajo de grado para optar al título profesional:
Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

"DISEÑO DEL CSIRT PARA LA DIRECCIÓN NACIONAL DE INTELIGENCIA - DNI"

ALUMNO: JUAN CARLOS MIKLY MELO

DIRECTOR: ERICH SIEGERT CEREZO

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2020

AGRADECIMIENTOS

Me gustaría agradecer a mi Dios por bendecirme para llegar hasta donde he llegado, haciendo posible este sueño anhelado. A un gran profesional el Dr. Manuel Sánchez Rubio, quien, sin su amistad, su ayuda, sus conocimientos, su experiencia, su paciencia y su motivación han logrado que pueda terminar este reto con éxito.

Un agradecimiento especial al Ingeniero y Experto en Transformación Digital, Manuel Díaz Hoyos, por todo su conocimiento, apoyo y guía en el desarrollo de este proyecto.

También me gustaría agradecer a mis docentes durante esta formación profesional porque todos han aportado con un granito de arena a mi conocimiento.

Y por último a mis jefes y compañeros de trabajo quienes apoyaron esta aventura y me han motivado durante esta etapa de formación.

DEDICATORIA

A Dios y a mi Familia. A Dios porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar; a mi familia, quienes a lo largo de mi vida han velado por mi bienestar y han sido mi apoyo en todo momento; depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Es por ello que soy lo que soy ahora. Los amo con mi vida.

RESUMEN

En el escenario global, se conoce en medios de comunicación, escándalos relacionados con intervenciones en elecciones, opinión pública, secretos militares y de Estado, entre otros, en donde es claro que la ciberseguridad juega un papel importante en las interacciones, cada vez mayores, de los ciudadanos del mundo a través del ciberespacio. Esto significa que el ciberespacio se ha convertido de manera muy rápida, en el escenario de enfrentamiento, en donde los intereses tangibles e intangibles pueden ser afectados.

Con este panorama; aunado a las labores y responsabilidades asignadas en el documento CONPES 3854 a la Dirección Nacional de Inteligencia, la cual es una organización de inteligencia estratégica joven, posicionada entre las entidades de inteligencia a nivel internacional y siendo un referente de estas, se presenta una oportunidad de innovación al proponer un plan estratégico general que permita reforzar las capacidades de ciberseguridad en la Dirección Nacional de Inteligencia - DNI y en los organismos de inteligencia, que defina un marco de referencia que permita aprovechar las oportunidades que se presentan en la tecnología y los riesgos, con el fin de capitalizarlos como oportunidades de crecimiento para el Estado Colombiano.

Por medio de actividades hostiles en el ciberespacio, otros países, organizaciones, o elementos hostiles, estarían en la capacidad de detectar y aprovechar estos riesgos, amenazas y oportunidades buscando afectar los fines del Estado Colombiano, en donde la información, la reputación institucional, afectación a infraestructura critica, daño a la población, son elementos críticos a proteger, los cuales se ven incrementados con el uso nuevas tecnologías (generalmente

extranjeras o foráneas), comunicación en la nube, IOT, redes sociales, los cuales pueden ser utilizadas en contra de los intereses del Estado.

Este proyecto plantea la estructuración de un equipo de respuesta a incidentes de seguridad informática – CSIRT con base en el Marco de Seguridad Cibernética (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), que permita entender y monitorear las amenazas que se pueden presentar por los ataques cibernéticos y problemas de seguridad en los sistemas del país.

Palabras Claves: Ciberseguridad, incidente, CSIRT, NIST, CSF.

ABSTRACT

On the global stage, scandals related to interventions in elections, public opinion, military and state secrets, among others, are known in the media, where cybersecurity plays an important role in the ever-increasing interactions, of the world's citizens through cyberspace. This means that cyberspace has become very quickly, the scene of confrontation, where tangible and intangible interests can be affected.

With this panorama; In addition to the tasks and responsibilities assigned in document CONPES 3854 (Digital, 2016) to the National Intelligence Directorate, which is a young strategic intelligence organization, positioned among intelligence entities at the international level and being a benchmark for these, an opportunity to innovation by proposing a general strategic plan to reinforce cybersecurity capabilities in the Dirección Nacional de Inteligencia - DNI and in intelligence agencies, which defines a reference framework that allows taking advantage of the opportunities presented by technology and risks, in order to capitalize on them as growth opportunities for the Colombian State.

Through hostile activities in cyberspace, other countries, organizations, or hostile elements, would be able to detect and take advantage of these risks, threats, and opportunities seeking to affect the purposes of the Colombian State, where information, institutional reputation, involvement Critical infrastructure, damage to the population, are critical elements to protect, which are increased with the use of new technologies (generally foreign or foreign), cloud communication, IOT, social networks, which can be used against the interests of the State.

This project proposes the structuring of a computer security incident response team - CSIRT based on the Cyber Security Framework (CSF) of the National Institute of Standards and Technology (NIST), which allows understanding and monitoring the threats that can be presented by cyber-attacks and security problems in the country's systems.

Key Words: Cybersecurity, incident, CSIRT, NIST, CSF.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

INTRODUCCIÓN

Colombia a partir del desarrollo de su primer Documento del Consejo Nacional de Política Económica y Social República de Colombia, emitido por el Departamento Nacional de Planeación, cuyo número es el 3701, donde se dictan los lineamientos de la política para Ciberseguridad y Ciberdefensa con temas de seguridad ha demostrado que tiene la capacidad de desarrollar el entorno digital, como política nacional. De igual forma, estas comodidades ofrecen a los delincuentes, oportunidades para difundir amenazas complejas que explotan a los dispositivos que permiten su consulta o la información que reposa en la nube, convirtiendo el espacio cibernético en un medio para victimizar al público.

Una de las conclusiones presentadas en el marco del seminario "Infraestructura Críticas, un desafío de Ciberseguridad" resalta como conclusión que:

El fraude fue el tipo de incidente cibernético más común reportado por el ColCERT (Grupo de respuesta a emergencias cibernéticas de Colombia) en la lista de incidentes cibernéticos de Colombia; según el seminario realizado por el Ministerio de Defensa y el comité Interamericano contra el Terrorismo de la OEA en 2013, esta lista contiene además, distintos tipos de hackeo y spoofing de páginas web y más de uno de los equipos de respuesta del país reportó ataques de haktivistas, dirigidos en su mayoría contra entidades estatales y militares e instituciones financieras generando para el gobierno Colombiano la aceptación del fenómeno generalizado que indica los bajos niveles de conciencia de la seguridad cibernética, lo que precipita hábitos de navegación

inseguros y había provocado la defraudación de usuarios del internet vulnerables. Además, la insuficiente capacitación sobre ataques avanzados, las dificultades para preservar y examinar evidencias digitales y la falta de cooperación de los proveedores de servicios de internet y otras organizaciones privadas constituyeron impedimentos importantes para poner freno a la delincuencia cibernética en Colombia.

Con este panorama; aunado a las labores y responsabilidades asignadas en el documento CONPES 3854 de 2016 (Consejo Nacional, de Política y Económica y Social, 2016), a la Dirección Nacional de Inteligencia, la cual es una organización de inteligencia estratégica joven, posicionada entre las entidades de inteligencia a nivel internacional como se manifestó por sus participantes en el pasado X Foro de Servicios de Inteligencia de Iberoamérica – FOSII, realizado en Cartagena en el mes de septiembre de 2016 y siendo un referente de estas; una de las conclusiones generadas al interior de este foro plantea el interrogante sobre cómo debe generar conocimiento especializado al interior de las agencias de inteligencia latinoamericanas, con la aplicación de métodos y metodologías de defensa cibernética para fortalecer los procesos de Inteligencia y Contrainteligencia a través de sus entidades de formación.

Para la Dirección Nacional de Inteligencia el uso de herramientas informáticas y la aplicación de métodos y metodologías de defensa cibernética para el sector de inteligencia, determinan el principal paradigma que tiene este nuevo enfoque, radica en la adecuada protección preparando e implementando los procesos y la infraestructura necesaria sobre la cual adoptar un modelo de ciberseguridad y la creación de un equipo de respuesta a incidentes adecuado para dar

tratamiento a eventos generados en los sistemas utilizados para las labores de campo y sortearlos adecuadamente.

ANTECEDENTES

Según la GUÍA DE SEGURIDAD(CCN-STIC-810) GUÍA DE CREACIÓN DE UN CERT / CSIRT CCN-STIC-810 Guía de Creación de un CERT/CSIRT Centro Criptológico Nacional, 2011 (CCN-CERT, 2011).

"¿UN CERT ES?

Tradicionalmente, se ha definido un CERT como una organización, equipo, unidad o capacidad de un organismo de ofrecer servicios y soporte a un colectivo determinado (denominado "comunidad") para prevenir, gestionar y responder a los incidentes de seguridad de la información que puedan surgir. Esta definición genérica viene materializándose en un equipo multidisciplinar de expertos que trabaja según unos procesos definidos previamente y que disponen de unos medios determinados para implantar y gestionar, de un modo centralizado, todas y cada una de las medidas necesarias para mitigar el riesgo de ataques contra los sistemas de la Comunidad a la que presta el servicio y responder de forma rápida y efectiva en caso de producirse. No obstante, el concepto de CERT y los servicios que engloban este tipo de estructuras ha ido evolucionando con el paso del tiempo y ampliando sus funciones. No sólo gestionan los incidentes de una organización, sino que también prestan otros servicios complementarios como la asistencia para mitigar riesgos (por ejemplo, mediante la ejecución y/o soporte en la realización de análisis de riesgos o vulnerabilidades), o para la recuperación después de registrar un problema. De hecho, el análisis forense es uno de los servicios que ENISA recomienda incluir a la hora de ampliar los servicios de este tipo de equipos, así como la gestión de las vulnerabilidades. Es decir, si bien el servicio básico de un CERT es el de gestión de incidentes, la mayor parte de ellos hoy en día están evolucionando hacia un modelo integral de gestión de la seguridad en donde se tienen en cuenta todos los elementos técnicos, humanos, materiales y

organizativos de un sistema y en donde predominan los servicios proactivos y de alerta temprana. De hecho, cada vez más, ofrecen a sus clientes servicios preventivos (seguridad proactiva, servicios para la mejora de la calidad de la gestión de la seguridad, desarrollo de herramientas de seguridad, detección de intrusiones, sistemas de alerta temprana...), formativos y de concienciación a las personas de su Comunidad (publicación de avisos sobre las vulnerabilidades del software y el hardware en uso, emisión de avisos sobre amenazas como códigos maliciosos o actividades sospechosas o de riesgo, publicación de recomendaciones y buenas prácticas, etc.) o de otro tipo (análisis de riesgos, planes de continuidad y de recuperación ante desastres, evaluación y certificación de productos, etc.)." (CCN-CERT, 2011). Tomando como base esta definición que es una de las mas acertadas, se describe la propuesta para la creación de un CSIRT en la Dirección Nacional de Inteligencia.

La diferencia entre un CSIRT y un PSIRT

El CSIRT de una organización y otros equipos de seguridad representados en la misma organización, como un PSIRT (Product Security Incident Response Team). Generalmente, el enfoque en los productos es el diferenciador clave entre el PSIRT y cualquier otro equipo de seguridad, incluidos, entre otros, los CSIRT dentro de una organización.

Dentro de una organización, un CSIRT empresarial se centra en la seguridad de los sistemas y redes informáticos que conforman la infraestructura de una organización. Si hay varios equipos de seguridad y CSIRT dentro de una organización grande, uno de ellos puede servir como coordinador y punto de contacto único para las partes externas. Estos equipos se denominan CSIRT coordinadores.

La diferencia clara entre estos dos radica en que "*el primero se centra en proteger la infraestructura de una organización, mientras que el segundo responde a las amenazas y fallas en los productos de la organización*" (FIRST, Forum Incident Response and Security Teams, 2018).

Dichos CSIRT coordinadores también se establecen como entidades independientes que prestan servicios a un conjunto específico de personas y / u organizaciones conocidas como circunscripciones. Las organizaciones que pertenecen a una circunscripción específica comparten algunas características comunes (como ser parte de una red nacional de investigación o pertenecer a un país específico). El CSIRT coordinador actúa como punto de contacto único para todo el grupo y se centra en los aspectos generales de seguridad de estas organizaciones.

Hoy en día, los CSIRT nacionales se han establecido como un tipo distintivo de CSIRT Coordinador para facilitar y, a menudo, coordinar las actividades de los CSIRT ubicados en una nación en particular u ofrecer servicios limitados para todos los ciudadanos, sectores específicos de entidades de infraestructura crítica, etc. de esta nación.

Con esta definición clara, se pretende abordar el tema a tratar, dejando claro el punto de partida referenciado por una entidad que posee una vasta experiencia en el campo de la Ciberseguridad y Ciberdefensa.

A nivel legal, revisión de las funciones de la DIRECCIÓN NACIONAL DE INTELIGENCIA - DNI.

Mediante el decreto de creación 4179 (Dirección Nacional de Inteliegncia - DNI, 2018) de 2011 Articulo 6, se le asignan las siguientes funciones a la Dirección Nacional de Inteligencia:

Corresponde a la Dirección Nacional de Inteligencia dentro del Marco Legal que regule las actividades de inteligencia y contrainteligencia, ejercer las siguientes funciones:

1. Desarrollar actividades de inteligencia estratégica y contrainteligencia bajo los principios de necesidad, idoneidad y proporcionalidad, en cumplimiento del marco legal y objetico misional, con el fin de:
   a) Contrarrestar en el ámbito nacional o internacional las capacidades y actividades de personas, organizaciones o gobiernos extranjeros que puedan representar un riesgo o una amenaza para la seguridad nacional.
   b) Contrarrestar acciones de grupos armados al margen de la ley actividades de terrorismo.
   c) Contribuir a la desarticulación de organizaciones de crimen organizado cuando representen amenazas contra la seguridad nacional.
   d) Contrarrestar actos que atenten gravemente contra la administración pública y proteger a las instituciones de nivel nacional y regional de la influencia de organizaciones criminales.
   e) Contribuir a la protección de los recursos naturales, tecnológicos y económicos de la Nación, cuando su amenaza comprometa el orden público;
   f) Proteger a las instituciones públicas de actos de penetración, infiltración, espionaje, sabotaje u otras actividades de inteligencia desarrolladas por gobiernos extranjeros, organizaciones criminales u organizaciones armadas al margen de la ley; y
   g) Responder ante cualquier otro requerimiento de inteligencia del presidente de la Republica y alto gobierno, para el cumplimiento de los fines esenciales del Estado.

Si se revisan en detalle estas funciones asignadas, la Dirección Nacional de Inteligencia cuenta con la total facultad legal para adelantar los mecanismos que permitan la protección de los intereses

del Estado y sus organizaciones, se ahí que la constitución del CSIRT del Sector de Inteligencia a nivel legal es totalmente valido para la entidad y para el estado, en contribución a garantizar la preservación de los intereses estratégicos del estado.

Otras Entidades que comparten el mismo esfuerzo.

Hacia el año de 2001 (Pérez, 2020) tiene origen, el Grupo Investigativo de Delitos Informáticos (GRIDI) de la Policía Nacional, posteriormente, con la masificación del uso de las TIC se denota un aumento de los delitos utilizados como medio o como fin por parte de la delincuencia. Para el año de 2010 se fortalecen las capacidades de este grupo y pasa a llamarse Grupo de Investigaciones Tecnológicas (GITEC). Con el aumento de los delitos informáticos, este grupo pasa a convertirse en el Área Centro Cibernético Policial (ARCIP) de la Dirección de Investigación Criminal e Interpol (DIJIN). Dicha transformación conllevó nuevos procesos, la incorporación de talento humano y la participación activa en escenarios estratégicos y operativos en materia de cibercriminalidad.

Finalmente, con la disposición del CONPES 3701 (Consejo Nacional, de Política y Económica y Social, 2011), catapulta la puesta en marcha de un grupo responsable de la ciberseguridad en Colombia, delegando dicha facultad al Centro Cibernético Policial. Sus funciones son (Policia Nacional, 2020):

a) Realizar la investigación criminal de las conductas que afecten a los niños, niñas y adolescentes descritas en la ley 599 de 2000, así como aquellas que la modifiquen, relacionadas con la pornografía que involucre personas menores de 18 años y la utilización

o facilitación de medios de comunicación para ofrecer actividades sexuales con menores de 18 años.

b) Dar cumplimiento a las responsabilidades adquiridas por la Policía Nacional con ocasión del acta de compromiso en desarrollo de la ley 679 de 2001 y normas que la modifiquen **"Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores".**

c) Fomentar la actualización y utilización de bases de datos de imágenes, videos, textos, audios con contenido de pornografía infantil obtenidas a través de las diferentes investigaciones, garantizando la utilización de protocolos universales que faciliten la cooperación policial internacional e intercambio de información en esta temática.

d) Generar los reportes de URL (Localizador uniforme de recursos) que contengan pornografía infantil, de acuerdo a los criterios de clasificación de contenidos Web y en previa reunión de la mesa de expertos, con el fin de realizar los bloqueos de dichas páginas mediante comunicación escrita al Ministerio de las tecnologías de la Información y las Comunicaciones.

e) Identificar las nuevas modalidades delictivas que surjan del uso inapropiado de las nuevas tecnologías y que afecten a los niños, niñas y adolescentes.

f) Adelantar campañas de prevención y difusión relacionadas con las amenazas y riesgos que afecten a niños, niñas y adolescentes en el uso de las Tecnologías de la Información y las Comunicaciones, así como el uso responsable de las mismas mediante la propuesta de códigos de buena conducta y autorregulación.

g) Participar en todas las instancias interinstitucionales como mesas, grupos de trabajo, comités, etc... Enfocados a la protección de los derechos de los niños, niñas y adolescentes en el uso de las nuevas tecnologías.

h) Propiciar el uso de la capacidad tecnológica y de difusión de la Policía Nacional, en la prevención, investigación y control de conductas que afectan a los niños, niñas y adolescentes en el uso de las nuevas tecnologías.

i) Emplear todas las herramientas tecnológicas disponibles para la persecución y proyección de investigaciones de carácter trasnacional de los delitos que afecten los derechos de los niños, niñas y adolescentes en el uso de las nuevas tecnologías.

j) Adelantar las coordinaciones necesarias ante la Unidad Nacional de Delitos Sexuales de la Fiscalía General de la Nación, encaminadas a fortalecer la investigación judicial y la retroalimentación de las entidades involucradas en la lucha contra la pornografía infantil en internet.

Para el año de 2011 (Mayorga Delgado, 2014), la posibilidad del uso de ciberespacio para Colombia deja entrever un cumulo de debilidades en ese ámbito, para lo cual el Gobierno expide una serie de lineamientos de política en materia de ciberseguridad y Ciberdefensa con el fin de dar respuesta a incidentes y delitos que se pudieran presentar afectando la estabilidad del estado Colombiano, esta responsabilidad quedo en manos del Ministerio de defensa de acuerdo al CONPES 3701 de 2011 (Consejo Nacional, de Política y Económica y Social, 2011).

A mediados del año 2013, el Ministerio Colombiano de Defensa, mediante la resolución. 3933 de 2011 (MINISTERIO DE DEFENSA NACIONAL, 2013), **crean** "*Grupos Internos de Trabajo del Ministerio de Defensa Nacional – Unidad de Gestión General*", **bajo el literal 2.5 DIRECCIÓN** DE SEGURIDAD PÚBLICA E INFRAESTRUCTURA se crea el grupo de Respuesta a

Emergencias Cibernéticas de Colombia – colCERT; con las siguientes funciones (Citadas conforme a la resolución 3933 de 2011):

a) Coordinar y asesorar a CSIRT (Grupos de respuesta a incidentes de seguridad informática) y entidades tanto del nivel público, como privados y de la sociedad civil para responder ante incidentes informáticos.
b) Ofrecer a las infraestructuras críticas nacionales, servicios de prevención ante amenazas cibernéticas, respuesta frente a incidentes cibernéticos, así como aquellos de información, sensibilización y formación en materia de seguridad informática.
c) Promover el desarrollo de capacidades locales/sectoriales para la gestión operativa de los incidentes de ciberseguridad y Ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
d) Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta temática.
e) Apoyar a los organismos de seguridad e investigación del Estado para la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.
f) Fomentar un sistema de gestión de conocimiento relavo a la Ciberdefensa y ciberseguridad orientado a la mejora de los servicios prestados por el colCERT.
g) Desarrollar y promover procedimientos, protocolos y guías de buenas prácticas y recomendaciones de Ciberdefensa y ciberseguridad para las estructuras críticas de la Nación, en conjunto con los agentes correspondientes y divulgarlos para su evaluación e implementación.

h) Proveer al Centro Cibernético Policial (CCP), y al Comando Conjunto Cibernético (CCOC), la información de inteligencia informática que sea requerida.

i) Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberseguridad y Ciberdefensa

Con base en esta normativa, el objetivo central del CONPES 3701 de 2011 (Consejo Nacional, de Política y Económica y Social, 2011), **plantea** *"fortalecer las capacidades del estado para enfrentar las amenazas que atentan contra la seguridad en el ámbito cibernético ..."* **y dentro de su primer objetivo específico,** *"Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas..."*, **dando** así nacimiento a la comisión intersectorial encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto a la gestión de la infraestructura tecnológica, información publica y ciberseguridad y Ciberdefensa.

Es allí que al Grupo de Respuesta a Emergencias Cibernéticas de Colombia –colCERT, se le encarga de coordinar a nivel nacional los aspectos de ciberseguridad y Ciberdefensa, prestando su apoyo y colaboración a las demás instancias nacionales tales como el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético – CCOC.

Figura 1. Modelo de Coordinación. [Gráfico]. Tomado de: Departamento Nacional de Planeación. (2011, 14 julio). Lineamientos de Política para Ciberseguridad y Ciberdefensa. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf (Consejo Nacional, de Política y Económica y Social, 2011)

En esta comisión se encontraba designado el director del Departamento Administrativo de Seguridad – DAS, que para ese entonces ya se encontraba en proceso de supresión, tomando sus funciones el Departamento Administrativo Dirección Nacional de Inteligencia - DNI.

Con base en la creación del CONPES 3854 de 2016 (Consejo Nacional, de Política y Económica y Social, 2016), el 2 de junio de 2018, con el acuerdo No. 002, se crea el comité de seguridad digital de carácter permanente, obedeciendo a la solicitud realizada por la presidencia

de la republica en la sesión no. 22 de diciembre de 2017 (Función Pública, 2018). En ese comité tiene como asistente permanente a un delegado de la Dirección Nacional de Inteligencia – DNI. La temática que estudia el comité esta indicada en los siguientes puntos:

a) Política y normatividad para la Seguridad Digital.
b) Protección y defensa de la infraestructura Critica Cibernética Nacional
c) Gestión de riesgos de seguridad digital
d) Crisis y seguimiento a amenazas Cibernéticas
e) Protección de datos personales
f) Asuntos internacionales de Seguridad Digital.
g) Comunicaciones estratégicas para la seguridad Digital

En esa línea las como lo muestra la figura siguiente estos organismos que conforman el comité trabajan de forma mancomunada para cumplir con las directivas impuestas por el Gobierno Nacional.

Figura 2. Comité Nacional de Seguridad Digital. [Gráfico]. Tomado de: Cámara de Comercio de Bogotá. (2019, abril). La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio.

https://web.certicamara.com/files/eventos/CiberseguridadCiberdefensaColombia.pdf (Cámara de Comercio de Bogotá, 2019)

Con base en esta estructuración organizacional orquestada por el Gobierno Nacional, se puede inferir que con el fin de potenciar las capacidades de protección y prevención en materia de Ciberseguridad y Ciberdefensa; de la misma manera dentro de las actividades que se desarrollan dentro la Dirección Nacional de Inteligencia, se realizan actividades de análisis de actividades, recolección de información en fuentes abiertas, entre otras, en materia de Ciberseguridad y Ciberdefensa tanto al interior como al exterior del país, como parte de las funciones enmarcadas en el ciclo de Inteligencia.

Figura 3. Dirección Nacional de Inteligencia. (s. f.). Ciclo de Inteligencia [Gráfico]. Tomado de: En Procedimiento Clasificado.

Por esta razón; la Dirección Nacional de Inteligencia, como cabeza del sector de inteligencia y contrainteligencia, cuenta con recursos técnicas, personal, procedimientos limitados preparados para apoyar las situaciones que, en materia de Ciberseguridad, la Presidencia de la República indique.

Es importante tener en cuenta el concepto de Ciberinteligencia, ya que es una de las actividades realizadas por la Dirección Nacional de Inteligencia; dicho concepto bastante acertado es el planteado por el Centro de Tecnologías Emergentes de la Universidad Carnegie Mellon (Carnegie Mellon University, 2013), **el cual expone una formulación sencilla, pero eficaz:** *"La adquisición y análisis de información para identificar, rastrear y predecir cibercapacidades, intenciones y actividades que ofrezcan vías de actuación para mejorar la toma de decisiones"*, dentro de ese proceso, una de las etapas es la protección, la cual deriva del hecho de la primera etapa que es la identificación cuyas actividades se fortalecen en función de la identificación de capacidades.

Estas capacidades desarrolladas y la experiencia que se ha acumulado en el apoyo de actividades de Ciberdefensa y Ciberseguridad, tanto a nivel nacional como internacional, hacen que sea una necesidad imperiosa crear un grupo concentrado con procesos, personal, procedimientos, protocolos y recursos que se articulen con los otros organismos que realizan esta actividad, desde el punto de vista de inteligencia civil, fortaleciendo el ecosistema de respuesta a incidentes Colombiano, cohesionado y operativo.

El modelo de trabajo propuesto al crear el CSIRT de inteligencia, es un modelo colaborativo, con las demás entidades del estado que conforman el ecosistema con capacidades similares, la academia y homólogos internacionales con el animo de intercambiar experiencias y conocimiento, como se plantea en la siguiente grafica:

Figura 4. Modelo de cooperación del ecosistema propuesto. [Gráfico]. Creación propia.

A nivel de Integridad del proceso de Ciberseguridad y Ciberdefensa Corporativo, de los Homólogos Nacionales y de la Integridad de las Instancias del Estado.

Como lo menciona Manuel Sánchez, 2017 (Sanchez G.-M. M., 2017); *"¿Cómo definiríamos la seguridad? Se entendería como las acciones que procuran la protección poniendo en valor el compartir, cooperar, colaborar en todo o parte de un objetivo, misión, etc.*, es decir: ***"Todos*** *aquellos esfuerzos y recursos mancomunados de prevención y protección de las instituciones y organizaciones, para compartir el propósito y objetivo del aseguramiento y todo lo que a él* ***corresponda"***. ***"La identificación, análisis y evaluación de los riesgos, amenazas y***

*vulnerabilidades son la clave principal para el planteamiento de las seguridades, pues seguridad, **además de una percepción, es la minimización o control real de riesgo**".*

Y lo que menciona ISACA (ISACA, 2017) en su artículo Incident Response – Being Prepared for the Worst Case Scenario, 2017 que dice traducido al español: *"**No es ningún secreto** que, en el mundo de hoy, la información está en mayor riesgo que nunca. Desafortunadamente, ahora debemos tratar de darnos cuenta de que no se trata de si se producirá un intento de incumplimiento en su red, sino más bien cuándo. A pesar de los mejores esfuerzos de una organización para proteger las redes y la información, continuarán existiendo errores humanos y vulnerabilidades del sistema. Teniendo en cuenta esa realidad, las organizaciones deben asegurarse de preparar un plan procesable **para cuando se desarrollen los peores escenarios**"*

Así las cosas, y teniendo en cuenta en ecosistema de responsabilidad legal a nivel de funciones que le fueron asignadas a la entidad de velar y proteger lo intereses del estado y evitar la penetración, infiltración y/o afectación de sus intereses en todos los niveles, la relevancia que involucra ser cabeza de sector de inteligencia, con todos los actores que se representan en la Comunidad de Inteligencia a nivel nacional, así como la importancia propia de preservar la confidencialidad, integridad, disponibilidad, no repudio, imagen corporativa y la resiliencia; se convierten en justificaciones suficientes para concluir que la Dirección Nacional de Inteligencia cuenta con los suficientes argumentos legales para conformar, estructurar y entrar en producción con el CSIRT del Sector de Inteligencia, manteniendo como finalidad prevenir la afectación de los intereses del estado en todos los entornos y niveles de infraestructura tecnológica que se administre por los organismos del estado.

A nivel mundial, se ha podido encontrar evidencia de un gran número de equipos de respuesta distribuidos en múltiples sectores. Para el caso de la unión europea, la ENISA o Agencia de la

Unión Europea para la ciberseguridad, reporta alrededor de 555 equipos de respuestas, distribuidos en 39 miembros y 516 no miembros de la red, con 274 que son miembros y 281 no miembros. De el total, el 17.25 pertenecen al sector gobierno y el 3.6% a fuerzas militares.

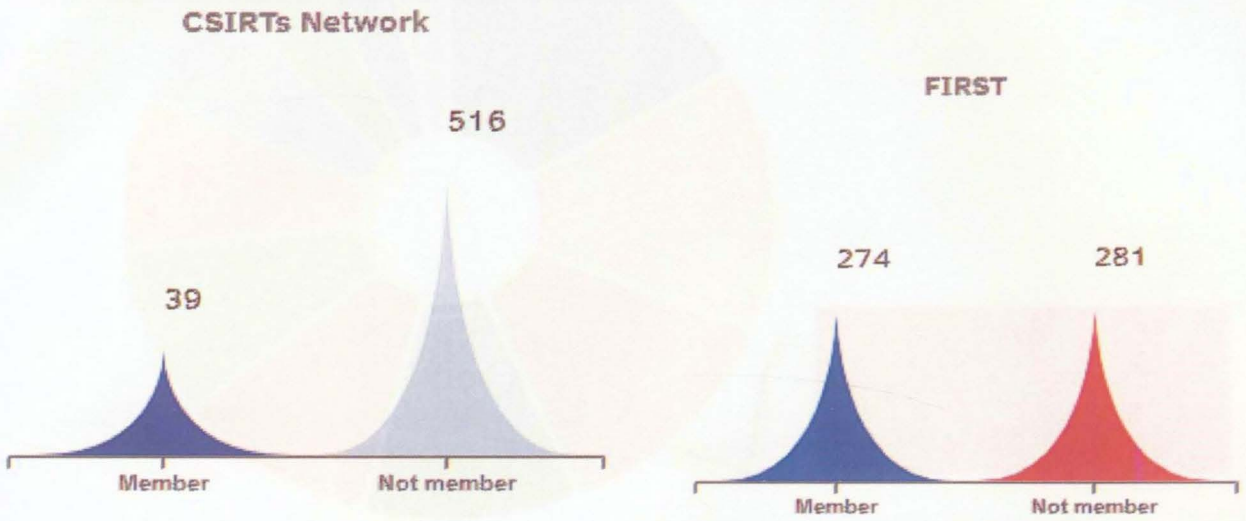

Figura 5. Estadísticas CSIRT ENISA. [Gráfico]. Recuperado de: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (European Union Agency for Cybersecurity - ENISA, 2020)

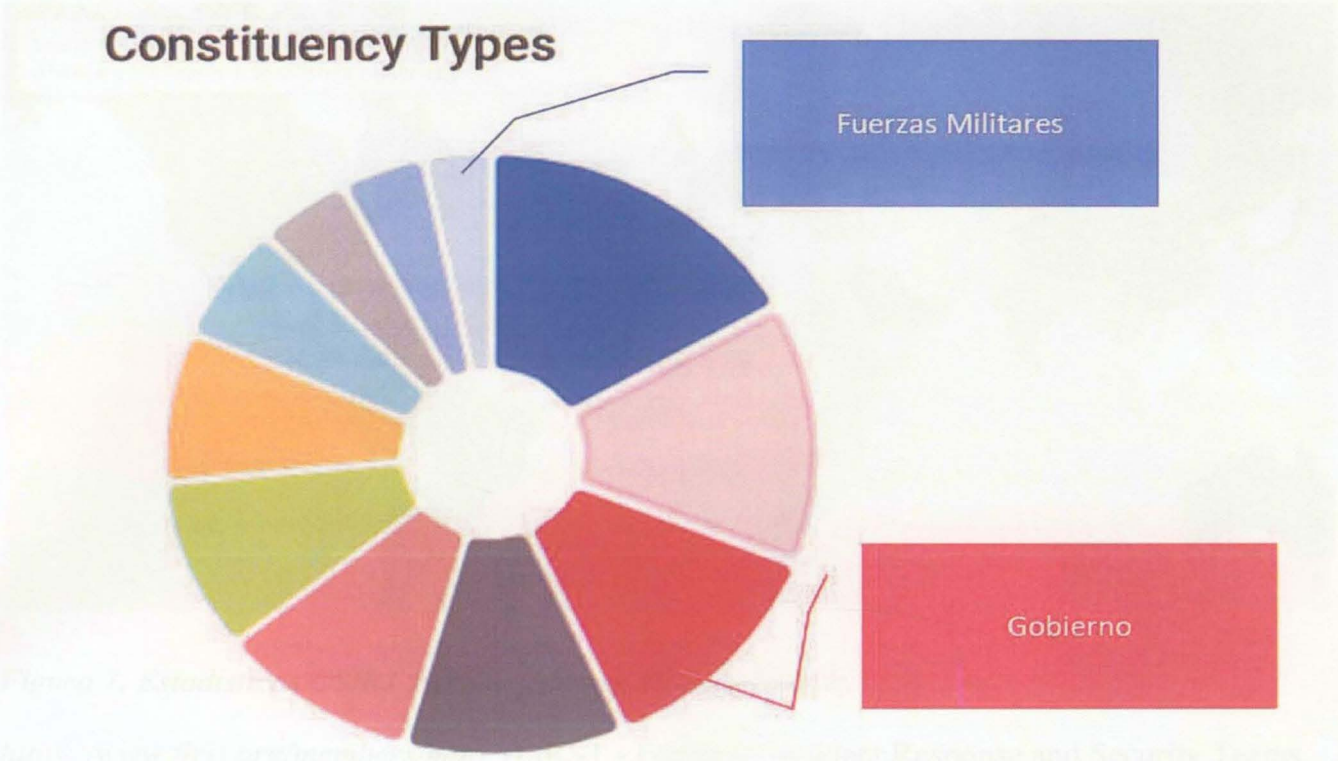

Figura 6. Estadísticas Sectores CSIRT ENISA. [Gráfico]. Recuperado de: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (European Union Agency for Cybersecurity - ENISA, 2020)

Adicionalmente, a nivel mundial según la FIRST, se reportan alrededor de 539 CSIRT miembros de 96 países diferentes, dentro de los cuales se destacan Estados Unidos, Alemania, España, Francia, Canadá, México y China.

Figura 7. Estadísticas CSIRT FIRST. [Mapa]. Recuperado de: https://www.first.org/members/map (FIRST - Forum of Incident Response and Security Teams, 2020)

Al demostrar la cantidad de equipos registrados a nivel mundial y según opiniones de expertos pertenecientes a GPPI, New América, la Unión Europea y el ministerio de asuntos internos de los Países Bajos (Morgus, 2015), existe una interdependencia o relación entre los CSIRT, las fuerzas de la ley u orden público y los servicios de inteligencia, debido a que estos grupos de respuestas deben estar coordinados de manera eficiente con los elementos del estado encargados de la ley y **de inteligencia estatal, todo debido a un fin inherente a estas dos últimas agrupaciones:** *"la seguridad de las redes como parte de los intereses del Estado"*.

Mientras que los grupos privados o de sectores económicos, se dedican a proteger sus infraestructuras, las agencias gubernamentales y de inteligencia se concentran en recolectar información e inteligencia con el fin de comprender ya actuar sobre las repercusiones físicas y

lógicas dentro de los intereses de un Estado. En este punto, es donde se hace evidente la necesidad de un CSIRT en el sector de inteligencia siendo este el articulador de la recolección, análisis y difusión de información relacionada con la Ciberinteligencia.

De esta manera, al igual que puede suceder en terrenos fuera del ciberespacio, la combinación de CSIRT privados y públicos, en combinación con las capacidades del sector de inteligencia, se puede generar una red que permita recolectar información y generar información estratégica de valor para contrarrestar, prevenir y capitalizar oportunidades para los estados, y en particular los riesgos que denominaremos no identificados.

MARCO TEÓRICO

Como parte del marco de referencia y punto de partida, es necesario definir de manera genérica el concepto de ciberseguridad, para tal fin la definición que más se ajusta es la de Manuel Sánchez, La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el entorno cibernético (Sanchez G.-M. M., 2011).

En la actualidad la seguridad de la información ha pasado a ser una de las principales preocupaciones de empresas, instituciones y gobierno. Gran parte de las operaciones comerciales, desde el nivel macroeconómico, hasta las pequeñas compras del día a día dependen en mayor o menor medida de las comunicaciones que se establecen para llevar a cabo las transacciones necesarias en estos intercambios económicos. Al mismo tiempo las gestiones que hacen los ciudadanos con las diferentes instituciones, así como las infraestructuras que soportan el bienestar de la sociedad poseen un grado de dependencia hacia las comunicaciones en internet cada vez más alto (Areito Bertolin, 2008).

De igual forma se debe partir de la definición clara de lo que es CSIRT, para lo cual se toma la definición entregada por ENISA, en su Producto WP2006/5.1 o CERT-D1/D2 (Areito Bertolin, 2008), el cual indica *"CSIRT significa Computer Security Incident Response Team (equipo de respuesta a incidentes de seguridad informática). Un CSIRT es un equipo de expertos en seguridad de las TI cuya principal tarea es responder a los incidentes de seguridad informática. El CSIRT presta los servicios necesarios para ocuparse de estos incidentes y ayuda a los clientes*

del grupo al que atienden a recuperarse después de sufrir uno de ellos." (Agencia Europea de Seguridad de las Redes y de la Información (ENISA), 2006).

Las capacidades para realizar tareas de búsqueda de información en fuentes abiertas y análisis de nuevos fenómenos que pueden ser amenazas en diferentes formas como Malware y Ciberinteligencia de grupos especializados (hackers, ciberterroristas, entre otros). Dadas las características intrínsecas de la seguridad de la información, en la formación impartida en el campo de la búsqueda de información en fuentes abiertas; esta Inteligencia de fuentes abiertas u «Open Source Intelligence» (OSINT) hace referencia al conocimiento recopilado a partir de fuentes de acceso público (Martínez, 2014), la generación de procedimientos es indispensable y es la que permite analizar situaciones más allá de la información que proporcionan las herramientas utilizadas en este tipo de procesos.

Importancia de la labor de inteligencia y su relación con el ciberespacio y la ciberseguridad

Con el fin de dar viabilidad a la importancia del sector de la inteligencia y su relación con la modernidad, específicamente con el ciberespacio y la ciberseguridad, se tendrá como hecho fundamental la globalización, la geopolítica, el incremento del uso de la tecnología y los fines esenciales del estado, incluidos en el artículo segundo de la constitución nacional de Colombia.

Existen numerosos reportes de prensa relacionados con eventos de "*ciberguerra*", ataques a infraestructuras críticas, robo de información, ATP´s, robo de información clasificada y secretos militares, lo cual muestra que el ciberespacio es un nuevo escenario de guerra, lo cual claramente es un escenario de inteligencia, por lo cual, la ciberseguridad es un elemento prioritario para la función, entendido como algo que se debe priorizara y gestionar de manera proactiva.

Figura 8. Información Online del fenómeno. [Infografía]. Recuperado de una consulta a Google https://www.google.com.co/search?hl=es-419&source=hp&ei=N9NnX66QM-O1ggevprvIDg&q=cyber+warfare&oq=cyber+wa&gs_lcp=CgZwc3ktYWIQARgDMgIIADICCAAyAggAMgIIADICCAAyAggAMgIIADICCAAyAggAMgIIADoFCAAQsQM6CAgAELEDEIMBOgUILhCxAzoICC4QsQMQgwE6CAguELEDEJMCOgQIABAKOgcIABCxAxAKOgoILhCxAxCDARAKUIURWOE0YPJLaABwAHgAgAGAAYgBzAeSAQMwLjiYAQCgAQGqAQdnd3Mtd2l6&sclient=psy-ab

A continuación, se muestran algunos hechos reales y comprobables relacionados con las amenazas cibernéticas:

Según el portal de Check Point Live Cyber Threat Map (Check Point Software Technologies LTD., 2020), para el día 13 de mayo de 2020 a las 8:15 am, se reportaban más de 17 millones de ataques cibernéticos. Adicionalmente dentro de los periodos comprendidos entre el 13

de febrero y 12 de mayo de 2020, se habrían presentado en promedio diario de 40 millones de ataques a infraestructura tecnológica.

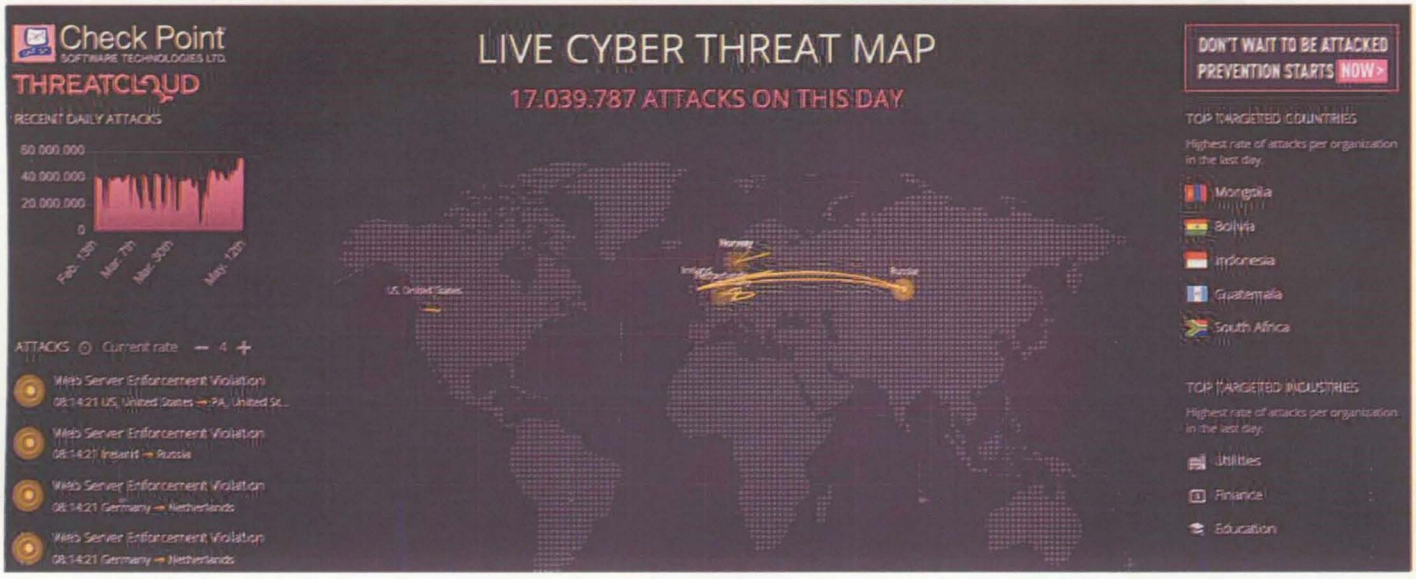

Figura 9. Ciberataques en el mundo. [Mapa]. Check Point Software Technologies LTD. Recuperado de: https://threatmap.checkpoint.com/ (Check Point Software Technologies LTD., 2020)

Según el portal Cybint (Milkovich, 2020), un estudio de la universidad de Merylan confirma que se produce cada 39 segundos en promedio, un ataque informático. Adicionalmente indican que en 2019 se produjeron costos de más de 2 trillones de dólares, según Juniper Research. En la figura a continuación, se muestran algunos puntos de interés que permitirán evidenciar la magnitud de las amenazas relacionadas con la ciberseguridad, la información, las infraestructuras críticas y la seguridad de los usuarios, los cuales a su vez son parte de un estado.

Figura 10. Relación de la ciberseguridad con la inteligencia estatal. [Gráfico]. *Creación propia. Con base en datos de ABC Software* (Natour, 2017).

De esta manera, podemos encontrar una serie de eventos o situaciones, que, al compararlos con lo enunciado en la normativa vigente, como es la constitución nacional y demás decretos de inteligencia, es función del sector el identificar y contrarrestar amenazas que pongan en peligro los intereses del Estado, relacionados con:

"Servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes,

creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales ***del Estado y de los particulares.*** *"* (Contitución Nacional de Colombia, 2020)

De esta manera, y siendo el Sector de inteligencia encargado de gestionar riesgos y amenazas, y encontrar oportunidades en pro de los fines esenciales del estado, resulta vital la creación de un CSIRT de inteligencia que permita coordinar los esfuerzos enfocados en la protección de dichos fines, desde un enfoque proactivo.

Con base en la identificación, clasificación y priorización de la infraestructura critica cibernética del país, ejercicio que se realizo con los diferentes actores responsables del tema de ciberseguridad, entre ellos la Dirección Nacional de Inteligencia – DNI y que se encuentran clasificados en el Catalogo de infraestructuras criticas cibernéticas de Colombia, la identificación de trece sectores, cuya criticidad para el país es muy alta; aunado al crecimiento de las actividades criminales como el ransomware, el malware, las APT y las nuevas amenazas sobre los dispositivos móviles, y teniendo en cuenta que los equipos de respuesta realmente son pocos a nivel nacional, su respuesta a nivel gubernamental descentralizado es lenta y poco oportuna; por otra parte el fortalecimiento de las actividades tanto preventivas como investigativas llevadas a cabo por la Dirección Nacional de Inteligencia con su equipo de Cinerseguridad, determina la necesidad que en dicha entidad se fortalezca esta unidad y se dedique de manera permanente a la respuesta de incidentes con el fin de integrarse a la colaboración interinstitucional contra dichos eventos.

Esto plantea la pregunta de investigación a tratar en este trabajo, planteando el interrogante de ¿Cuál debe ser el modelo de un Centro de Respuesta a Incidentes Cibernéticos para la Dirección Nacional de Inteligencia?, lo cual trataremos a continuación.

PROBLEMA DE INVESTIGACIÓN

Colombia a partir del desarrollo de su primer CONPES (Consejo Nacional, de Política y Económica y Social, 2011), donde se dictan los lineamientos de Ciberseguridad y Ciberdefensa, ha demostrado que tiene la capacidad de desarrollar el entorno digital, como política nacional, y desde el 2010, está tratando de llevar a todos los rincones de su geografía la conectividad, no como un servicio privilegiado más sino como un derecho que tiene cada ciudadano, buscando posicionarse como parte del mundo interconectado que brinda comodidades al tener acceso a la información. De igual forma estas comodidades ofrecen a los delincuentes, oportunidades para difundir amenazas complejas que explotan a los dispositivos que permiten su consulta o la información que reposa en la nube, convirtiendo el espacio cibernético en un medio para victimizar al público.

Como lo indican estudios de entidades dedicadas a la seguridad como Trend Micro Incorporated, desde 2012, las tendencias de las actividades cibernéticas ilícitas en todo el mundo demostraron cómo algunas amenazas antes desconocidas habían evolucionado hasta volverse omnipresentes y convertirse en un peligro para todo tipo de usuarios del internet. Colombia no escapa a estas amenazas de acuerdo con el colCERT [1]— el CSIRT nacional de Colombia — Nuestro país registró menos incidentes cibernéticos en los últimos años, lo que lo coloca junto con Chile como uno de los pocos países latinoamericanos con esa distinción. No obstante, no es claro si esto se debió a una reducción real en el número de incidentes, a una mejor gestión de la seguridad por parte de las agencias gubernamentales atendidas por los CSIRT o a la implementación de

[1] Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

políticas que cambiaron la cobertura de la asistencia prestada por los equipos de respuesta de Colombia.

Sea como fuere, el fraude fue el tipo de incidente cibernético más común reportado por el colCERT en la lista de incidentes cibernéticos de Colombia; esta lista contiene además, distintos tipos de Hacking y Spoofing de páginas web y más de uno de los equipos de respuesta del país reportó ataques de hacktivistas, dirigidos en su mayoría contra entidades estatales y militares e instituciones financieras generando para el gobierno Colombiano la aceptación del fenómeno generalizado que indica los bajos niveles de conciencia de la seguridad cibernética, lo que precipita hábitos de navegación inseguros y había provocado la defraudación de usuarios del internet vulnerables. Además, la insuficiente capacitación sobre ataques avanzados, las dificultades para preservar y examinar evidencias digitales y la falta de cooperación de los proveedores de servicios de internet y otras organizaciones privadas constituyeron impedimentos importantes para poner freno a la delincuencia cibernética en Colombia; donde no existe un ente gubernamental que permita generar conocimiento continuo y extendido, no solo a entidades como la Policía y las Fuerzas Militares, sino entes de gobierno descentralizados; no se desconoce que existen iniciativas dispersas y por qué parte de entes comerciales este sea un nicho de venta que se ofrece con unos altos costos a las entidades con mayor presupuesto.

En el escenario global, se conoce en medios de comunicación, escándalos relacionados con intervenciones en elecciones, opinión pública, secretos militares y de Estado, entre otros, en donde es claro que la ciberseguridad juega un papel importante en las interacciones, cada vez mayores, de los ciudadanos del mundo a través del ciberespacio. Esto significa que el ciberespacio se ha convertido de manera muy rápida, en el escenario de enfrentamiento, en donde los intereses tangibles e intangibles pueden ser afectados.

Figura 11. Interconexión de los mundos en el ciberespacio. [Gráfico]. Creación propia.

Con este panorama; aunado a las labores y responsabilidades asignadas en el documento CONPES 3854 (Consejo Nacional, de Política y Económica y Social, 2016), a la Dirección Nacional de Inteligencia, la cual es una organización de inteligencia estratégica joven, posicionada entre las entidades de inteligencia a nivel internacional y siendo un referente de estas, se presenta una oportunidad de innovación al proponer una plan estratégico general que permita reforzar las capacidades de ciberseguridad en la Dirección Nacional de Inteligencia y en el País, que defina un marco de referencia que permita aprovechar las oportunidades que se presentan en la tecnología y los riesgos, con el fin de capitalizarlos como oportunidades de crecimiento para el Estado Colombiano, en donde se pueden tocar temas relacionados con la academia, la tecnología y su uso, gobierno digital orientado a la ciberseguridad, entre otros.

Con base en la pregunta planteada, se puede plantear una matriz DOFA (deGerencia, 2018), el cual permite establecer cual es la situación actual de la Dirección y con base en este plantear la estrategia a seguir.

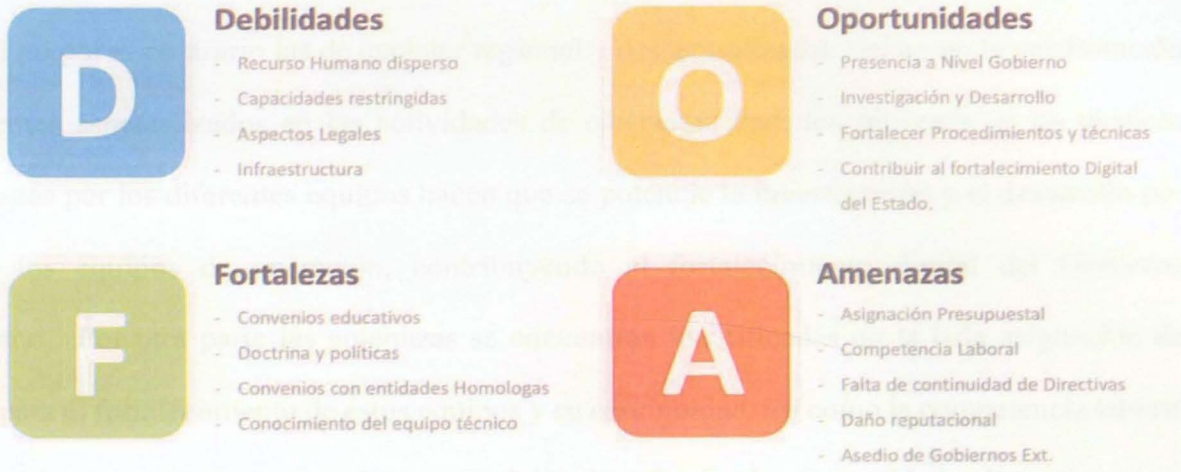

Figura 12. Matriz DOFA de la Dirección Nacional de Inteligencia. [Gráfico]. Creación propia.

Como se puede inferir desde las capacidades internas; las debilidades que tiene la creación de un CSIRT dentro de la Dirección Nacional de Inteligencia – DNI, indica que se posee un recurso humano capacitado y entrenado pero esta disperso en varias dependencias cuyas capacidades son restringidas entre ellas la limitada infraestructura tecnológica, ya que no se tiene un área dedicada única y exclusivamente para tal fin; así como algunos aspectos legales como la falta de funciones de policía judicial para judicializar los resultados de las investigaciones. Sin embargo las fortalezas con las que cuenta la entidad, esta en sus convenios con entidades educativas, con las cuales se puede trabajar proyectos de investigación y desarrollo, así como la fortaleza que se tiene en cuanto a la fuerte doctrina y políticas que se han implantado, cuyo fruto esta relacionado con la certificación ISO 27001 obtenida por la entidad, aumenta la credibilidad de las acciones realizadas

por la entidad que llevan a una interacción con homólogos internacionales por medio de convenios que fortalecen el conocimiento de ;los equipos técnicos.

En cuanto a los factores externos como las oportunidades, esta la presencia de la Dirección a nivel Gobierno, que le permite un transito entre las entidades gubernamentales no solo de nivel central, si no por el contrario las de carácter regional y descentralizadas, así como la colaboración con los entes especializados en las actividades de ciberseguridad; los procesos y las técnicas desarrolladas por los diferentes equipos hacen que se potencie la investigación y el desarrollo por parte de los equipos de operación, contribuyendo al fortalecimiento digital del Gobierno Colombiano. Por otra parte las amenazas se encuentran identificadas en la baja asignación de recursos para el fortalecimiento de estos equipos y su continuidad, así como la competencia laboral que busca el recurso humano capacitado especializado, ofreciendo oportunidades llamativas para los funcionarios, así como la continuidad de los proyectos al presentarse el cambio de las directivas de la entidad y lo mas complicado es el asedio de gobiernos externos con el fin de generar daños reputacionales a los entes de Gobierno.

Por medio de actividades adversas en el ciberespacio, otros países, organizaciones, o elementos hostiles, estarían en la capacidad de detectar y aprovechas estos riesgos, amenazas y oportunidades buscando afectar los fines del Estado Colombiano, en donde la información, la reputación institucional, afectación a infraestructura critica, daño a la población, son elementos críticos a proteger, los cuales se ven incrementados con el uso nuevas tecnologías (generalmente extranjeras o foráneas), comunicación en la nube, IOT, redes sociales, los cuales pueden ser utilizadas en contra de los intereses del Estado.

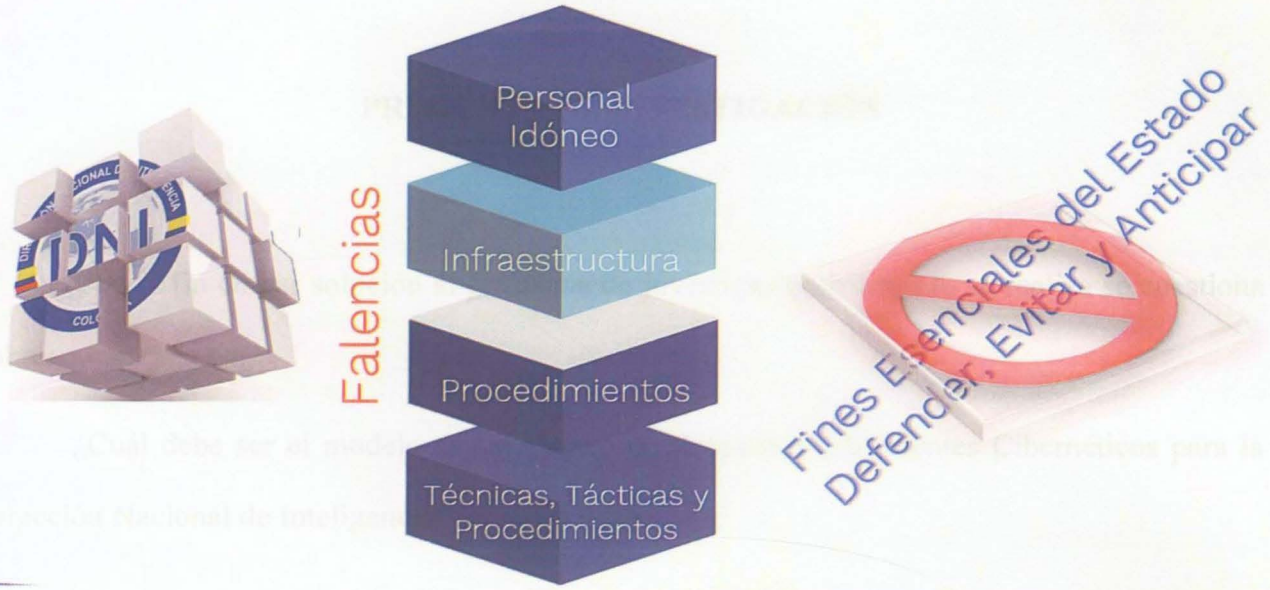

Figura 13. Elementos de riesgos y oportunidades. [Gráfico]. Creación propia.

Esto permite entender la necesidad de contar con un modelo o marco de referencia ágil que permita gestionar de manera correcta (proactiva y reactivamente), la ciberseguridad desde el SOC de la Dirección Nacional de Inteligencia - DNI.

PREGUNTA DE INVESTIGACIÓN

Con el fin de dar solución al problema de investigación planteado se realiza se cuestiona sobre:

¿Cuál debe ser el modelo de un Centro de Respuesta a Incidentes Cibernéticos para la Dirección Nacional de Inteligencia?

Esto permitirá entender las características, normativas necesarias, elementos físicos, tecnológicos y humanos necesarios para el correcto funcionamiento del CSIRT para el sector de inteligencia.

JUSTIFICACIÓN

El CONPES 3701 del 2011 (Consejo Nacional, de Política y Económica y Social, 2011) de Ciberseguridad y Ciberdefensa, le fueron asignadas tareas y actividades encaminadas al fortalecimiento de la política de Gobierno, y en su plan de acción y seguimiento liderado por el DNP se le asignaron actividades a cumplir en los siguientes 4 años a los ministerios y departamentos administrativos, así:

#	Actividades Plan de Accion	Responsable
1	Aprobar los lineamientos de Política para el desarrollo e impulso de la ciberdefensa y la ciberseguridad, presentados en este documento.	Departamento Nacional de Planeación
2	Solicitar al Ministerio de Defensa Nacional y al Ministerio de Tecnologías de la Información y las Comunicaciones adoptar el mecanismo de coordinación intersectorial más adecuado para emitir los lineamientos rectores del colCERT. En caso de no existir uno, se solicita su creación.	Ministerio de Defensa Nacional, Ministerio de Tecnologías de la Información y las Comunicaciones
3	Solicitar al Ministerio de Defensa Nacional crear el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT.	Ministerio de Defensa Nacional
4	Solicitar al Ministerio de Defensa Nacional que una vez creado el colCERT, emita los modelos de seguridad en el ciberespacio que minimicen el nivel de riesgo al que las entidades están expuestas.	Ministerio de Defensa Nacional
5	Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones y a la Comisión de Regulación de Comunicaciones realizar el acompañamiento al Ministerio de Defensa Nacional en las actividades que se consideren pertinentes para la conformación y el desarrollo de las actividades del colCERT.	Ministerio del Tecnologías de Información y las Comunicaciones, Comisión de Regulación de las Comunicaciones
6	Solicitar al Ministerio de Justicia (Ministerio del Interior y de Justicia), al Ministerio del Tecnologías de Información y las Comunicaciones, y a la Dirección Nacional de Inteligencia (Departamento Administrativo de Seguridad o quien haga sus veces), destinar recurso humano con conocimientos técnicos y/o jurídicos en el tema de seguridad de la información y ciberseguridad, para apoyar la ejecución de actividades del colCERT.	Ministerio de Justicia (Ministerio del Interior y de Justicia), Ministerio del Tecnologías de Información y las Comunicaciones, DNI (DAS o quien haga sus veces)
7	Solicitar al Ministerio de Defensa Nacional crear el Centro Cibernético Policial – CCP.	Ministerio de Defensa Nacional
8	Solicitar al Ministerio de Defensa Nacional crear el Comando Conjunto Cibernético – CCOC.	Ministerio de Defensa Nacional
9	Solicitar al Ministerio de Defensa Nacional realizar en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones estudios en seguridad de la información, así como la identificación de la infraestructura crítica nacional.	Ministerio de Defensa Nacional
10	Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones emitir un documento con las directrices en temas de seguridad de la información basado en estándares internacionales, que deberán ser implementadas por las entidades del sector público.	Ministerio de Tecnologías de la Información y Comunicaciones
11	Solicitar a la Comisión de Regulación de Comunicaciones realizar un análisis regulatorio acerca de los aspectos técnicos que deben cumplir los proveedores de redes y servicios de telecomunicaciones para garantizar los principios de confidencialidad de datos, integridad de datos y disponibilidad, así como las medidas para autenticación y acceso de los usuarios a la red y el no repudio de las comunicaciones y, en caso de ser requerido a partir de tal análisis, llevar a cabo los ajustes a que haya lugar frente al marco regulatorio vigente.	Comisión de Regulación de las Comunicaciones
12	Solicitar al Ministerio de las Tecnologías de la Información y las Comunicaciones, facilitar los canales institucionales para que el colCERT pueda realizar la sensibilización y concienciación en temas de seguridad cibernética.	Ministerio de Tecnologías de la Información y las Comunicaciones
13	Solicitar al Ministerio de Defensa Nacional en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, diseñar las campañas de sensibilización y concienciación en temas de seguridad cibernética.	Ministerio de Defensa Nacional
14	Solicitar al Ministerio de Defensa Nacional implementar gradualmente asignaturas en seguridad de la información, ciberdefensa y ciberseguridad (teórico-prácticas), en las escuelas de formación y de capacitación de oficiales y suboficiales.	Ministerio de Defensa Nacional
15	Solicitar al Ministerio de Defensa Nacional adelantar un plan de capacitación en temas de seguridad de la información para los funcionarios del Estado, con el apoyo de organismos internacionales.	Ministerio de Defensa Nacional
16	Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones, al Ministerio de Defensa Nacional y a la Dirección Nacional de Inteligencia (Departamento Administrativo de Seguridad o a quien haga sus veces), diseñar e implementar planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial.	Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, DNI (DAS o quien haga sus veces).
17	Sugerir a la Fiscalía General de la Nación en coordinación con el Consejo Superior de la Judicatura diseñar e implementar planes de capacitación sobre temas de investigación y judicialización de delitos informáticos, para policía judicial, jueces y fiscales.	Fiscalía General de la Nación
18	Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información.	Ministerio de Tecnologías de la Información y Comunicaciones
19	Solicitar al Ministerio de Justicia (Ministerio del Interior y de Justicia) realizar en coordinación con el el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de Información y Comunicaciones, un documento en el que se analice la normatividad actual y se propongan las modificaciones necesarias en materia de seguridad de la información y protección de datos para prevenir el ciberdelito, identificando las dificultades de interpretación y aplicación.	Ministerio de Justicia (Ministerio del Interior y de Justicia)
20	Solicitar al Ministerio de Justicia (Ministerio del Interior y de Justicia), en coordinación con el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones, con base en el análisis realizado, adelantar las iniciativas tendientes a expedir o reformar las leyes que sean necesarias así como reglamentar aquellas a que haya lugar, en aras de garantizar el marco normativo adecuado para la ciberseguridad, la ciberdefensa y la seguridad de la información.	Ministerio de Justicia (Ministerio del Interior y de Justicia)
21	Solicitar al Ministerio de Relaciones Exteriores apoyar al colCERT, en materia de cooperación internacional, en los temas de ciberseguridad, ciberdefensa y seguridad informática, en los que se incluya la designación del colCERT como punto de contacto internacional en temas referentes a la ciberseguridad y la ciberdefensa.	Ministerio de Relaciones Exteriores
22	Solicitar al Ministerio de Relaciones Exteriores, estudiar la viabilidad y conveniencia para Colombia de adherir a los principales instrumentos internacionales en materia de seguridad de la información y protección de datos, con el directo apoyo del Ministerio de Defensa Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones. En caso de que el estudio produzca una recomendación positiva, iniciar los trámites de adhesión al instrumento que corresponda.	Ministerio de Relaciones Exteriores

Tabla 1. Plan de Acción y Seguimiento CONPES 3701 2011. Recuperado de (Dirección Nacional de Inteligencia - DNI, 2011).

En este plan de acción y seguimiento, ya se identifican tareas de la Dirección Nacional de Inteligencia, específicamente asumiendo las actividades asignadas en ese momento al Departamento Administrativo de Seguridad, el PAS tenía en este párrafo en la parte de responsables "*Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, Dirección Nacional de Inteligencia - DNI (DAS o quien haga sus veces)*"; desde ese momento se identificó que la Dirección Nacional de Inteligencia - DNI reemplazaría o asumiría algunas funciones del DAS en proceso de supresión (WRadio, 2020).

Esta situación fue aclarada en las sesiones de seguimiento al cumplimiento del CONPES del Departamento Nacional de Planeación DNP, año en que fue invitado a los comités de acción y seguimiento a la Política CONPES 3701 de Ciberseguridad y Ciberdefensa; lo anterior con la salvedad de que la entidad no tenía asignadas metas ni actividades en este CONPES; por haber sido creada posterior a su lanzamiento, pero desde ahí comenzó la participación activa en la Comunidad de Seguridad Digital Nacional y en la asesoría y participación en los diferentes eventos nacionales de seguridad, ciberseguridad y Ciberdefensa.

Dentro de los eventos nacionales de seguridad digital a los cuales fue convocada la Dirección Nacional de Inteligencia, figura la conformación de los Puestos de Mando Unificados PMU Ciber, convocados para las jornadas electorales realizadas por la Registraduría, cuyo fin radicaba en el monitorear y verificar el comportamiento de la infraestructura, canales de comunicación, plataformas y sistemas de información que participaban de la jornada electoral. Durante una de las jornadas de octubre de 2016, fue cuando se identificó la afectación en la integridad de uno de los portales de la Registraduría de consulta de cedulas, como se muestra en las noticias reportadas en su momento.

Investigan hackeo a la página web de la Registraduría Nacional

Recommend 1 Share septiembre 30, 2016 5:12 pm

Tags de esta nota: Fiscalía General • HACKER • Portal web • Registraduría

La indagación es adelantada por la Fiscalía General, con el propósito de determinar el origen y los autores del hackeo ocasionado en el sitio web de la Registraduría Nacional del Estado Civil tres días antes al plebiscito del próximo domingo.

La investigación se lleva a cabo pese a que Juan Carlos Galindo, registrador nacional del Estado Civil, asegurara que la entidad garantizará que no habrá ningún inconveniente durante el proceso de votación del plebiscito.

Un grupo de expertos fiscales y agentes de policía judicial en temas de informática, será el encargado de adelantar el proceso investigativo para de practicar pruebas y encontrar rastros que permitan determinar quiénes fueron los responsables del ataque a la página.

Se pretende identificar cómo fueron evadidos los controles de seguridad y vulnerada la plataforma web de la Registraduría Nacional, situación que por varias horas hizo se viera afectado el servicio para aquellos usuarios que consultaban el portal.

Con estas labores se busca dar total transparencia al proceso electoral del 2 de octubre y así evitar alteraciones en desarrollo de esta jornada de votación del plebiscito.

Figura 14. Noticia de afectación de la integridad y disponibilidad del portal de la Registraduría. [Infografía]. Recuperado de: Investigan hackeo a la página web de la Registraduría Nacional http://www.radiosantafe.com/2016/09/30/investigan-hackeo-a-la-pagina-web-de-la-registraduria-nacional/ (Radio Santafé, 2016).

Inicio / Judicial / Hackearon a la página de la Registraduría

Hackearon a la página de la Registraduría

Judicial 28 sep. 2016 - 3:10 p. m.
Por: Redacción Política

Varios usuarios que han intentado consultar su puesto de votación o si son jurados para el plebiscito de este domingo, denunciaron en redes sociales fallas en el sistema.

A solo cuatro días de la votación del plebiscito con el que los colombianos decidirán si respaldan o no el acuerdo de paz entre el Gobierno y las Farc, la página web de la Registraduría Nacional del Estado Civil (www.registraduria.gov.co) fue objeto de ataques de hackers que, aunque no afectaron de forma definitiva el portal, sí prendieron las alarmas de cara a la importante decisión que tomarán los colombianos.

Figura 15. Noticia de afectación de la integridad y disponibilidad del portal de la Registraduría [Infografía]. Recuperado de: el Espectador https://www.elespectador.com/noticias/judicial/hackearon-a-la-pagina-de-la-registraduria/ (El Espectador, 2020).

Debido a la criticidad de la situación, fue convocada una mesa técnica de investigación e indagación conformada por personal de la Fiscalía, DIJIN, colCERT y la Dirección Nacional de Inteligencia - DNI, lo cual refleja el posicionamiento adquirido a nivel Nacional de Seguridad Digital.

Otro evento relevante de participación fue la construcción del CONPES 3854 de 2016 (Consejo Nacional, de Política y Económica y Social, 2016), Política Nacional de Seguridad Digital, el cual requirió múltiples mesas técnicas de trabajo, lo cual obtuvo como producto un CONPES aterrizado a la necesidad nacional y direccionado a atender y entender la problemática de Seguridad Digital Nacional. Por su activa participación en su construcción, la Dirección Nacional de Inteligencia - DNI fue incluida dentro de la portada del CONPES.

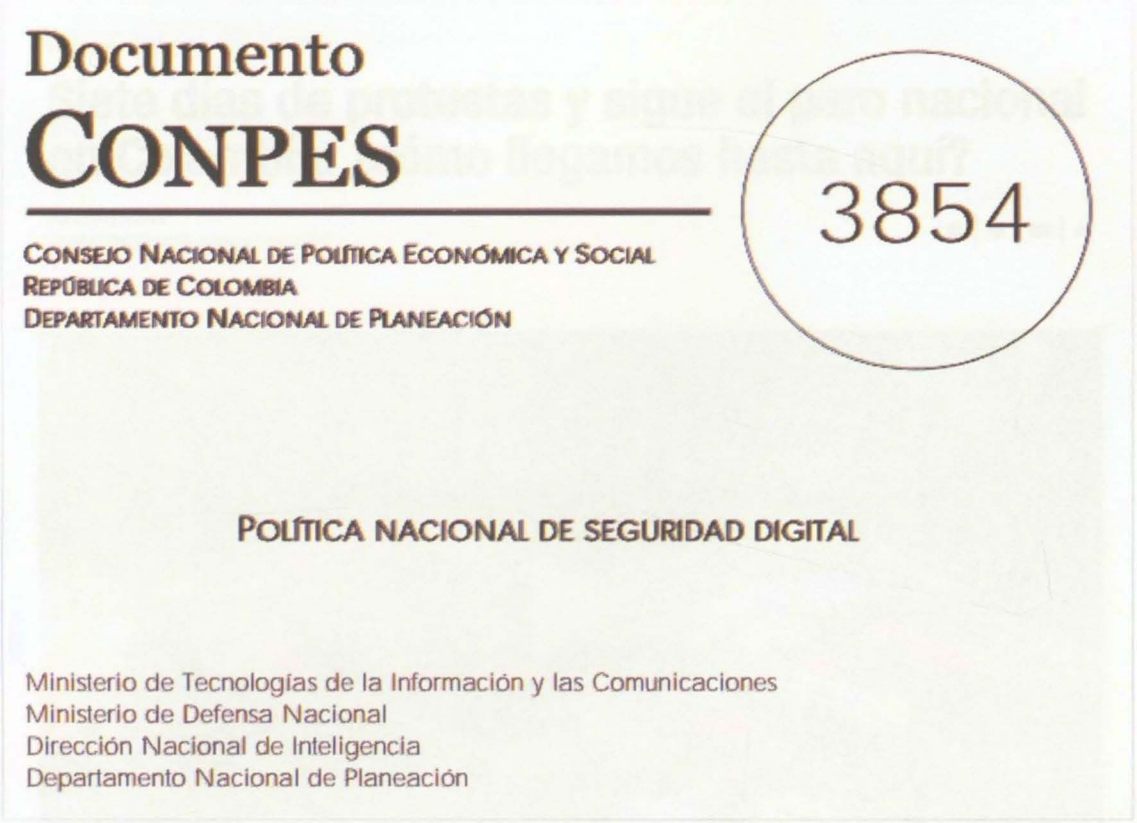

Figura 16. Inclusión de la Dirección Nacional de Inteligencia - DNI como constructor activo de la Político. Recuperado de: Consejo Nacional, de Política y Económica y Social. Documento CONPES 3854 - Política de Seguridad Digital.

https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-

Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y (Consejo Nacional, de Política y Económica y Social, 2016)

Otro evento relevante que muestra la participación de la entidad en los eventos y jomadas nacionales que tienen que ver con la seguridad digital nacional, fue las marchas de protesta realizadas en noviembre de 2019.

COLOMBIA

Siete días de protestas y sigue el paro nacional en Colombia: ¿cómo llegamos hasta aquí?

Por CNN Español
14:49 ET(18:49 GMT) 27 November, 2019

(CNN Español) — Llegamos a siete días de protestas en Colombia y el paro nacional, convocado por diversos sectores no parece tener un fin cercano. Este martes, tras una reunión con el presidente Iván Duque, el Comité del Paro Nacional convocó a una nueva jornada de manifestaciones.

Figura 17. Jornadas de protesta en Colombia nov/2019. [Infografía]. Recuperado de: Cable News Network – CNN. https://cnnespanol.cnn.com/2019/11/27/siete-dias-de-protestas-y-sigue-el-paro-nacional-en-colombia-como-llegamos-hasta-aqui/ (Cable News Network - CNN, 2020).

Estas marchas se vieron marcadas por la masiva manipulación de las redes sociales y falsas noticias - fakenews; ante lo cual se convocó al PMU Ciber en el C4 Policial, a fin de realizar seguimiento a tendencias y monitorear el comportamiento de las redes sociales.

Debido a la gran desinformación que se presentó durante las jornadas, como se muestra a continuación:

DEMOCRACIAABIERTA

Movilización, desinformación y pánico en Colombia: es la hora de la responsabilidad

Durante la última semana, miles de manifestantes han paralizado las calles de las principales ciudades de Colombia.

Paro Nacional Colombia. Beverly Goldberg.

Durante la última semana, miles de manifestantes han paralizado las calles de las principales ciudades de Colombia. El desencadenante fue en un paro nacional de protesta convocado para el día 21 de noviembre, pero que, ante la inusitada y violenta reacción del Estado, ha continuado intermitentemente y se anuncia nuevamente para hoy.

Muchos analistas y comentaristas vinculan estas protestas a lo que se ha venido a denominar una "tormenta ciudadana", inspirada en movilizaciones recientes que estallaron en Chile y Ecuador, con resultados diferentes y de las que el gobierno de Duque debería aprender.

Figura 18. Jornadas de protesta en Colombia nov/2019. [Infografía]. Recuperado de: openDemocracy. https://www.opendemocracy.net/es/democraciaabierta-es/movilizaci%C3%B3n-desinformaci%C3%B3n-y-p%C3%A1nico-en-colombia-es-la-hora-de-la-responsabilidad/ (openDemocracy, 2020).

El comité nacional de seguridad digital, por intermedio de MINTIC emitió un boletín para **ser difundido a la ciudadanía, llamado** "*Lineamientos de seguridad de la información, frente a*

manifestaciones violentas en el ciberespacio", **donde se incluían teléfonos, correos y link`s de** contacto ciudadano para indagar y corroborar las noticias de desinformación que se estaban presentando, y la Dirección Nacional de Inteligencia - DNI formaba parte de esos nodos de contacto ciudadano, como articulador del proceso de seguridad digital nacional.

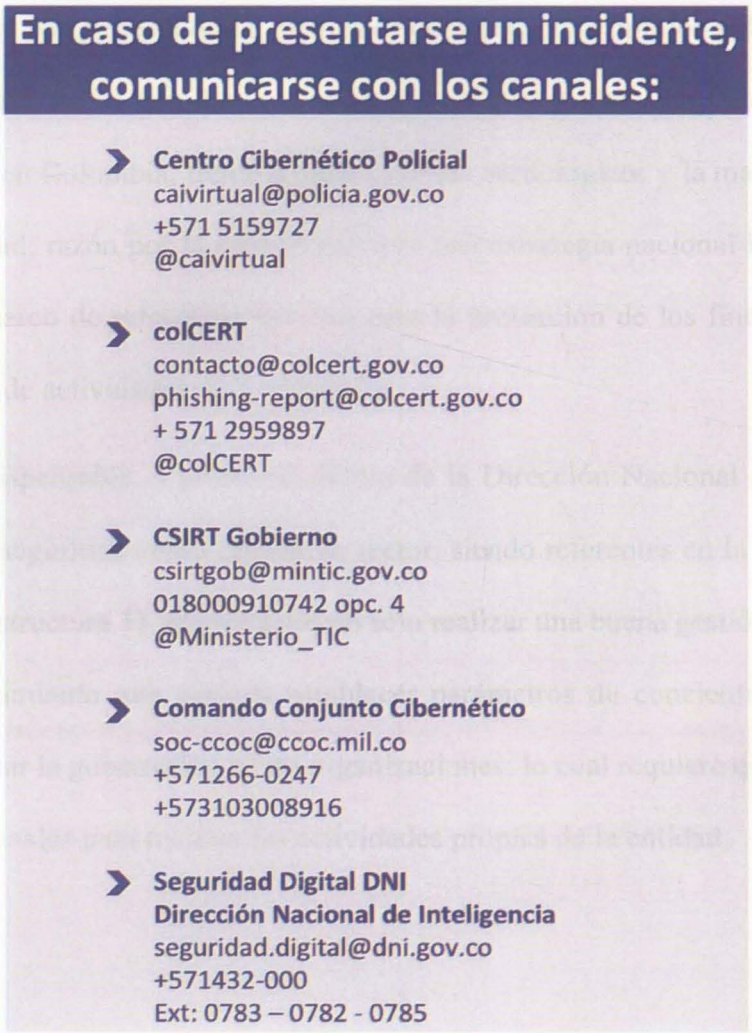

Figura 19. Lineamientos de seguridad de la información, frente a manifestaciones violentas en el ciberespacio. [Infografía]. Recuperado de: Ministerio de Tecnologias de la Información - MINTIC (Ministerio de Tecnologias de la Información - MINTIC, 2019).

Lo cual demuestra la participación y posicionamiento que ha tenido la entidad en la política nacional de seguridad digital desde su creación.

Actualmente, el mundo se mantiene en un constante cambio de transformación digital, en el cual se puede apreciar un crecimiento de las amenazas de los Estados, relacionadas no solo con geopolítica, sino también con geoeconomía, medios de comunicación, opinión pública, entre otros aspectos. Adicionalmente, no se percibe un lineamiento oficial y claro respecto al papel de la inteligencia estratégica en Colombia, frente a estos cambios tecnológicos y la masificación de los servicios de conectividad; razón por la cual se requiere una estrategia nacional inicial que tenga como fin generar un marco de referencia mínimo para la protección de los fines esenciales del estado, en el desarrollo de actividades de inteligencia.

Por esto, es indispensable el posicionamiento de la Dirección Nacional de Inteligencia - DNI en temas de Ciberseguridad como cabeza de sector, siendo referentes en la protección de la información y su infraestructura TI, permitiendo no solo realizar una buena gestión proactiva, sino también generar conocimiento que permita establecer parámetros de concientización, difusión gubernamental, apalancar la gobernanza en las organizaciones; lo cual requiere que se fortalezcan las estrategias institucionales para realizar las actividades propias de la entidad.

Con ese fin y gracias al fácil uso de internet y el crecimiento exponencial del tema de ciberseguridad, es posible acotar un modelo de los diferentes aportados por los investigadores de estos temas y aplicarlo a la organización.

Como menciona ISACA en su artículo Incident Response – Being Prepared for the Worst Case Scenario, 2017 (Gates, ISACA NOW BLOG , 2017) que dice traducido al español: *"¿Quién necesita respuesta a incidentes? En resumen: todos. Todas las empresas tienen propiedad intelectual, información de identificación personal (PII), información financiera o alguna forma de información confidencial que puede ser peligrosa cuando está en las manos equivocadas. Establecer un plan procesable dará como resultado tiempos de respuesta más rápidos y minimizará los daños como resultado de un incidente.*

Los riesgos potenciales que enfrenta su organización como resultado de una respuesta deficiente a un incidente son enormes y pueden variar según la industria. Dicho esto, a continuación, se detallan algunos de los riesgos más comunes a tener en cuenta al evaluar el valor del plan de respuesta a incidentes de su organización:

Riesgos operacionales. Un incidente como una violación del sistema podría resultar en que los sistemas y aplicaciones críticos no funcionen. Esto puede conducir a la pérdida de funciones comerciales centrales (como el cierre de una línea de producción), así como a posibles vulnerabilidades de seguridad.

Riesgos reputacionales. Responder mal a un incidente puede tener impactos muy negativos en la imagen pública de su organización, así como a los ojos de sus clientes actuales y potenciales.

Riesgos de cumplimiento. En algunos casos, un incidente puede resultar en la incapacidad de cumplir con los requisitos reglamentarios e introduce la posibilidad de multas y / o sanciones por parte de los órganos rectores.

Riesgos financieros. Todos los riesgos mencionados anteriormente tienen el potencial de resultar en un impacto financiero negativo para su organización. Estos, junto con la posibilidad de pérdida de activos, el costo de las reparaciones, los honorarios legales y otros costos ***inesperados deben considerarse****".*

En esta descripción se ubican gran parte de las justificaciones de porque la Dirección Nacional de Inteligencia debe contar con la capacidad de un grupo de gestión de incidentes que permita mediante el monitoreo y correlación de eventos generar los procesos de identificación, contención, recolección, análisis, aplicación de correctivos y mejoras y documentación como base de conocimiento y consulta; que permita la mitigación de los riesgos y la mejora continua en los procesos de aseguramiento de la información y la infraestructura tecnológica al servicio de la Entidad.

Revisión del Entorno - CSIRT Existentes.

CSIRT Policial.

Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL (PONAL, 2020), un grupo creado para atender las necesidades de prevención, atención e

investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.

Misión. Garantizar las condiciones necesarias para el aseguramiento de la plataforma tecnológica de la Policía Nacional, como apoyo a la estrategia de ciberseguridad y Ciberdefensa de la Nación.

Objetivos Específicos

Proveer asistencia técnica, asesoría y apoyo a la comunidad y a las organizaciones en general, en la protección de amenazas y/o incidentes informáticos. Consolidar los procesos y procedimientos de atención de incidentes de seguridad de la información mediante el uso de estándares y buenas prácticas. Activar los mecanismos de colaboración para la coordinación y gestión de incidentes entre entidades.

Servicios.

- Análisis de artefactos cibernéticos mediante Sandbox
- Análisis de APK
- Entrenamiento Capture the Flag
- Plataforma MISP (Malware Información Sharing Platform)

Según lo que se identifica en el CSIRT Policial, es una actividad reactiva, en el sentido de que los clientes (posibles afectados), deben conocer esta instancia de autoridad, de apoyo y orientación y reportar los casos de los cuales hayan sido objeto de afectación.

CSIRT Gobierno (Gobiernoenlinea, 2020)

Esta instancia se articula con las instancias del ColCERT, C4, CCOCI, Csirt Policial y el MINTIC, integrando esfuerzos de seguimiento y monitoreo al Ciberespacio en tiempo real.

Su propósito es brindar servicios de respuesta a las entidades del Estado, además de contribuir con el fortalecimiento de la seguridad y generación de confianza ante la ciudadanía. El proyecto es el resultado de un convenio suscrito entre la Policía Nacional y el MinTIC por un valor de $4.500 millones de pesos, el cual hace parte de las actividades previstas en los documentos CONPES 3701 de 2011 y 3854 de 2016, relacionados con la ciberseguridad y Ciberdefensa y la seguridad digital, respectivamente.

CSIRT Financiero.

El CSIRT Financiero (csirtasobancaria, 2020) es el equipo de respuesta de apoyo a la respuesta de incidentes del sector financiero que fomenta la colaboración de sus miembros y el intercambio de información para afrontar de manera efectiva las amenazas cibernéticas. Nuestro equipo,

altamente calificado contribuye en los procesos de gestión de riesgos y seguridad de datos con el fin de crear espacios digitales seguros.

Funciones

- Apoyar a las entidades financieras en el fortalecimiento de sus capacidades preventivas y reactivas.
- Fortalecer los estándares de ciberseguridad del sector
- Ser el punto focal del sector financiero para la gestión de crisis e incidentes sectoriales.
- Ejercer la vocería frente a las autoridades nacionales en materia de ciberseguridad
- Promotores de la comunidad de intercambio de información de ciberseguridad del sector financiero con organismos nacionales e internacionales.

Este CSIRT esta direccionado al sector privado, específicamente al sector financiero, contribuyendo a la protección de este sector e integra casi la totalidad del sector, excepto los bancos de Bancolombia y BBVA, por estos contar con sus propias infraestructuras SOC de protección y prevención.

Si bien, forma parte de la comunidad, por su naturaleza privada, poco comparte a nivel de alertas y eventos en términos de oportunidad y reacción en la contención de fenómenos que se presenten en el Ciberespacio.

Teniendo lo anterior, y lo revisado en los capítulos anteriores, en particular antecedentes, podemos concluir que la necesidad de un CSIRT de inteligencia, resulta fundamental al momento de cohesionar una red de cooperación enfocada a la recolección y análisis de información que provea información de valor para toma de decisiones en un mundo altamente interconectado, lo cual se denomina Inteligencia Estratégica y Contrainteligencia de Estado.

Como se puede observar en la siguiente figura, se puede determinar que Colombia tiene en su haber la mayor cantidad de CSIRT a nivel de Latinoamérica, lo que transmite una imagen de seguridad a nivel de la región.

Figura 20. Algunos elementos generales de un CSIRT según CCN España. [Mapa]. *Recuperado de: www.observatoriociberseguridad.com ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe 2020 Reporte Ciberseguridad (Banco Interamericano de Desarrollo , 2020)*

El modelo de interacción que se plantea con los diferentes CSIRT existentes, busca es fortalecer las capacidades con que cuentan en la actualidad estos grupos, aumentando las relaciones con los diferentes actores, involucrándose con la academia por medio de convenios, que

permitan perfilar y forjar personal técnico necesario para el mantenimiento de estos equipos, empoderando un nivel de respuesta a todos los sectores del país brindando capacidades que puedan brindar la base en materia de seguridad, para el cumplimiento de la Estrategia de Integración Digital del Estado.

Figura 21. Modelo de Interacción del CSIRT de la Dirección Nacional de Inteligencia. [Gráfico]. Creación propia.

ALCANCE

Para esta investigación, se delimito un alcance relacionado con la proposición teórica de elementos mínimos necesarios para la implementación de un CSIRT en el sector de inteligencia, que cumpla con las condiciones necesarias y se adapte a las necesidades propuestas en este documento.

Un elemento importante es que, si bien se toman como referencias estándares mundiales, ejemplos de CSIRT, opiniones de expertos, entre otros, se tomaran ciertas libertades para proponer elementos de las necesidades debido a que el conocimiento en el área de inteligencia es muy limitado en su bibliografía y el autor cuenta con considerables años de experiencia en el sector.

Dentro de las limitantes encontradas, se percibe la falta de documentación especifica en temas de estructuración, conformación o diseño de Grupos de Respuestas o CSIRT para el sector de inteligencia, sin embrago se pudo encontrar información académica y de organismos multilaterales, relevante para otros sectores, incluyendo Gobierno.

OBJETIVOS

A continuación, se muestran el objetivo general y los objetivos específicos para el desarrollo de esta propuesta

Objetivo general

- Diseñar y estructurar un modelo de CSIRT ajustado a la Dirección Nacional de Inteligencia - DNI.

Objetivos específicos

- Analizar las posibles debilidades, oportunidades, fortalezas y amenazas que se pueden presentar con la implementación del CSIRT para el Sector.
- Diseñar un modelo de CSIRT ajustado a la Dirección Nacional de Inteligencia y a la Comunidad de Inteligencia y su entorno funcional en el estado para fortalecer la anticipación e identificación de la amenaza.
- Proponer un planeamiento de implementación de corto, mediano y largo plazo, detallando la arquitectura y capacidades desarrolladas en cada fase.

METODOLOGÍA

Este trabajo realiza una investigación cuyo enfoque es de tipo cualitativo (Sampieri, 2014) de manera descriptiva y analítica del modelo propuesto por el National Institute of Standards and Technology (NIST), revisando la existencia de los diferentes equipos de respuesta a incidentes nacionales y estructura la opción de puesta en marcha.

A través de la aplicación de conocimientos técnicos, el planteamiento de esta solución podrá determinar la adecuada implementación, con opciones viables para el fortalecimiento del equipo necesario en la Dirección Nacional de Inteligencia.

DISEÑO METODOLÓGICO

Para esta investigación se utilizará un método cualitativo, en el cual se basará principalmente en información abierta disponible, e información de organizaciones, expertos, informes, documentos científicos y gubernamentales, con el fin de extraer los elementos más importantes y redefinirlos para las necesidades del sector de inteligencia en Colombia.

Como fuentes de información se utilizarán bases de datos académicas e información abierta disponible en el buscador Google, Bing, Google Académico, Science Research, entre otros.

HIPÓTESIS DE LA INVESTIGACIÓN

Para esta investigación se propondrá las siguientes Hipótesis con el fin de sustentar la necesidad de la creación de un CSIRT sectorial para la Inteligencia Estatal.

Hipótesis 1: Los riesgos, oportunidades y amenazas para la implementación del CSIRT sectorial, estará relacionadas principalmente con necesidades tecnológicas y de personal, más que por necesidades de recursos económicos.

Hipótesis 2: El modelo de CSIRT requerirá estar interconectado con otros sectores estratégicos.

Con el fin de tener una referencia de carácter gubernamental, y relacionada con los temas de Inteligencia y ciberseguridad, el Centro Criptológico Nacional de España (Ministerio de Defensa de España, 2011), genero ayudas con el fin de crear CERTS que cuenten con unos componentes mínimos para el gobierno.

Dentro de los elementos principales podemos resaltar:

Figura 22. Algunos elementos generales de un CSIRT. [Gráfico]. *Creación propia.*

De la misma forma agencia Europea de Seguridad de las Redes y de la Información (ENISA, 2020) sugiere elementos similares, sin embargo, es enfático en la necesidad de definir el

modo en el cual interactuara con las demás agencias, pares o CSIRT de infraestructuras tanto gubernamentales como no gubernamentales. Esto puede estar ligado directamente dentro del elemento de Modelo de funcionamiento, agregando conceptos como son:

- Políticas.
- Ámbito de actuación.
- Servicios.
- Plan de respuesta.

Debido a los elementos mencionados anteriormente, se ve la necesidad de definir una estrategia empresarial completa para la creación del CSIRT, la cual se desarrollará a lo largo del presente capitulo.

Componentes de un CSIRT

ISACA (Gates, 2017) en su documento relaciona una serie de componentes que recomienda ser tenidos en cuenta para que con plan de respuesta a incidentes sea exitoso, así:

*"**La determinación de los componentes de un plan de respuesta a incidentes exitoso variará** de una empresa a otra, pero en esencia debería ofrecer lo siguiente:*

- *Un compromiso ejecutivo y respaldo de la iniciativa de respuesta a incidentes.*
- *Un Equipo de Respuesta a Incidentes (IRT, por sus siglas en inglés) compuesto por miembros con diferentes áreas de experiencia que van desde TI hasta legal y comunicaciones.*
- *Un plan de comunicación definido.*
- *Un plan para apoyar, mantener y probar el plan de respuesta a incidentes regularmente*

- *Un enfoque organizado y estructurado que defina claramente los roles y responsabilidades de todas las partes involucradas.*
- *Una definición clara de lo que significa un incidente para su organización y cómo la respuesta del incidente se alinea con los esfuerzos de seguridad organizacionales existentes, como la continuidad del negocio y los planes de recuperación ante desastres.*
- *Un plan bien definido sobre cómo monitorear y analizar las posibles amenazas al medio ambiente.*
- *Un plan de operación que define cómo se declaran los incidentes y los pasos iniciales para la recopilación de información.*
- *Un proceso posterior al incidente para las lecciones aprendidas y la mejora del proceso.*

Un programa de respuesta a incidentes exitoso debe alinearse con los estándares establecidos por el Instituto Nacional de Estándares y Tecnología (NIST), la Organización Internacional de Normalización (ISO) y la Biblioteca de Infraestructura de Tecnología de la Información (ITIL)".

Entorno de Aplicación para el CSIRT de Inteligencia

Basado en las funciones que se documentaron en apartes anteriores de este trabajo, y en los entornos de desarrollo, servicios y requerimientos que se podrían presentar para el CSIRT de Inteligencia, se identifica el siguiente entorno de aplicación:

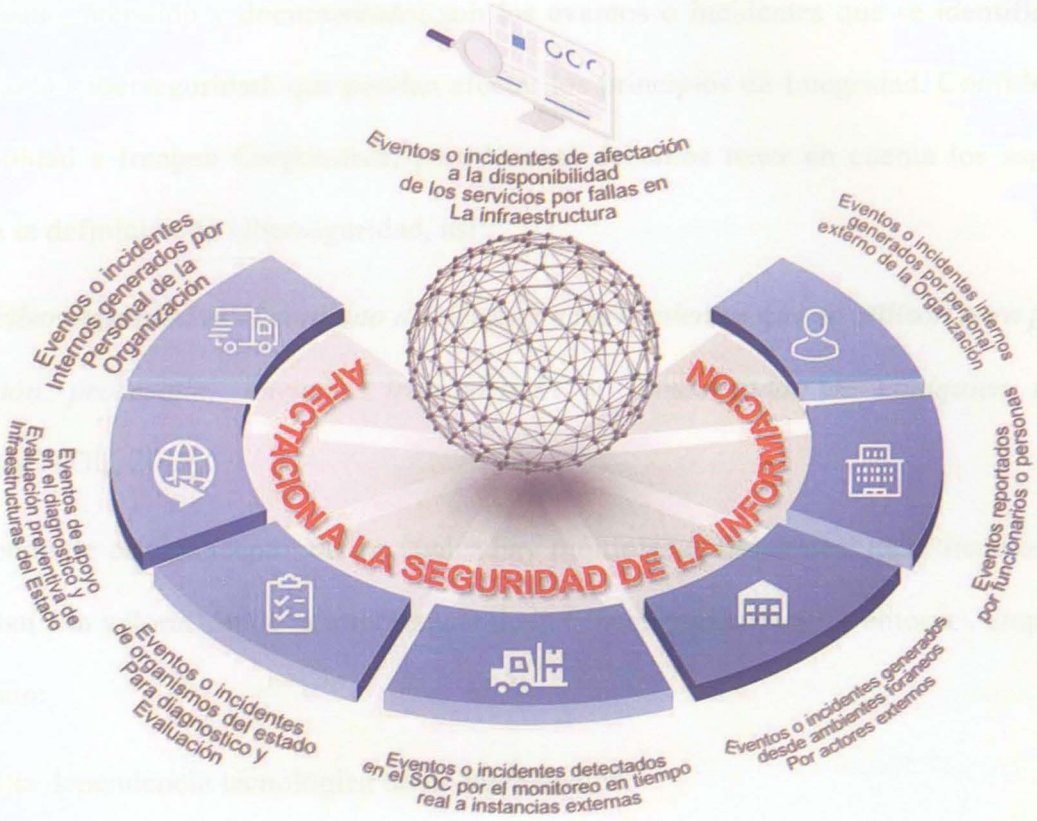

Figura 23. Entorno de aplicación de eventos e incidentes para el CSIRT de Inteligencia. [Infografia]. Creación propia.

Ahora bien, se procederá al análisis de cada uno de estos componentes en el entorno de la Dirección Nacional de Inteligencia - DNI, para identificar aspectos de mejora, o vacíos funcionales, administrativos o de procedimientos que deban ser documentados, así como la interacción que se realizará con otros entes de Gobierno.

Afectación de la Seguridad de la Información

En este proceso debemos identificar que no necesariamente se deba materializar el riesgo para ser verificado, atendido y documentado; son los eventos o incidentes que se identifiquen en el entorno de la Ciberseguridad, que puedan afectar los principios de Integridad, Confidencialidad, Disponibilidad e Imagen Corporativa; para lo cual debemos tener en cuenta los aspectos que involucra la definición de ciberseguridad, así:

"La ciberseguridad es el conjunto de técnicas y herramientas que se utilizan para proteger la *información procesada, enviada, transportada y almacenada en cualquier dispositivo informático"* (GL, 2019).

Partiendo de este concepto, de los cuales hay múltiples definiciones; identificamos variables que aportan a la valoración de la importancia de la Ciberseguridad en los entornos empresariales, algunos son:

- Alta dependencia tecnológica de la organización.
- Dependencia de la actividad preventiva de los usuarios finales.
- Adecuada aplicación de buenas prácticas en la gestión y administración de la infraestructura tecnológica.
- Aplicación de controles y registros de acceso físico a instalaciones.
- Monitoreo del comportamiento de los ambientes de red, internet y servicios y sistemas de información.
- Construcción de procesos, protocolos, procedimientos e instructivos que delimiten y canalicen las actuaciones de las personas en la organización.

Debido a esto, podemos calificar a la Ciberseguridad como un componente transversal a la organización, por medio del cual se pueden materializar los riesgos de pérdida o fuga de información para las organizaciones.

Para todos los esquemas de servicio; que tendrá el CSIRT de Inteligencia, se deben tener en cuenta en la atención de cualquier evento, la valoración de mantenimiento de la cadena de custodia y preservación de la evidencia como punto focal de la indagación y verificación de los diferentes tipos de eventos que se presenten; de ahí que se deba contar con la coordinación directa con las instancias con funciones de policía judicial; para su actuar cuando se requieran.

Eventos o incidentes internos generados por personal de la organización.

En este aspecto, la entidad cuenta con unos esquemas ya implementados a nivel de registro, bloqueo y control de actividad de usuarios en la red; así como la existencia de un sistema de gestión de seguridad de la información, que involucra políticas, procesos, procedimientos, manuales e instructivos para el adecuado uso y gestión de la seguridad de la información corporativa; existe el monitoreo digital en tiempo real, control físico de acceso y retiro de activos y elementos a la entidad y verificaciones físicas periódicas en las instalaciones, que permiten la identificación de la violación de la política; ejemplo de ello, incumplimiento del escritorio limpio al termino de labores, o dejar sin seguridad cajoneras o gabinetes de uso y almacenamiento de información o equipos.

Así mismo, en este esquema se incluyen actividades de envío de información al exterior de la corporación, con llevar a cabo los controles, procesos y procedimientos demandados para este fin, buscando siempre proteger los medios, métodos, fuentes, procesos y procedimientos de la entidad.

Estos procesos de control del sistema de gestión de la seguridad de la información aplican para personal de planta de la entidad, contratistas y personal externo que visita las instalaciones.

El incumplimiento a algún control de la política genera la generación de eventos e incidentes que se documentan y gestionan, midiendo los niveles de riesgo generados por los usuarios.

Eventos o incidentes internos generados por personal externo de la organización.

Para este caso, son eventos detectados a nivel físico, de proceso, o de ingreso a algún esquema tecnológico o de servicio; por parte de un actor externo, que puede ser identificado como que se buscaba afectar o intervenir algún esquema corporativo o se pueda afectar la integridad de algún componente tecnológico.

Estos eventos se deben documentar, para dejar los registros del evento o incidente detectado, para su mejora en procesos y consulta.

Eventos o incidentes generados desde ambientes digitales foráneos por actores externos.

En este caso, se identifican fenómenos que llegan desde ambientes de las redes WAN, que puede incluir canales de datos, de internet y esquemas de conectividad propios; los cuales se ven afectados por actores que intentan penetrar la infraestructura corporativa, en este proceso, gran parte de estos eventos o incidentes son detectados en el SOC corporativo que integra las plataformas del SIEM que a su vez integra los registros de los esquemas de servicio, conectividad, protección, sistemas de seguridad, control y sistemas de información; lo cual requiere el diagnostico, evaluación, contención, remediación y documentación de todo el evento, así como la inclusión de posibles daños colaterales que se puedan haber presentado con la situación.

Eventos o incidentes de afectación a la disponibilidad de los servicios por fallas en la infraestructura.

En este caso, se pueden presentar afectaciones en servicios y sistemas de información, por falla tecnológica de hardware o software o por una inadecuada aplicación de cambios en hardware o software por parte de personal técnico que aplica procesos de cambio en la infraestructura tecnológica y de servicios.

En este proceso, de primera mano se aplican procesos de recuperación del servicio, diagnóstico y evaluación; que permitan la identificación de los cursos de acción para la remediación; dentro de estos procesos se deben identificar si hay daños colaterales a otros servicios y sistemas de información corporativos y la valoración de la posible pérdida de información corporativa.

Eventos o incidentes detectados en el SOC por el monitoreo en tiempo real a instancias externas.

En este caso, esta situación se puede presentar, cuando se tengan esquemas de monitoreo de servicios y protección de esquemas tecnológicos de otras entidades del estado; de común acuerdo; estos eventos detectados en el SOC; permiten la identificación de la actividad o evento objeto de aclaración, le cual debe ser escalado formalmente a las áreas de gestión y administración de la entidad propietaria; a fin de indagar de la posible vulneración de las políticas de seguridad; o si por el contrario, obedece a procesos rutinarios que posiblemente no fueron documentados por las áreas de manera oportuna.

Estos eventos o situaciones deben quedar documentadas y trazadas en los esquemas de servicio; a fin de poder justificar los alcances de servicio y verificación que adelantan las áreas del CSIRT ante la identificación de las diferentes alertas que se presenten.

Eventos o incidentes de organismos del estado para diagnóstico y evaluación.

Para este proceso, se deben identificar 2 procesos separados de requerimiento que se podrían presentar, así:

- Los requerimientos generados por las instancias de gobierno de manera directa por intermedio de comunicación oficial de solicitud del apoyo o mediante la coordinación directa con el Director General de la Dirección Nacional de Inteligencia - DNI en el diagnóstico de un evento o incidente presentando; en lo cual la actuación del equipo técnico del CSIRT se enmarca o varía de acuerdo a la información entregada de contexto del caso presentado y la recolección de evidencia mediante entrevistas y recolección de registros, así como la documentación del caso; en este proceso se identifican como prioridades la presentación de la confidencialidad de la información y adecuado manejo del evento o incidente manejado.
- Por medio del comité nacional de seguridad digital y/o del a comunidad de seguridad digital que lo integra, podrían requerirse la evaluación y diagnóstico de alguna situación particular del ámbito del ciberespacio, que aún no es clara su catalogación; a fin de determinar cursos de acción y recomendación, lo cual, de acuerdo a su diagnóstico, determina los lineamientos a las instancias pertinentes.

Eventos de apoyo en el diagnóstico y evaluación preventiva de infraestructuras del estado

En este caso, esta actividad se realiza a nivel preventivo, básicamente en el diagnostico e identificación de brechas de seguridad, pruebas de penetración e identificación de

vulnerabilidades, con los alcances en profundización que se generen en los acuerdos de actividad y reserva.

Eventos reportados por funcionarios o personas

Para este caso, se podrían reportar eventos reportados por personas que identificaron una actividad o evento anómalo, el cual debe ser diagnosticado, valorado y clasificado, para determinar si es de pertinencia de atención del CSIRT o notificarlo a la instancia administrativa interna o externa que le compete.

Descripción de la estrategia CSIRT-INTELCO

A continuación, se definirán los elementos mínimos para la estrategia y funcionamiento del CSIRT de inteligencia Colombiano o CSIRT-INTELCO, el cual tendrá como modo de funcionamiento de una organización independiente, lo cual significa que actuará como un órgano independiente (Ministerio de Defensa de España, 2011), apoyado y financiado por el gobierno, principalmente por los órganos establecidos para realizar actividades de inteligencia. Este organismo nacería dentro de la agencia cabeza de sector de inteligencia y dependería directamente del Director General, sin embrago tendría una estructura orgánica separada a la de la agencia de inteligencia con el fin de independizar su funcionamiento y prepararla para su creación como órgano independiente a largo plazo.

Misión

Proteger la infraestructura crítica de amenazas cibernéticas, gestionando de manera proactiva y aprovechando las oportunidades con el fin de fortalecer la seguridad y protección de los fines esenciales del estado.

Visión

Ser el CSIRT articulador de la estrategia de Ciberseguridad Nacional y de las capacidades de organismos similares, siendo referente a nivel regional.

Principios y Valores

Para la definición de valores, se tendrán en cuenta los estipulados para el sector Gobierno (Función-Pública, 2017), los cuales son los que se muestran en la figura a continuación.

Figura 24. Valores de la función pública. [Infografía]. Creación propia con base en Valores del Servicio Público. Rescatado de: Función Pública.

https://www.funcionpublica.gov.co/documents/418537/24621277/2017-06-07_valores_del_servidor_publico_codigo_integridad (Función-Pública, 2017).

Adicionalmente, se proponen valores adicionales (EAE Business School, 2020), con el fin de fortalecer la cultura organizacional dentro del CSIRT, los cuales los definiremos como:

- Aprendizaje y adaptabilidad: Este principio o valor permitirá al talento humano, tener a la capacidad de ser resilientes y adaptarse a las condiciones cambiantes con un enfoque en la innovación, teniendo en cuenta la temática o razón de ser, relacionada con la ciberseguridad.
- Capacidad de análisis y autocrítica: Consecuente con los anterior, el talento humano debe estar en la capacidad de reconocer sus errores, deficiencias y opciones de mejora y aprender de los mismos, buscando generar procesos de gestión del conocimiento y mejora continua.

Funciones

- Servicios Reactivos ante los eventos que busquen realizar acciones no autorizadas.
- Ciberinteligencia Sectorial y Estatal
- Monitoreo de esquemas de servicio y plataformas de internet propias y de Gobierno.
- Monitoreo de esquemas de servicio y plataformas internas propias y de Gobierno
- Disponibilidad en monitoreo 24x7x365
- Gestión de incidentes y toma de medidas de contención y prevención
- Incorporación de nuevas tecnológicas y herramientas de seguridad informática

- Servicios proactivos como la verificación de cumplimiento de estándares de ciberseguridad y Ciberdefensa de los organismos del estado.
- Resguardar la integridad de la información y las comunicaciones de las instituciones
- Crear confianza digital para el Estado y trasladarla a la Comunidad en General
- Servicios de gestión de calidad de la seguridad de la información como actividades preventivas de protección de infraestructuras propias y externas, a nivel de mejora en configuración de infraestructura y cultura de seguridad de la información corporativa.

Objetivos estratégicos.

Siendo la misión y la visión, nuestro objetivo maestro, se definieron 4 objetivos estratégicos relacionados con el cuadro de mando integral o BSC (Kaplan & Norton, 2004), los cual nos delimita las siguientes 4 dimensiones:

Figura 25. Dimensiones del BSC del CSIRT-INTELCO. [Gráfico]. Creación propia.

Para esto, se definieron los siguientes objetivos estratégicos:

- Financiero: Lograr autosuficiencia y ahorro en gastos de funcionamiento, fundamentado en actividades de desarrollo e innovación, y apoyo de los sectores de tecnología.
- Cliente: Proveer estrategias agiles que permitan prevenir y contrarrestar amenazas cibernéticas antes de que estas ocurran.
- Procesos internos: Gestionar de manera proactiva las posibles amenazas y oportunidades, dentro y fuera de la organización, adaptando los modelos de trabajo a las condiciones cambiante del entorno.
- Crecimiento y aprendizaje: Contar con personal altamente capacitado y dotado con las herramientas para gestionar su conocimiento, tecnología e innovación.

Estrategia, organigrama y recurso humano del CSIRT-INTELCO

Para el organigrama, se basará la estructura en lo propuesto por (Albluwi, 2017) en su disertación sobre los requisitos para un CSIRT, en donde fundamenta la estructura en 4 grandes bloques, como se muestra en la figura a continuación.

Figura 26. Estructura CSIRT-INTELCO. [Gráfico]. Basado en: Framework for Performance Evaluation of Computer Security Incident Response Capabilitie. (Albluwi, 2017)

El equipo Core estaría encargado del manejo, planificación y la verificación de las actividades que se realizan en el CSIRT (Albluwi, 2017). Para esto, el talento humano debe poseer competencias tanto en la gerencia o gestión de la operación, como un alto componente técnico con el fin de comprender las implicaciones de la operación.

El equipo debe estar conformado por un equipo de soporte en temas técnicos, principalmente relacionados con:

- Redes y comunicaciones.
- Almacenamiento y procesamiento.
- Administración de aplicaciones.
- Mesa de servicio y soporte tecnológico.
- Forense.
- Desarrollo e innovación.
- Administrativo y logística.

- Bases de datos.
- Otros servicios.
- Reparación y mantenimiento.

Otro grupo importante estaría relacionado con elementos externos, con el fin de cubrir asesorías o consultorías relacionadas con temas de convenios, legales y tecnológicos, debido a que es fundamental contar con un conocimiento y punto de vista externo sobre temas legales y técnicos que son propios de terceros (Albluwi, 2017). De esta manera, el CESIRT puede concentrarse en las actividades que realmente son parte del Core del negocio.

Por último, deben existir directivas que se enfocaran en apoyar a los grupos Core y de soporte, apoyando en la definición de estrategias empresariales, talento humano, manejo financiero, adquisición, control y seguimiento de los diferentes proyectos, convenios y relacionamiento de alto nivel gerencial con el fin de facilitar la consecución de los objetivos.

Capacidades

Según, lo planteado por ISACA (Mukundhan, 2015), en el siguiente gráfico, podemos identificar el ciclo de vida en la respuesta a incidentes de una organización.

Se mencionan las siguientes fases:

- Preparación de incidentes
- Detección y Análisis
- Contención, erradicación y recuperación
- Actividades posteriores al incidente

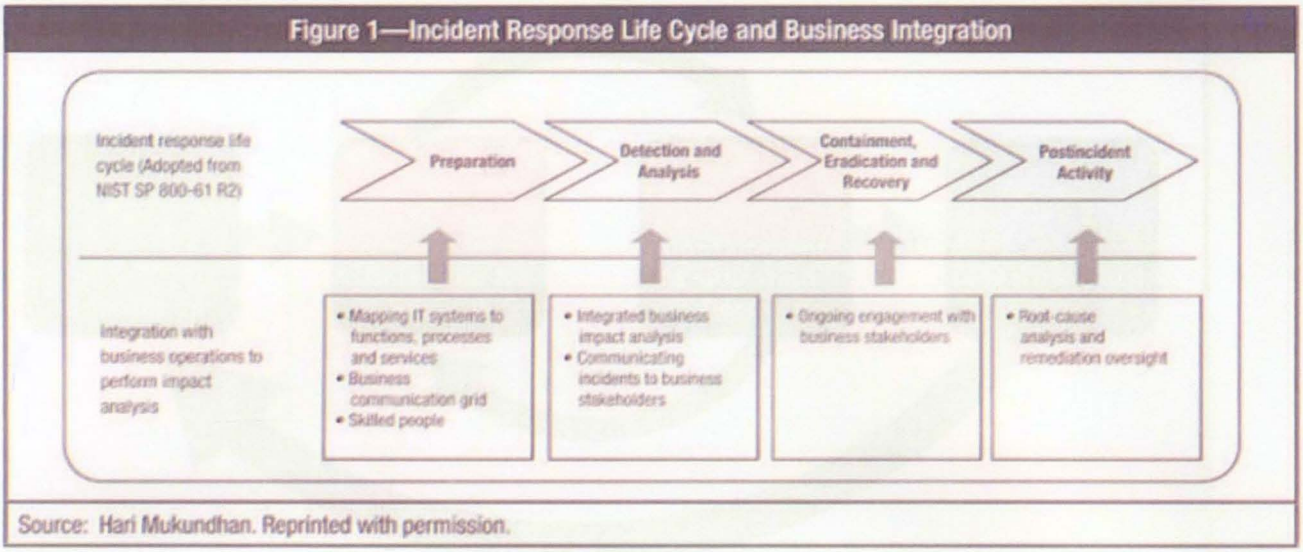

Figura 27. Ciclo de Vida de la Respuesta a Incidentes. [Gráfico]. Recuperado de: ISACA. A Business-integrated Approach to Incident Response https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/a-business-integrated-approach-to-incident-response (Mukundhan, 2015)

Este ciclo de vida se muestra en el NIST con un alcance similar, pero identificando los ciclos que deben generar reprocesos internos para lograr un flujo eficiente y eficaz al momento de la atención del incidente:

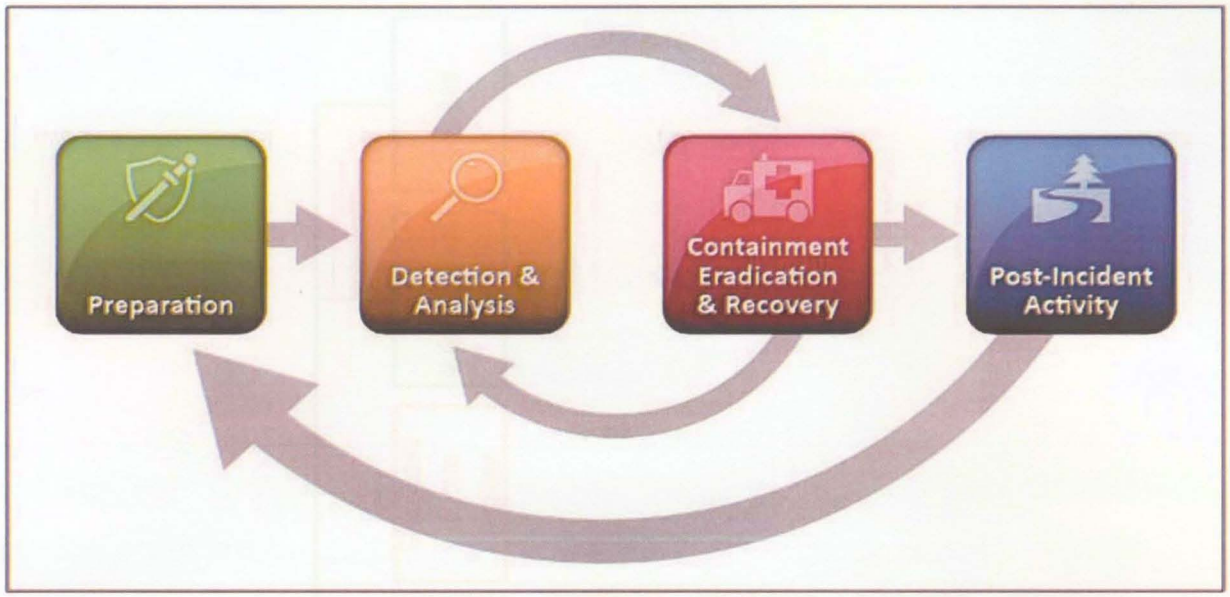

Figura 28. NIST Ciclo de Vida de la Respuesta a Incidentes. [Gráfico]. Recuperado de: Computer SecurityIncident Handling Guide (Paul Cichonsk, 2012).

Estructura organizacional propuesta.

Con base en el capítulo 2.5 del NIST *"**COMPUTER SECURITY** INCIDENT HANDLING **GUIDE**"* (Paul Cichonsk, 2012), donde se identifican organizacionalmente las siguientes instancias:

- Intrusion Detection
- Advisory Distribution
- Education and Awareness
- Información Sharing

Por lo tanto, se propone las siguientes instancias para el CSIRT de Inteligencia:

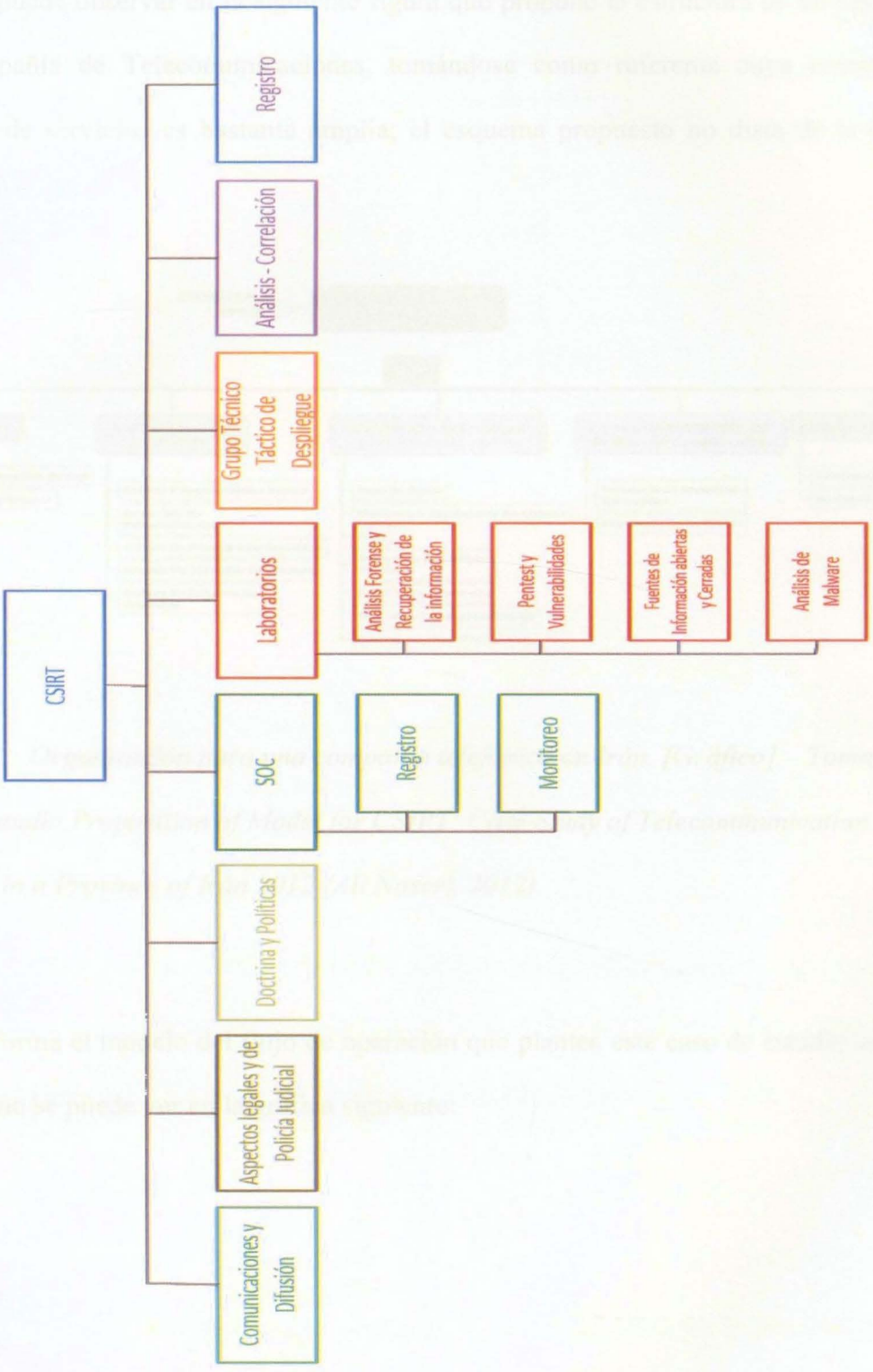

Figura 29. Organización propuesta. [Gráfico]. Creación propia.

Como se puede observar en la siguiente figura que propone la estructura de un CSIRT, para una Compañía de Telecomunicaciones, tomándose como referente cuya complejidad y cobertura de servicios es bastante amplia; el esquema propuesto no dista de la propuesta realizada

Figura 30. Organización para una compañía telefónica en Irán. [Gráfico]. Tomado del caso de estudio Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Irán 2012 (Ali Naseri, 2012).

De igual forma el modelo del flujo de operación que plantea este caso de estudio es bastante complejo, como se puede ver en la grafica siguiente:

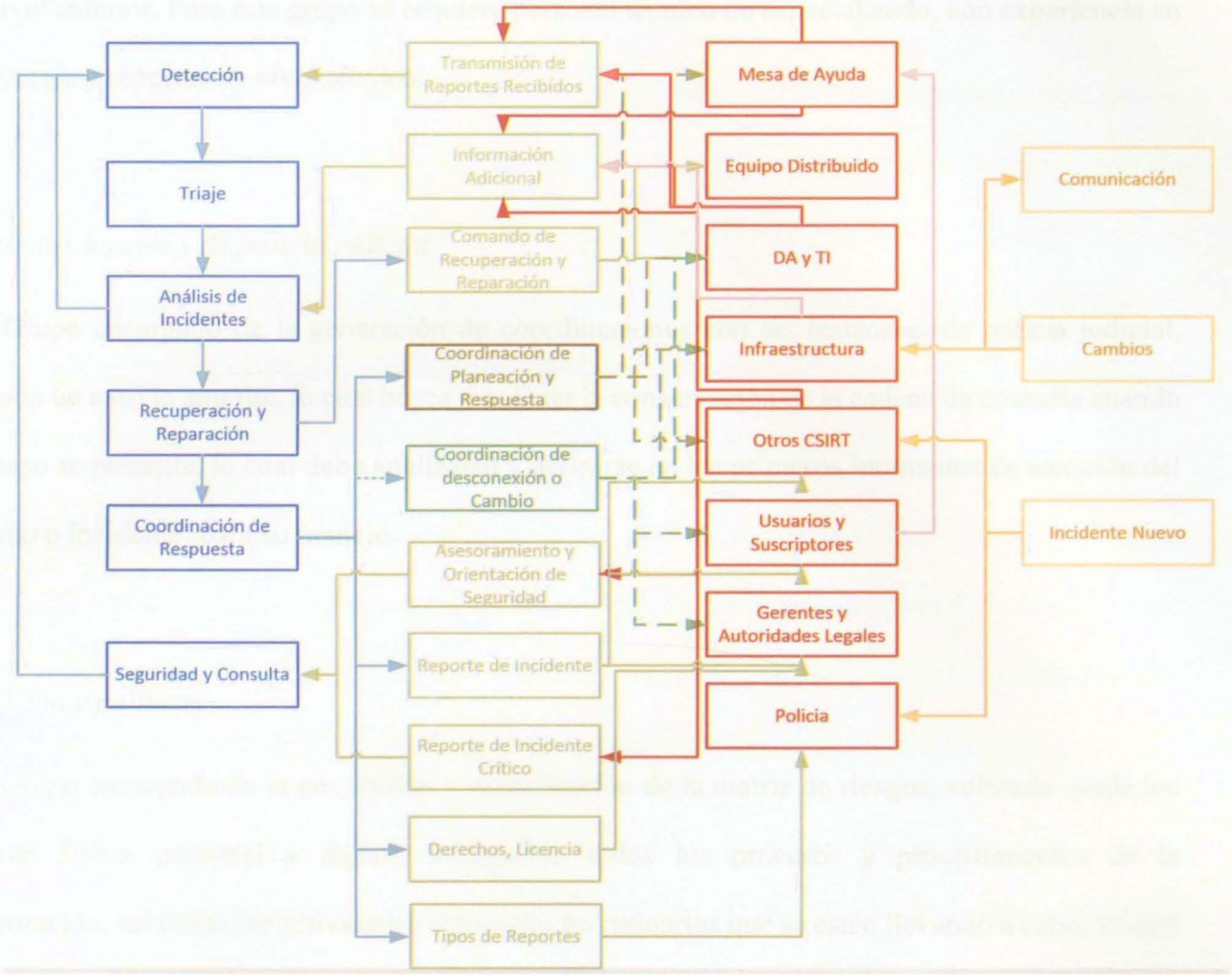

Figura 31. Modelo de flujo de actividades para una compañía telefónica en Irán. [Gráfico]. Tomado del caso de estudio Proposition of Model for CSIRT: Case Study of Telecommunication Company in a Province of Irán 2012 (Ali Naseri, 2012).

Comunicaciones y difusión

Grupo encargado de la consolidación y difusión de informes oficiales técnicos de resultados, requerimientos y coordinaciones con la comunidad y grupos de interés, avances, estado del arte de casos, en general es la instancia oficial de salida de información de resultados, alertas y difusiones

al nivel exterior. Para este grupo se requiere personal técnico no especializado, con experiencia en proyectos y reportes de nivel técnico.

Aspectos legales y de policía judicial

Grupo encargado de la generación de coordinaciones con las instancias de policía judicial, cuando un caso lo amerite, lo cual busca mantener la conservación de la cadena de custodia cuando un caso se presente, lo cual debe analizarse y definirse en los primeros momentos de atención del evento o incidente, para su manejo.

Doctrina y políticas

Grupo encargado de la generación y actualización de la matriz de riesgos, valorada desde los niveles físico, personal y digital, incluyendo todos los procesos y procedimientos de la corporación, así como las actividades especiales no rutinarias que se estén llevando a cabo; lo cual permite tener un espectro de situación actualizado; lo cual beneficia al personal del grupo del SOC, en términos de anticipación a la amenaza, conocimiento de la situación en tiempo, modo y lugar, lo cual permite una adecuada toma de decisiones.

A nivel de políticas, este grupo debe mantener actualizados los protocolos, procesos y procedimientos, los cuales deben estar alineados al core del negocio, medidos en su efectividad y eficiencia y balanceados en términos de control y producción corporativa.

SOC

Este grupo es el core del equipo de respuesta, su eficacia en términos de la integración de los activos de información y sistemas tecnológicos estratégicos, por no decir que toda la infraestructura; la eficaz inclusión de alertas basada en los Indicadores de Compromiso e Indicadores de Comportamiento; esto a nivel de usuarios, infraestructura y sistemas de información; permite la oportuna identificación de eventos o fenómenos que pueden ser objeto de identificación y análisis para su atención, de acuerdo a la situación presentada.

Registro

Esquema apoyado en la integración de eventos de todos los entornos de la corporación, buscando la inclusión y automatización de la mayor cantidad de procesos, actividades, sistemas de información corporativos; así como flujos de autorización en procesos internos.

Monitoreo

Grupo permanente de visualización de la actividad en tiempo real de la totalidad de los eventos e incidentes que se presenten, le corresponde su identificación, confirmación y reporte de eventos que pueda materializar un riesgo para la corporación.

Infraestructura

Grupo tecnológico no permanente que actúa por demanda ante una falla de los esquemas de monitoreo del CSIRT, integrado por funcionarios del CSIRT de otros grupos, el cual es el encargado de la corrección de fallas o integración de nuevos esquemas de monitoreo a las herramientas que administra el CSIRT.

Laboratorios

En este esquema, se identifican esquemas de capacidades requeridas por demanda, ante la atención de un evento o incidente, que requiere la actuación de capacidades adicionales, estas capacidades técnicas son:

Análisis forense y recuperación de información

Este proceso, se puede presentar para la conformación y/o determinación de responsabilidades de actores, que comprometieron la seguridad con medios digitales y de almacenamiento de información, es un proceso especializado, con herramientas mixtas de uso libre y licenciadas, el cual requiere de la pericia, dominio y experiencia de sus operadores para obtener óptimos resultados.

Pentest y vulnerabilidades

Esta es una actividad que en la mayoría de los casos es preventiva, basada en la identificación de vectores de riesgo y amenaza de plataformas y esquemas tecnológicos; el cual requiere de un proceso de test diagnóstico, reporte, remediación, re-test y mejoramiento continuo.

Los diagnósticos que se presentan en esta instancia de laboratorio son para el momento y puede variar su alcance y remediación con el correr del tiempo.

Fuentes de información abiertas y cerradas

Esta instancia de capacidad, debido a su evolución permanente en términos de crecimiento del espectro del internet, redes sociales y nuevas tecnologías; requiere de la búsqueda de información que permita la correlación de eventos e incidentes, que permita su identificación y cruce con situaciones que ya se esté presentando a nivel del ciberespacio.

Esta correlación e identificación se apoya con fuentes abiertas de internet y cerradas como bases de conocimiento, suscripciones de información especializada, los cuales permiten tener un alcance eficiente y eficaz, que redunda en información de alto valor para los casos atendidos por el CSIRT.

Análisis Estático y Dinámico de Artefactos Cibernéticos

Este grupo, permite el análisis de instancias de archivos ejecutables, que requieren una identificación de su comportamiento, en términos de seguridad, ejecución colateral con otros actores, que permita la identificación de indicadores de compromiso y comportamiento.

Estos artefactos pueden ser maliciosos o no, ya que pueden formar parte del proceso de pentest y vulnerabilidades para planes de remediación de artefactos no dañinos.

Grupo Técnico Táctico de despliegue

Grupo técnico no permanente, convocado por demanda, el cual actúa cuando se requiere de la atención y evaluación en sitio de una situación presentada. Este diagnóstico en sitio permite el dimensionamiento de los niveles de afectación y compromiso, de allí se disparan las actividades de contención y cierre.

Este grupo debe ser multidisciplinario, debido a que su actuar depende del tipo de evento presentado, enviando el personal especializado para su debida actuación y atención.

Análisis – Correlación

Este grupo es el encargado de analizar la información recolectada por los demás grupos acerca del caso, a fin de identificar aspectos de correlación con otros eventos o incidentes históricos como en curso, a fin de identificar actuaciones y comportamientos con otros fenómenos y situaciones; esto podar reflejar campañas masivas, o recurrentes periódicas que deben permitir su control, contención y remediación.

Registro – Base de Conocimiento

La inclusión de los eventos con una información completa y situacional, que involucre toda la información recolectada, analizada y procesada; a fin de permitir que el sistema genere las consultas, procesos e informes documentados; a fin de poder ser incluido en la base de conocimiento apara consulta posterior y para la generación de informes.

A continuación, se muestra el organigrama general de trabajo, en donde las áreas operacionales y de soporte deben ser iguales o superior al 70% del personal total. De la misma manera, s fundamental mantener una curva salarial acorde a la importancia de las actividades, en donde las áreas operacionales priman ante cualquier otra área, incluyendo la gerencia y dirección, esto debido a la especialidad en cuanto a las competencias necesarias para pertenecer al equipo Core.

Figura 32. Organigrama general CSIRT-INTELCO. [Gráfico]. Creación propia.

A continuación, se muestra la descripción de las necesidades de personal requeridas para ser contratadas en 1 año.

CARGO	CANTIDAD	SALARIOS APROXIMADO TOTALES (MES)	FUNCIONES GENERALES
GERENTES SENIOR	4	$ 56.000.000	Este personal se encargará de cargos como son CIO, CEO, CFO, Gerente de comunicaciones y demás actividades administrativas.
GERENTE DE OPERACIONES E INNOVACIÓN Y DESARROLLO	2	$ 36.000.000	Este profesional se encargará de gerenciar las operaciones Core del CSIRT.
EXPERTOS SENIOR EN TECNOLOGÍA	5	$ 60.000.000	Lideraran la operación y participaran en el desarrollo de actividades tanto de apoyo como operativas. Su función no se limitará a liderazgo.
EXPERTOS JR. EN TECNOLOGÍA	10	$ 90.000.000	Estará a cargo de las actividades técnicas, mecánicas, tanto de apoyo como operativas previamente definida por los empleados senior y directivos. Tomaran decisiones y lideraran actividades operativas.

TÉCNICOS EXPERTOS EN TECNOLOGÍA	10	$ 70.000.000	Estará a cargo de las actividades técnicas, mecánicas, tanto de apoyo como operativas previamente definida por los empleados senior y directivos.
ASISTENTES ADMINISTRATIVOS	5	$ 25.000.000	Se encargarán de la realización de tareas de carácter técnico y asistencial, relacionadas con el apoyo a las actividades administrativas y necesidades logísticas del CSIRT.

Tabla 2. Necesidades de cargos para el CSIRT-INTELCO. Creación propia.

En cuanto a los perfiles requeridos, se debe tener en cuenta que en necesario contar personal técnico en su mayoría que tengan perfiles de ingenieros de sistemas, informática, telecomunicaciones, computación, en general y en la medida que sea requerido, conocimientos y capacitaciones, relacionadas con sistemas operativos, redes en general, seguridad perimetral, Hacking, VPN, DDOS, antivirus y en general sobre plataformas de seguridad entre otras. Es fundamental que se tengan conocimientos generales en metodologías de seguridad, normas internacionales, estándares de industria y parte del equipo debe dominar lenguajes de programación de bajo nivel, así como poseer habilidades blandas que le permitan afrontar retos y mantener buenas relaciones con el equipo en general.

No se proponen perfiles muy específicos, ya que acorde a las etapas de implantación, se deberá comenzar a contratar personal el cual deberá ser capacitado frente a los procedimientos que sean emitidos para esta implementación.

Esto significa que, teniendo en cuenta temas de aportes parafiscales y demás contingencias, el valor mensual a pagar estaría alrededor de los 350 millones de pesos. Los valores propuestos se basan en el mercado actual laboral, considerando mantener un salario competitivo con el fin de

disminuir riesgos como son fuga de información, alta rotación de personal, promoviendo satisfacción económica.

Esto deberá estar a acompañado por la promoción de estrategias de desarrollo y bienestar como son:

- Planes de Capacitación.
- Becas académicas (nivel postgrado, maestría y doctorado).
- Psicología laboral.
- Planes vacacionales y de entretenimiento.
- Plan de carrera según estudios y logros laborales por puntación.

De la misma manera, se deberá crear un comité de ética, el cual permitirá generar estrategias, controles y gestionar de manera proactiva, las conductas poco éticas dentro del CSIRT.

Con el fin de lograr una estrategia organizacional interna y teniendo en cuenta las necesidades el CSIRT en temas de innovación, ecosistema externo (el cual se tratará en el capítulo siguiente), liderazgo, desarrollo, necesidades de infraestructura y otros aspectos, se tomara como estrategia articuladora o modelo, lo propuesto por Manuel Díaz Hoyos, experto en Transformación Digital, en el denominado *"árbol de resiliencia"* (Díaz, 2018), la cual integra los elementos nombrados y realiza un particular énfasis en la resiliencia y adaptabilidad, la gestión de riesgos e interacción con ecosistema externo, incluyendo socios estratégicos, competencia, temas de gobierno, normativa, entre otros.

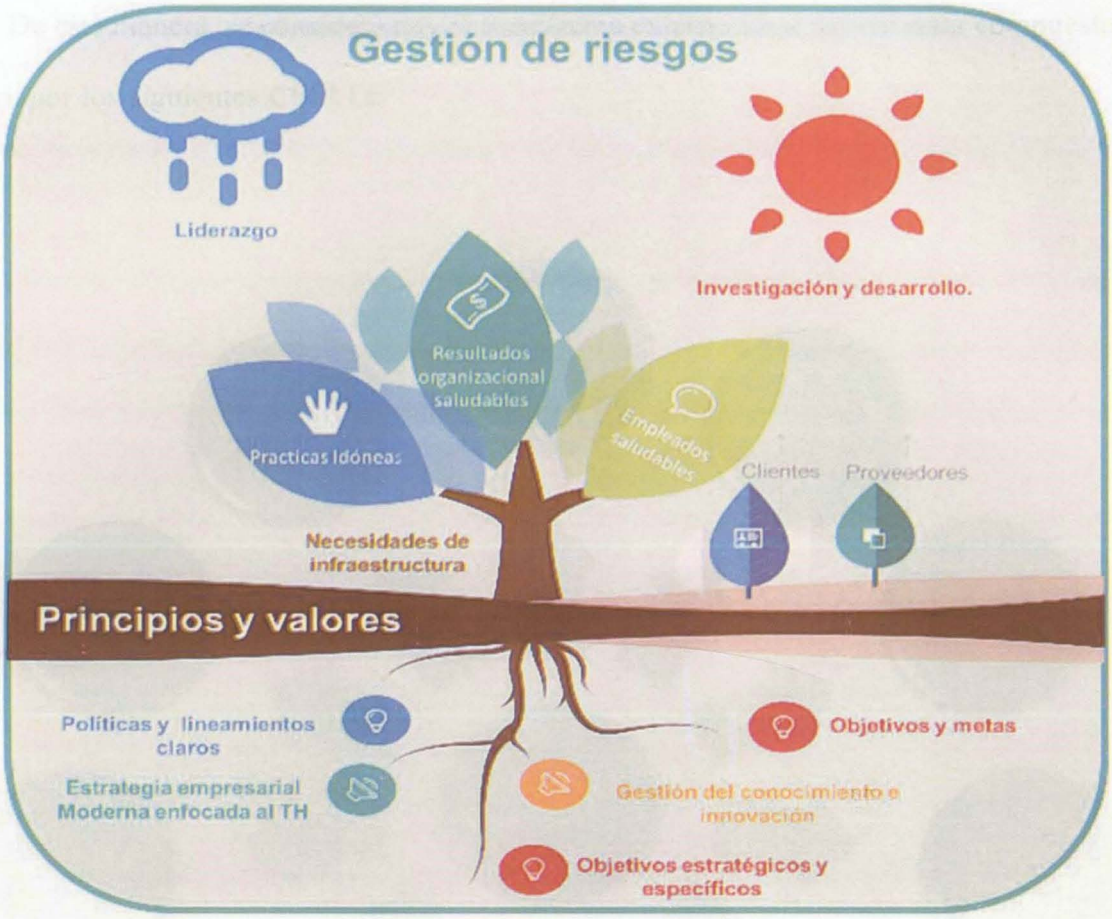

*Figura 33. Modelo de Árbol de Resiliencia. [*Gráfico*]. Tomado de: Manuel Díaz, Propuesta de un modelo proactivo de resiliencia y adaptabilidad organizacional emulando un ecosistema, para el sector de empresas de tecnología (Díaz, 2018) .*

Ecosistema externo

Arte de la tarea que debe realizar el CSIRT-INTELCO es el de promover la creación de otros CSIRT y generar un ecosistema de colaboración de información entre las diferentes infraestructuras críticas del país en donde el papel del sector de comunicaciones, tecnología y academia resulta fundamental para el éxito de la protección de la ciberseguridad del Estado.

De esta manera, se considera que el ecosistema externo ideal deberá estar compuesto como mínimo, por los siguientes CSIRTs:

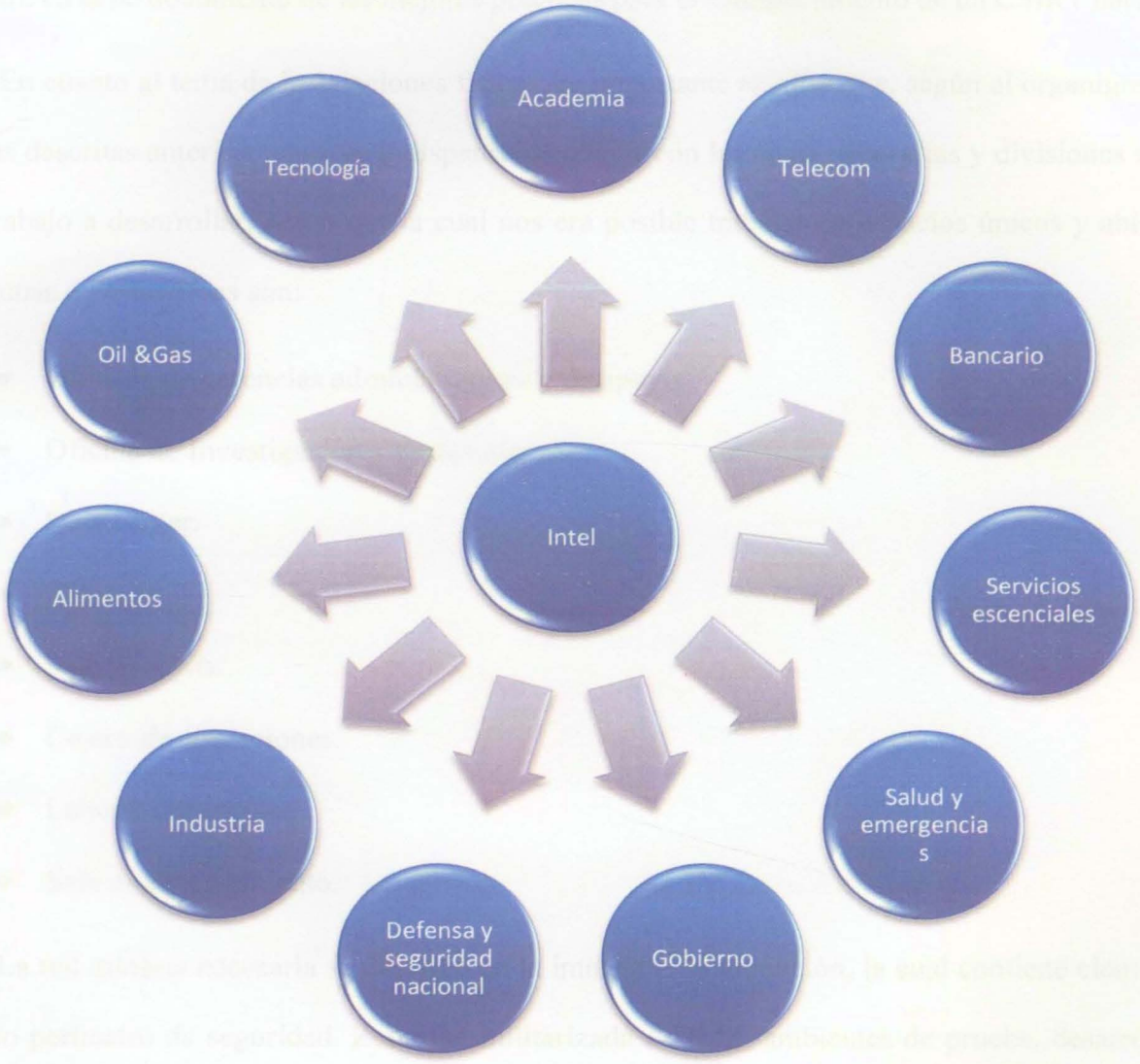

Figura 34. Ecosistema deseado. [Gráfico]. Creación propia.

Requerimientos Tecnológicos y físicos

Para los requerimientos de infraestructura TI y activos fijos, se tendrá como base lo establecido por la Organización de estados americanos (Organization of American States - OAS, 2016), en el de documento de las mejores prácticas para el establecimiento de un CSIRT nacional.

En cuanto al tema de instalaciones físicas, es importante resaltar que, según el organigrama y áreas descritas anteriormente, es indispensable contar con las áreas necesarias y divisiones según el trabajo a desarrollar, razón por la cual nos era posible trabajar en espacios únicos y abiertos. Algunas de estas áreas son:

- Oficinas de gerencias administrativas y de apoyo.
- Oficina de Investigación y desarrollo.
- Data center.
- Almacén.
- Sala de crisis.
- Centro de operaciones.
- Laboratorio técnico.
- Sala de entrenamiento.

La red mínima necesaria se describe en la imagen a continuación, la cual contiene elementos como perímetro de seguridad, Zona Desmilitarizada o DMZ, ambientes de prueba, desarrollo y producción, red expuesta a internet, entre otros.

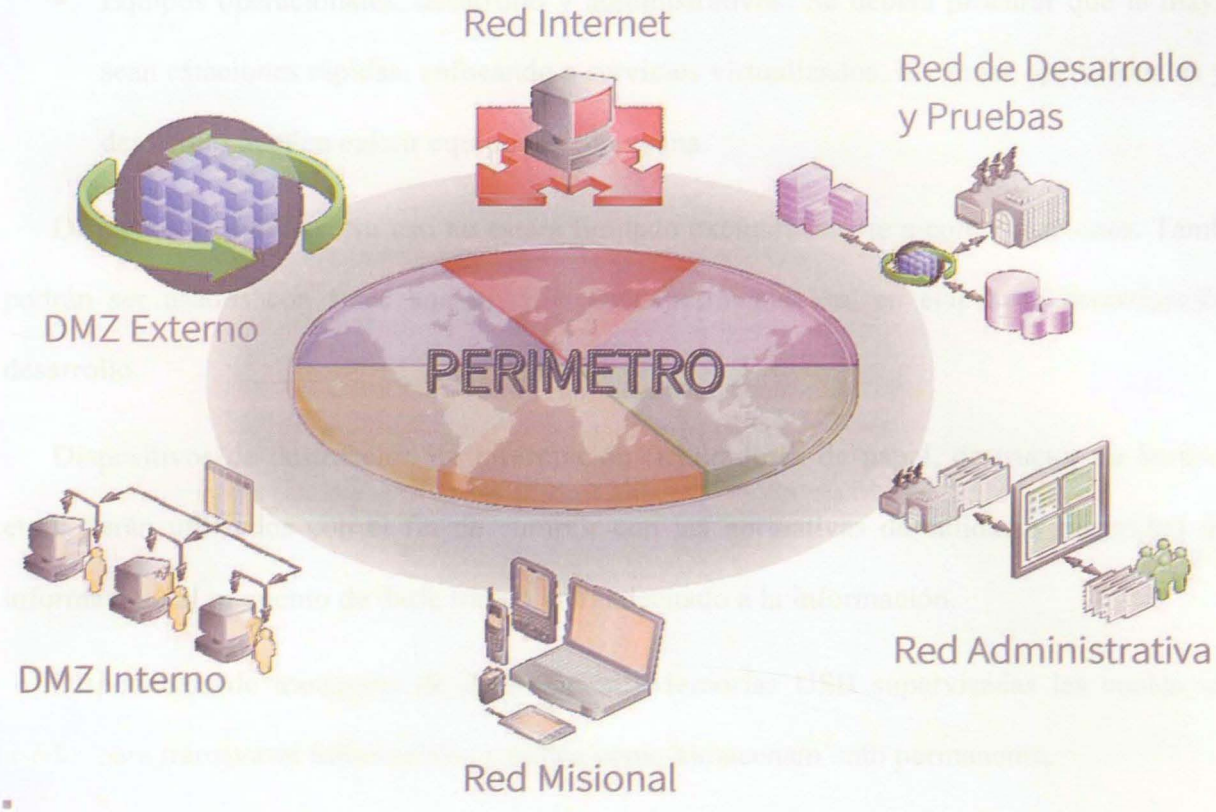

Figura 35. Ecosistema deseado. [Gráfico]. Creación propia.

Servidores y equipos de cómputo:

- Servidores para almacenamiento de información o file server.
- Servidores de virtualización de servicios y directorio activo.
- Servidores de Back-up.
- Servidores de Investigación y desarrollo.
- Servidor de monitoreo.
- Hub y correlación de eventos.
- Sistema de logs y rastreo de incidentes.

- Equipos operacionales, desarrollo y administrativos: Se deberá procurar que la mayoría sean estaciones rápidas, enfocando a servicios virtualizados. En temas operacionales y de desarrollo pueden existir equipos de alta gama.

Dispositivos móviles: Su uso no estará limitado exclusivamente a comunicaciones. También podrán ser usados con fines operativos y de experimentación, en etapas de investigación y desarrollo.

Dispositivos de destrucción de información (trituradoras de papel, destructor de hardware, etc.): Serán utilizados con el fin de cumplir con las normativas de calidad y seguridad de la información, al momento de darle tratamiento adecuado a la información.

Dispositivos de transporte de información: Memorias USB supervisadas las cuales serán usadas para transportar información, y nunca como almacenamiento permanente.

Software especializado: Software relacionado con análisis de vulnerabilidades y amenazas, inteligencia de negocios, inteligencia artificial, lenguajes de programación, automatización de procesos robóticos, entre otros.

Necesidades de estrategias, políticas, normativas y certificaciones

Con el fin de asegurar un correcto funcionamiento del CSIRT, es indispensable genera la documentación procedimental necesaria. Para esto, se definen una serie de necesidades, las cuales están descritas en el grafico a continuación:

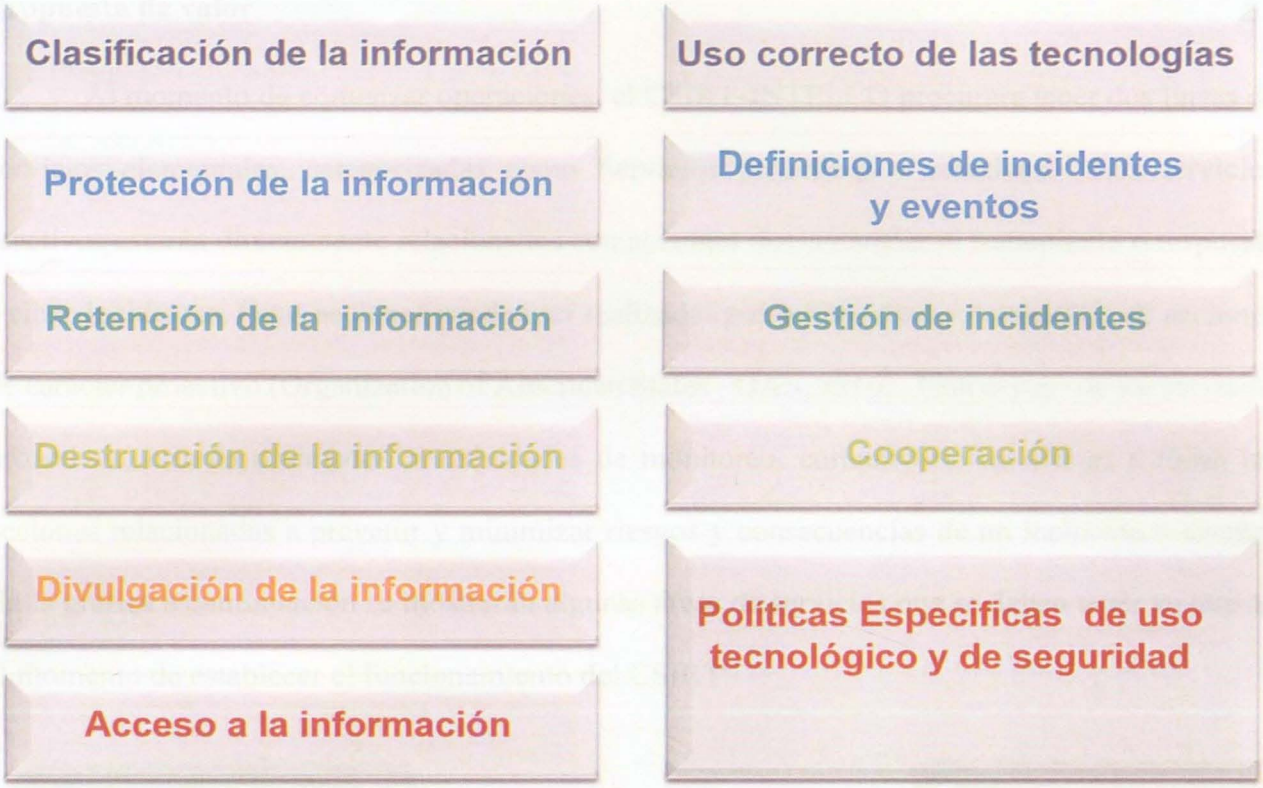

Figura 36. Políticas mínimas necesarias. Basado en (Organization of American States - OAS, 2016). [Gráfico]. Creación propia.

Adicionalmente, con el fin de mantener las mejores prácticas, se deberá buscar la certificación en normas internacionales como son:

- ISO27001: Seguridad de la información.
- ISO9001: Gestión de la calidad.
- Iso22301 y 22313: Gestión de la continuidad del negocio.

Propuesta de valor

Al momento de comenzar operaciones, el CSIRT-INTELCO procurara tener dos líneas de servicios elementales, categorizadas como Servicios proactivos y reactivos. Los servicios reactivos estarán directamente relacionados con acciones direccionadas al tratamiento o respuesta a ciber-incidentes. Estas acciones pueden ser realizadas por solicitud o a consecuencia de acciones de carácter proactivo (Organization of American States - OAS, 2016). Para el caso de los servicios proactivos, estarán orientados a actividades de monitoreo, comunicaciones alertas y todas las acciones relacionadas a prevenir y minimizar riesgos y consecuencias de un incidente o evento. En la gráfica a continuación se mostrarán algunas áreas de servicios que se deben tener en cuenta al momento de establecer el funcionamiento del CSIRT.

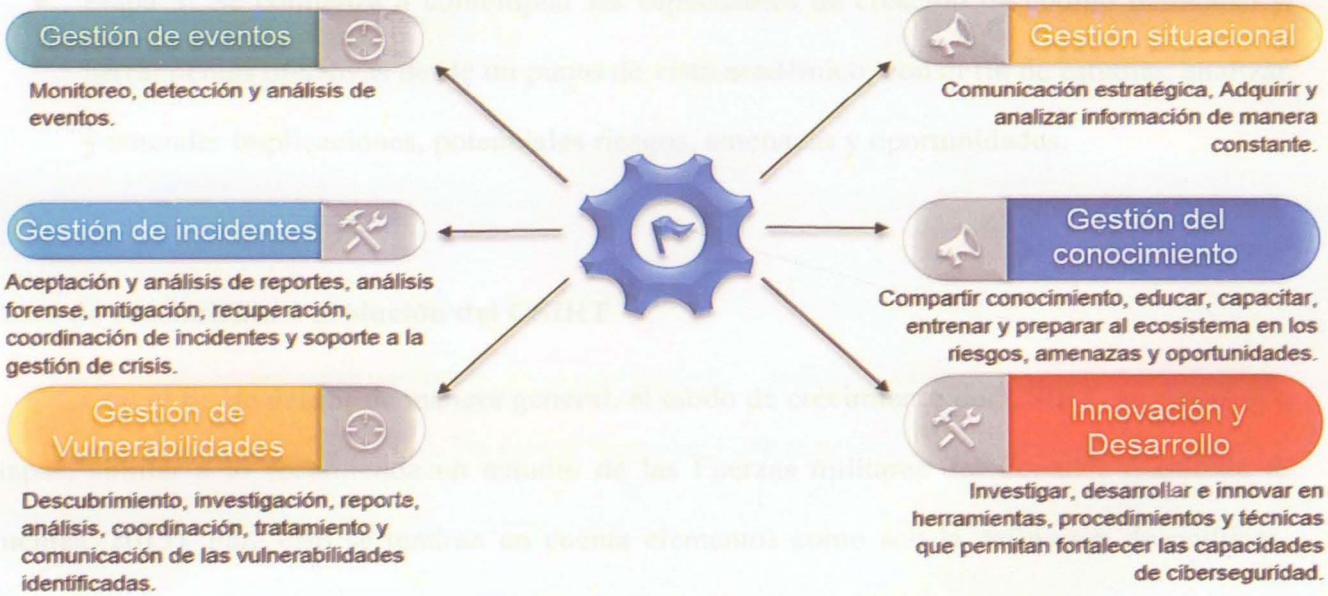

Figura 37. Políticas mínimas necesarias. Basado en (FIRST, 2020). [Gráfico]. Creación propia.

Para el caso de investigación y desarrollo, se deben crear un plan de crecimiento en las capacidades de desarrollo, enfocándolo en 3 etapas principales (Organization of American States - OAS, 2016):

- Etapa 1: Permitirá mantener un conocimiento general de los desarrollos y avances tecnológicos que se presentan en el mundo de la ciberseguridad y Ciberdefensa. Esta etapa es meramente de conocimiento y creación de conceptos e ideas que permitan plantear líneas de investigación específicas.
- Etapa 2: Se centrará en el desarrollo de capacidad de automatización de procesos, obtención y análisis en tiempo real de la información relacionada con incidentes y eventos. Implicará también investigación y desarrollo de herramientas de monitoreo y detección.
- Etapa 3: Se comienza a contemplar las capacidades de creación de código malicioso y herramientas ofensivas desde un punto de vista académico, con el fin de estudiar, analizar y entender implicaciones, potenciales riesgos, amenazas y oportunidades.

Fases de crecimiento o evolución del CSIRT

Con el fin de definir de manera general, el modo de crecimiento del CSIRT, se tomaron 6 etapas, similar a lo recomienda un estudio de las Fuerzas militares del Ecuador (Andrade & Fuentes, 2015). Para esto se tendrán en cuenta elementos como son la definición de políticas, instructivos, capacitación, crecimiento escalado de las capacidades o servicios, entre otros elementos. En la figura a continuación se muestran las diferentes etapas propuestas para la evolución del CSIRT, tal y como se muestra en la gráfica a continuación.

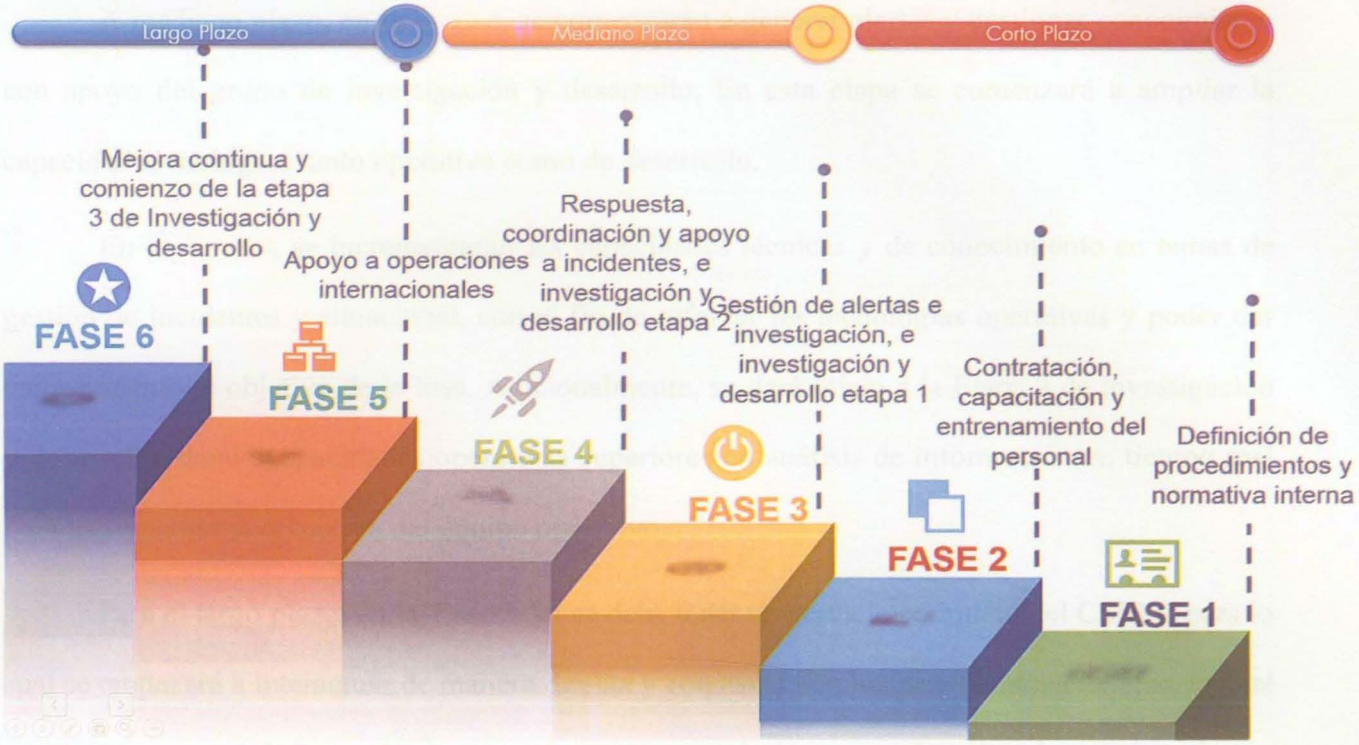

Figura 38. Fases del CSIRT. [Gráfico]. Creación propia basado en (Andrade & Fuentes, 2015).

Para el corto plazo, en la **Fase 1**, se realizará una definición de los procedimientos internos de cada área, manuales, instructivos y guías que permitan definir el modo de trabajo, asociándolo con la normativa externa e interna. En esta etapa se va a adquirir la tecnología relacionada a la red administrativa, y parte de la red operacional como son los elementos de entrenamiento y capacitación. En esta etapa se deberán tener contratados los diferentes lideres y directivos con el fin de desarrollar las actividades anteriormente citadas.

En la **Fase 2**, ya se debe realizar el proceso de contratación y capacitación del personal operativo. Una ves el personal este capacitado, apoyara en la definición de la infraestructura DMZ interno y externo, la infraestructura operativa y perimetral.

A mediano plazo, en la Fase 3, se comenzarán a generar alertas y gestionar conocimiento con apoyo del grupo de investigación y desarrollo. En esta etapa se comenzará a ampliar la capacidad tecnológica tanto operativa como de desarrollo.

En la Fase 4, se incrementarán las capacidades técnicas y de conocimiento en temas de gestión de incidentes y situacional, con el fin de reforzar las tecnologías operativas y poder dar cumplimiento al objetivo de la fase. Adicionalmente, se dará inicio a la Etapa 2 de investigación y desarrollo, dando capacidades operativas superiores en análisis de información en tiempo real para incrementar la respuesta del equipo operativo.

Para el largo plazo, en la Fase 5, ya se debe tener un servicio completo del CSIRT, para lo cual se empezará a interactuar de manera directa y constante con los pares internacionales, lo cual permitirá compartir información y generar nuevos conocimientos en el equipo de trabajo.

En la Fase 6, se realizarán procesos de mejora continua y perfeccionamiento de los elementos pertenecientes a las Fases anteriores, relacionando lo aprendido al interior del CSIRT, nacional e internacionalmente.

Matriz estratégica mínima

En la matriz estratégica a continuación, se muestran la secuencia de actividades mínimas requeridas con el fin de dar inicio a las actividades del CSIRT-INTELCO.

Objetivo	Actividad	Entregable	Tiempo de ejecución	Responsable	Apoyo
Creación y designación de directivas	Contratar cargos gerenciales	Contratos y conformación legal	1 mes	Sector Inteligencia	Gobierno Nacional
Definición de estrategia empresarial	Definición de estrategia de talento humano	Documento de estrategia	2 meses	Director CSIRT, Gerente de Talento Humano	Alta Gerencia

	Definición de estrategia financiera, administrativa y logística.	Documento de estrategia	2 meses	Gerente administrativo	Alta Gerencia
	Definición de normativa interna.	Manuales y procedimientos	6 meses	Gerente operativo y Gerente de investigación desarrollo	Alta Gerencia
Adquisición de activos físicos y humanos y terceros	Adquisición de infraestructura física	Según sea la modalidad	1 mes	Gerencia administrativa	Gerente operativo y Gerente de investigación desarrollo
	Adquisición de infraestructura tecnológica	Según sea la modalidad	2 meses	Gerencia administrativa	n/a
	Adquisición del talento humano	Contratos laborales	Constante	Gerencia de talento Humano	Gerente operativo y Gerente de investigación y desarrollo
	Capacitación de personal	Actas y certificados	Constante	Gerencia de talento Humano	CSIRT
	Contratación áreas de apoyo externo	Según sea la modalidad	Constante	Gerencia de talento Humano	Alta Gerencia
	Instalación tecnológica	Reportes de evento	Constante	Gerente operativo y Gerente de investigación y desarrollo	CSIRT
Creación y designación de directivas	Creación y firma de convenios	Convenio	Constantemente	Asesores jurídicos, Gerente General	Alta Gerencia
Objetivo	**Actividad**	**Entregable**	**Tiempo de ejecución**	**Responsable**	**Apoyo**
Operación CSIRT	Entrar a Operación CSIRT	Reportes e informes de eventos	hito	Gerente operativo y Gerente de investigación desarrollo	CSIRT

	Investigación y desarrollo Etapa 1	Reportes e informes de eventos	6 meses	Gerente operativo y Gerente de investigación desarrollo	CSIRT
	Investigación y desarrollo Etapa 2	Reportes e informes de eventos	2 años	Gerente operativo y Gerente de investigación desarrollo	CSIRT
	Investigación y desarrollo Etapa 3	Reportes e informes de eventos	5 años	Gerente operativo y Gerente de investigación y desarrollo	CSIRT
	Mejora continua	Reportes e informes de eventos	Continuamente	Alta Gerencia	CSIRT

Tabla 3. Matriz estratégica propuesta. Creación propia.

Niveles de Afectación

A nivel de la organización, o del componente del estado que se vio afectado; pueden identificarse los siguientes niveles:

- Daño Reputacional
- Compromiso de la Propiedad Intelectual o Información privilegiada corporativa - Espionaje
- Robo o Perdida de Información
- Afectación de la integridad de infraestructura
- Afectación de la integridad de la información

Los elementos de afectación corporativa a ser controlados, monitoreados e identificados se resumen en:

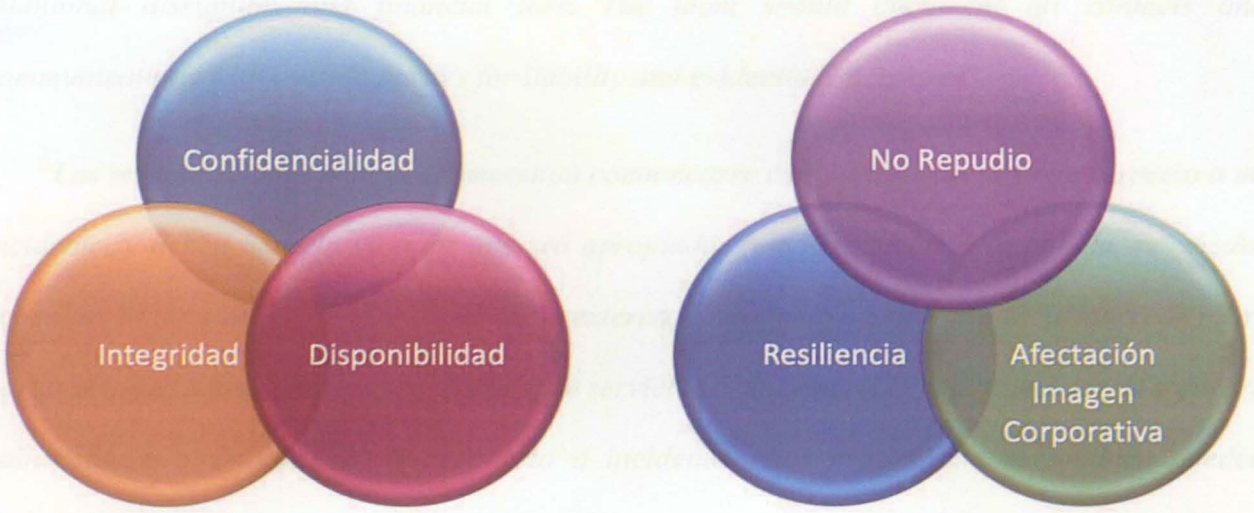

Figura 39. Elementos de afectación a ser controlados. [Gráfico]. Creación propia.

Flujo de información con otras partes interesadas.

Como lo menciona la guía del NIST (Paul Cichonsk, 2012) ***"COMPUTER SECURITY INCIDENT HANDLING GUIDE"*** **en el numeral 2.3.4** *"Organizations often need to communicate with outside parties regarding an incident, and they should do so whenever appropriate, such as contacting law enforcement, fielding media inquiries, and seeking external expertise. Another example is discussing incidents with other involved parties, such as Internet service providers (ISPs), the vendor of vulnerable software, or other incident response teams. Organizations may also proactively share relevant incident indicator information with peers to improve detection and analysis of incidents. The incident response team should discuss information sharing with the* ***organization's public affairs office, legal department, and management before an incident*** *occurs to establish policies and procedures regarding information sharing. Otherwise, sensitive information regarding incidents may be provided to unauthorized parties, potentially leading to*

additional disruption and financial loss. The team should document all contacts and communications with outside parties for liability and evidentiary purposes".

*"**Las organizaciones a menudo necesitan comunicarse con partes externas con respecto a un** incidente, y deben hacerlo siempre que sea apropiado, como contactar a la policía, responder consultas de los medios y buscar experiencia externa. Otro ejemplo es discutir incidentes con otras partes involucradas, como los proveedores de servicios de Internet (ISP), el proveedor de software vulnerable u otros equipos de respuesta a incidentes. Las organizaciones también pueden compartir de manera proactiva información relevante de indicadores de incidentes con sus pares para mejorar la detección y el análisis de incidentes. El equipo de respuesta a incidentes debe analizar el intercambio de información con la oficina de asuntos públicos, el departamento legal y la administración de la organización antes de que ocurra un incidente para establecer políticas y procedimientos con respecto al intercambio de información. De lo contrario, se puede proporcionar información confidencial sobre incidentes a partes no autorizadas, lo que puede generar interrupciones adicionales y pérdidas financieras. El equipo debe documentar todos los contactos y comunicaciones con terceros con fines de responsabilidad y evidencia".*

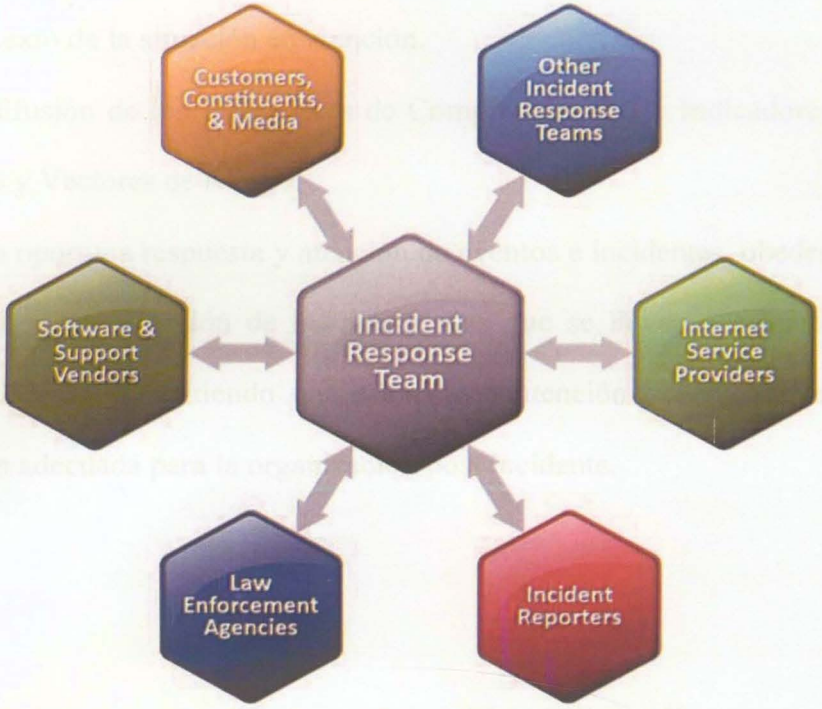

Figura 40. Entorno de información con otras partes interesadas. [Gráfico]. Recuperado de (Paul Cichonsk, 2012)

Para este caso en particular, estos flujos de comunicación se pueden direccionar hacía varias necesidades, así:

- Apoyo tecnológico y de contexto de situación del evento

  En este caso particular, pocas veces, a una entidad se le presenta un evento único que no se haya presentado en el Ciberespacio en general, o que haya sido direccionado como son **llamados "Zero Day" o ataque direccionado para la corporación afectada; por lo tanto se** pueden acudir a otros centros de respuesta para pedir si este tipo de eventos ya se tienen

referenciados o identificados; o a nivel de proveedores y aliados tecnológicos para poder tener un contexto de la situación en atención.

- A nivel de difusión de los Indicadores de Compromiso IoC e Indicadores de Actividad IoBs, Alertas y Vectores de Riesgo.

El éxito de la oportuna respuesta y atención de eventos e incidentes, obedece a la efectiva comunicación y coordinación de las actividades que se llevan a cabo entre las partes internas y externas, permitiendo una eficiente contención oportuna y la dinámica de estabilización adecuada para la organización post incidente.

CONCLUSIONES

Debido a la transformación tecnológica a la que se ha enfrentado el mundo, los riesgos y amenazas que se presentan en el ciberespacio, es indispensable la creación de un CSIRT para el sector de inteligencia, que permita apoyar al ecosistema de infraestructuras críticas con información y capacidades de respuesta proactiva y reactiva a las distintas amenazas, a nivel nacional con cubrimiento de los estamentos de Gobierno, centralizados como descentralizados, apoyando las regiones.

Es indispensable trabajar en conjunto con socios nacionales e internacionales como son los CSIRT sectoriales, extranjeros y multilaterales. Esto permitirá el intercambio y obtención de información de valor que permita realizar las estrategias correspondientes para buscar en primer lugar, la prevención más que la reacción, implementando procesos de difusión y capacitación más fuertes y con mayor cubrimiento.

Se requiere continuar con la investigación, enfocándola en la definición de fuentes de financiamiento y valoración financiera del proyecto. Esto permitirá darle viabilidad economía y comenzar el proyecto de implementación; como ya se comento se debe fortalecer esta debilidad, para evitar que la implementación y funcionamiento de estos equipos no se vea truncada, si no por el contrario permanezcan en el tiempo y se fortalezcan.

El elemento humano, su retención y capacitación, son herramientas fundamentales en la creación del CSIRT propuesto. Acompañado por la implementación de estrategias empresariales que eviten la fuga de talento y de información, teniendo en cuenta que estos funcionarios serán también agentes de inteligencia que desarrollaran actividades de recolección de información para fortalecer la prevención de eventos.

A nivel de las funciones asignadas a la Dirección Nacional de Inteligencia, tanto en el decreto de creación como en la Ley de Inteligencia, se cuentan con las facultades legales para el diseño y estructuración del CSIRT del Sector de Inteligencia, el cual básicamente busca proteger los intereses estratégicos del Estado, en un ambiente de coordinación y apoyo con los otros CSIRT compartiendo experiencias como información, que permita la adecuada implementación de procesos de prevención de anomalias.

A nivel de la comunidad de seguridad digital a nivel nacional, durante los 9 años de funcionamiento, la Dirección Nacional de Inteligencia se ha posicionado como un actor relevante y referente en el manejo de políticas de seguridad y protección de la información, que le ha permitido fortalecer la doctrina como las políticas al interior como al exterior de la entidad, replicando esta doctrina como las políticas a las entidades que así lo solicitan.

La entidad cuenta con la Certificación de ISO27001:2013, desde el 2016; en todos sus procesos misionales y administrativos, lo cual demuestra el adecuado manejo de la política de seguridad de la información, en sus manuales, procesos, procedimientos, instructivos y formatos que generan un ecosistema fuerte para la protección de la información corporativa, siendo referente de Gobierno.

La constitución del CSIRT del Sector de Inteligencia, unifica y contribuye a la Seguridad de la Información tanto a nivel interno, como en el ecosistema de seguridad digital nacional, fortaleciendo las iniciativas de las políticas de transformación digital emitidas por el Gobierno Nacional.

La formalización del CSIRT de Inteligencia, genera un ecosistema interno que fortalece la justificación para la inversión en los procesos de aseguramiento tecnológico y doctrina en

seguridad de la información, dando continuidad a los procesos internos cuya proyección se darina a nivel de normativa gubernamental.

La imagen del CSIRT del Sector de Inteligencia a nivel de las demás organizaciones del Estado se vincula como un organismo de apoyo y asesoría que los acompaña en la protección de las infraestructuras tecnológicas, estatales como privadas a nivel nacional.

REFERENCIAS

CCDCOE. (2012). *Cyber Defence Exercise Locked Shields 2012 - After Action Report.* Tallin.

CCDCOE. (2013). *Cyber Defence Exercise Locked Shields 2013 - After Action Report.* Tallin.

MINDEFENSA-ESPAÑA. (2011). *GUÍA DE CREACIÓN DE UN CERT / CSIRT .* España: Editor y Centro Criptológico Nacional.

ENISA. (16 de 04 de 2020). *Agencia Europea de Seguridad de las Redes y de la Información.* Obtenido de https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

Kaplan, R., & Norton, D. (2004). *Mapas Estratégicos.* Barcelona: HBS press.

Función-Pública. (16 de 04 de 2020). Obtenido de https://retos-directivos.eae.es/7-valores-empresariales-claves-para-cualquier-compania/

Función-Pública. (16 de 04 de 2020). *Función Pública.* Obtenido de https://www.funcionpublica.gov.co/documents/418537/24621277/2017-06-07_valores_del_servidor_publico_codigo_integridad

ALBLUWI, Q. (2017). Framework for Performance Evaluation of Computer Security Incident Response Capabilities. *UNIVERSITY OF RHODE ISLAND.*

DIAZ, M. (2018). PROPUESTA DE UN MODELO PROACTIVO DE RESILIENCIA Y ADAPTABILIDAD ORGANIZACIONAL EMULANDO UN ECOSISTEMA, PARA EL SECTOR DE EMPRESAS DE TECNOLOGÍA. *Tesis de Grado MBA*, Universidad EAN.

OAS. (2016). *Best Practices for Establishing a National CSIRT.* Washington D.C: General Secretariat of the Organization of American States.

FIRST. (23 de 04 de 2020). *FIRST-FIRST CSIRT Services Framework.* Obtenido de https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

cybintsolutions. (13 de 05 de 2020). Obtenido de https://www.cybintsolutions.com/cyber-security-facts-stats/

Contitució-Nacional-de-Colombia. (13 de 05 de 2020). Obtenido de https://www.constitucioncolombia.com/titulo-1/capitulo-0/articulo-2

threatmap.checkpoint. (13 de 05 de 2020). Obtenido de https://threatmap.checkpoint.com/

Andrade, R., & Fuentes, W. (2015). *DISEÑO Y DIMENSIONAMIENTO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT). CASO DE ESTUDIO: ESCUELA POLITÉCNICA DEL EJÉRCITO.*

wradio. (13 de 07 de 2020). Obtenido de https://www.wradio.com.co/noticias/actualidad/gobierno-firma-decreto-para-ampliar-plazo-de-liquidacion-del-das/20131101/nota/2006443.aspx

radiosantafe. (13 de 07 de 2020). Obtenido de http://www.radiosantafe.com/2016/09/30/investigan-hackeo-a-la-pagina-web-de-la-registraduria-nacional/

elespectador. (13 de 07 de 2020). Obtenido de https://www.elespectador.com/noticias/judicial/hackearon-a-la-pagina-de-la-registraduria/

bibliotecadigital. (13 de 07 de 2020). Obtenido de https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

DIRECCIÓN NACIONAL DE INTELIGENCIA - DNI. (2011). *Investigación Archivo Interno DIRECCIÓN NACIONAL DE INTELIGENCIA - DNI 2011 Plan de Acción y Seguimiento Conpes 3701 – Identificación de tareas asignadas para la vigencia del CONPES.* Bogotá: DIRECCIÓN NACIONAL DE INTELIGENCIA - DNI.

CNN. (13 de 07 de 2020). Obtenido de https://cnnespanol.cnn.com/2019/11/27/siete-dias-de-protestas-y-sigue-el-paro-nacional-en-colombia-como-llegamos-hasta-aqui/

opendemocracy. (13 de 07 de 2020). Obtenido de https://www.opendemocracy.net/es/democraciaabierta-es/movilizaci%C3%B3n-desinformaci%C3%B3n-y-p%C3%A1nico-en-colombia-es-la-hora-de-la-responsabilidad/

MINTIC. (2019). *NOV 2019.*

PONAL. (13 de 07 de 2020). Obtenido de https://cc-csirt.policia.gov.co/

Gobiernoenlinea. (13 de 07 de 2020). Obtenido de https://estrategia.gobiernoenlinea.gov.co/623/w3-article-77743.html

csirtasobancaria. (13 de 07 de 2020). Obtenido de https://www.csirtasobancaria.com/quienes-somos

isaca. (13 de 07 de 2020). Obtenido de https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/incident-response-being-prepared-for-the-worst-case-scenario

ciberpatrulla. (13 de 07 de 2020). Obtenido de https://ciberpatrulla.com/que-es-la-ciberseguridad/

isaca. (2020). *A Business-integrated Approach to Incident Response.* Obtenido de https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/a-business-integrated-approach-to-incident-response

isaca. (s.f.). *A Business-integrated Approach to Incident Response .* Obtenido de https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/a-business-integrated-approach-to-incident-response

NIST. (2012). *COMPUTER SECURITY INCIDENT HANDLING GUIDE.* Obtenido de NIST National Institute of Standards and Technology "COMPUTER SECURITY INCIDENT HANDLING GUIDE"

Digital, D. C.-P. (2016). Obtenido de Biblioteca Digital Camara de Comercio de Bogotá: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

CCN-CERT, C. C. (septiembre de 2011). *Guía Esquema Nacional de Seguridad.* Obtenido de Guia de Creación de CERT's: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-CSIRT.pdf

FIRST, Forum Incident Response and Security Teams. (2018). *Product Security Incident Response Team (PSIRT) Maturity Document.* Obtenido de FIRST - Forum Incident Response and

Security Teams: https://www.first.org/standards/frameworks/psirts/psirt_maturity_document

Dirección Nacional de Inteliegncia - DNI. (3 de Noviembre de 2018). *Decretos.* Obtenido de Decreto 4179 del 3 de Noviembre de 2011. Creación de la DIRECCIÓN NACIONAL DE INTELIGENCIA - DNI: http://www.dni.gov.co/wp-content/uploads/2018/10/Decreto-4179-del-3-de-Noviembre-de-2011.-Creaci%C3%B3n-de-la-DNI.pdf

Mayorga Delgado, A. (09 de 10 de 2014). *Lineamientos, Tendencias y Estrategias sobre Ciberseguridad y Ciberdefensa en Colombia.* Obtenido de Repositorio Institucional Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2868/Trabajo%20de%20grado1904.pdf?sequence=1&isAllowed=y

Consejo Nacional, de Política y Económica y Social. (11 de Abril de 2016). *Documento CONPES 3854 - Política de Seguridad Digital.* Obtenido de Biblioteca Digital Cámara de Comercio de Bogotá: https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y

Consejo Nacional, de Política y Económica y Social. (14 de Julio de 2011). *Documento CONPES 3701 - Lineamientos de Política para Ciberseguridad y Ciberdefensa.* Obtenido de Documentos CONPES Económicos: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Sanchez, G.-M. M. (20 de 06 de 2017). *Manuel Sanchez, Gomez-Merelo .* Obtenido de Un nuevo Código de Seguridad Global: https://seguridadpersonalyprofesional.com/2017/06/26/un-nuevo-codigo-de-seguridad-global-por-manuel-sanchez-gomez-merelo/

ISACA. (1 de Marzo de 2017). *ISACA Now Blog .* Obtenido de Incident Response – Being Prepared for the Worst-Case Scenario : https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/incident-response-being-prepared-for-the-worst-case-scenario

MINISTERIO DE DEFENSA NACIONAL. (6 de Junio de 2013). Obtenido de RESOLUCIÓN 3933 DE 2013: https://normograma.info/men/docs/pdf/resolucion_mindefensa_3933_2013.pdf

Pérez, F. C. (11 de Abril de 2020). *SeguriLatam*. Obtenido de El CAI Virtual es pionero en la prevención, sensibilización y atención de ciberincidentes: https://www.segurilatam.com/entrevistas/el-cai-virtual-es-pionero-en-la-prevencion-sensibilizacion-y-atencion-de-ciberincidentes_20200411.html

Policia Nacional. (2020). *Centro Cibernético Policial*. Obtenido de Funciones: http://www.buango.com/dijin/grupi-funciones.php

Función Pública. (5 de Junio de 2018). *Documentos*. Obtenido de Acuerdo No. 2 del 5 de junio de 2018: https://www.funcionpublica.gov.co/documents/28587410/34112007/Acuerdo+02+de+2018+Comite+de+Seguridad+Digital.pdf/13e084c8-60b9-a4cc-0fde-ea56a669a318?t=1570630459779

Cámara de Comercio de Bogotá. (Abril de 2019). *Eventos Realizados*. Obtenido de La Ciberseguridad y Ciberdefensa en Colombia y los esfuerzos interinstitucionales para afrontar las nuevas amenazas emergentes en el ciberespacio: https://web.certicamara.com/files/eventos/CiberseguridadCiberdefensaColombia.pdf

European Union Agency for Cybersecurity - ENISA. (Septiembre de 2020). Obtenido de CSIRTs by Country - Interactive Map: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

FIRST - Forum of Incident Response and Security Teams. (Septiembre de 2020). Obtenido de Members around the world: https://www.first.org/members/map

Morgus, R. &. (Noviembre de 2015). *Transatlantic Dialogues on Security and Freedom in the Digital Age*. Obtenido de National CSIRTs and Their Role in Computer Security Incident Response: http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf

Sanchez, G.-M. M. (6 de Julio de 2011). *Manuel Sanchez Gómez-Merelo* . Obtenido de Infraestructuras Críticas y Ciberseguridad: https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/

AREITIO BERTOLIN, J. (2008). *Seguridad de la Información Redes, informática y Sistema de información.* Madrid - España: Ediciones Paraninfo S.A.

Agencia Europea de Seguridad de las Redes y de la Información (ENISA). (2006). Obtenido de Producto WP2006/5.1(CERT-D1/D2): https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

Check Point Software Technologies LTD. (13 de Mayo de 2020). *Threatcloud.* Obtenido de Live Cyber Threat Map: https://threatmap.checkpoint.com/

Martínez, A. (28 de Mayo de 2014). *INCIBE-CERT.* Obtenido de OSINT / La información es poder: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder