Propuesta de estrategia para el fortalecimiento de las capacidades del grupo Colcert

Juan Bautista Lozano Castellanos

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

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

PROPUESTA DE ESTRATEGIA PARA EL FORTALECIMIENTO DE LAS CAPACIDADES DEL GRUPO COLCERT

ALUMNO: JUAN BAUTISTA LOZANO CASTELLANOS

DIRECTOR: STEVEN JONES CHALJUB

MAESTRÍA DE CIBERSEGURIDAD Y CIBERDEFENSA

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

Bogotá – Colombia

2019

Aceptación del Trabajo

Nota de Aceptación:

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Agradecimientos

A Dios todo poderoso por permitirme adelantar y culminar mis estudios de maestría y generar nuevos conocimientos para fortalecer las capacidades técnicas, humanas y de gestión en mi vida laboral; de igual forma a mi señora madre y a mi esposa por el apoyo incondicional para alcanzar este objetivo. Finalmente, a MINTIC por la oportunidad de participar en los estudios, así como a la escuela superior de guerra y a toda su planta de personal por el tiempo y confianza necesaria para sacar adelante este proyecto.

Tabla de Contenido

Índice de Ilustraciones

Índice de tablas

Resumen

Un nuevo ámbito de conocimiento e interacción se ha estado fortaleciendo en los últimos años: el Ciberespacio, cuyas bondades como su bajo costo y fácil transaccionalidad de operaciones, ha generado la necesidad de vivir en un mundo más interconectado, con la posibilidad de acceder a estos beneficios sin importar, tiempo, distancia o ubicación física, generando una dependencia cada vez más alta para las personas en el uso de esta tecnología, abriendo toda una red de cooperación, nuevos mercados y conocimiento que aporta al desarrollo personal e incluso de las naciones a las que representan. Sin embargo, la falta de implementación de buenas prácticas para el buen uso de este nuevo ambiente virtual, ha generado la aparición de nuevas amenazas para el ser humano, los procesos y la infraestructura tecnológica que soporta la información personal y de las entidades.

Estas amenazas, han generado que los Estados a nivel Mundial, y en este caso en particular Colombia, desarrollen capacidades técnicas, humanas y operativas que afronten este escenario de nuevos delitos informáticos y mitiguen los riesgos y amenazas latentes del mismo. Como consecuencia de esto, a partir del año 2011 con el CONPES 3701, se adelanta en Colombia una estrategia de Ciberdefensa y Ciberseguridad, que ha sido implementada y apropiada por diferentes organismos y entidades del orden nacional, con el fin de desarrollar acciones en materia de protección, defensa, concientización y generación de políticas para el uso del Ciberespacio. A partir de este CONPES, se estableció una estructura organizativa y se crearon lineamientos que facilitan la prevención, detección, mitigación y respuesta frente a las amenazas cibernéticas a nivel nacional , y a su vez asignaron roles y funciones para la Comisión Sectorial:

el Grupo de Respuesta a Incidentes Informáticos (colCERT), el Comando Conjunto Cibernético (CCOC) y el Centro Cibernético Policial (CCP), organismos creados para prevención, judicialización, seguridad y defensa Nacional ante amenazas y delitos cibernéticos.

Posteriormente con el CONPES 3854 de 2016 "Política Nacional De Seguridad Digital", se identificaron los principales ejes de acción bajo los cuales se busca fortalecer y consolidar la estrategia planteada desde 2011. Como parte de estos ejes de acción se dispusieron diferentes actividades para el fortalecimiento de la estrategia de ciberseguridad y ciberdefensa de la nación y en particular de los organismos creados y encargados de salvaguardarla como lo son el colCERT, el CCP, CCOC y CSIRT de la Policía. Es así, como dentro de su Plan de Acción y Seguimiento (PAS) se dispuso una tarea enfocada a "*elaborar el plan de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del Grupo colCERT, como punto focal nacional para la gestión de incidentes digitales en Colombia*", quien durante la vigencia del CONPES 3701 realizó diferentes esfuerzos por capacitar y entrenar a los diferentes organismos que apoyan la Ciberdefensa y Ciberseguridad, sin embargo, de acuerdo a lo señalado en este último CONPES: "*aún se requiere establecer una visión global y estratégica en torno a la seguridad digital, cuya ausencia se evidencia en la forma en que se interpretan los conceptos, y en el alcance de las acciones que cada entidad debe ejecutar sobre la materia y en la dispersión de los esfuerzos realizados por cada entidad en el cumplimiento de sus funciones y competencias*".

Con lo anterior en el presente documento se realiza un análisis de estrategias y buenas prácticas a nivel internacional, en lo relacionado a políticas de Ciberseguridad, estándares de

creación de CERT y CSIRT, con el fin de proponer una estrategia para el cumplimiento de esta tarea asignada en el CONPES, en el fortalecimiento de las capacidades técnicas, de gestión y de operación en Ciberdefensa y Ciberseguridad, que le permita ser el organismo central de coordinación, contacto y monitoreo para la seguridad digital de Colombia.

Abstract

A new field of knowledge and interaction has been strengthening in recent years, Cyberspace, whose benefits as an economy and easy transactional operations, has generated the need to live in a more interconnected world, with the possibility of accessing these benefits without import, time, distance or physical location, generating an increasingly higher dependence of people on the use of this technology, opening up a whole network of cooperation, new markets and knowledge that contributes to the personal development and even of the nations to which represent However, the lack of implementation of good practices for the proper use of this new virtual environment, has generated the emergence of new threats to humans, processes and technological infrastructure that supports personal information and the entities they represent.

These threats have generated that the States at the World level, and in this case in particular Colombia, develop technical, human and operational capacities that face this scenario of new computer crimes and mitigate the risks and latent threats of the same. As a consequence of this, starting in 2011 with the CONPES 3701, a Cyber Defense and Cybersecurity strategy is being developed in Colombia, which has been implemented and appropriated by different agencies and entities of the national order, in order to develop actions in the field of protection, defense, awareness and generation of policies for the use of Cyberspace. From this CONPES, an organizational structure was established, guidelines were created to facilitate the prevention, detection, mitigation and response to cyber threats at the national level, and in turn assigned roles and functions for the Sectoral Commission, the Response Group a Computer Incidents (colCERT), the Joint Cybernetic Command (CCOC) and the Police Cyber Center (CCP),

organizations created for prevention, prosecution, security and national defense against threats and cyber-crimes.

Subsequently, with the CONPES 3854 of 2016 "National Policy on Digital Security", the main lines of action were identified under which the strategy proposed since 2011 is to be strengthened and consolidated. As part of these lines of action, different activities for strengthening were set out of the cybersecurity and cyberdefense strategy of the nation and in particular of the organisms created and in charge of safeguarding it, such as the colCERT, CCP, CCOC and CSIRT of the Police. Thus, as part of its Plan of Action and Follow-up (PAS) a task focused on "preparing the plan to strengthen the operational, administrative, human, scientific, physical and technological infrastructure of the ColCERT Group, as a focal point was established. for the management of digital incidents in Colombia ", who during the validity of CONPES 3701 made different efforts to train and train the different organizations that support Cyberdefense and Cybersecurity, however, according to what was stated in the latter CONPES:" It is still necessary to establish a global and strategic vision around digital security, whose absence is evident in the way in which the concepts are interpreted, and in the scope of the actions that each entity must execute on the matter and in the dispersion of the efforts made by each entity in the fulfillment of its functions and competences ".

With the above in this document an analysis of strategies and good practices at the international level is carried out, in relation to Cybersecurity policies, creation standards of CERT and CSIRT, in order to propose a strategy for the fulfillment of this assigned task in the CONPES, in the strengthening of the technical, management and operation capacities in

Cyberdefense and Cybersecurity, which allows it to be the central coordination, contact and monitoring body for the digital security of Colombia.

Palabras Clave

CERT - Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team).

CSIRT – Equipo de respuesta ante Incidentes Informáticos.

Ciberespacio.

Cibercrimen.

Ciberdefensa.

Ciberseguridad.

Amenazas cibernéticas.

Ataques cibernéticos.

Incidentes informáticos.

Infraestructura crítica.

Delitos informáticos.

Keywords

CERT - Computer Emergency Response Team (CERT).

CSIRT - Computer Incident Response Team.

Cyberspace.

Cybercrime

Cyberdefense

Cybersecurity

Cyber threats

Cyber attacks

Computer incidents.

Critical infrastructure.

Cybercrime.

Introducción

El Ciberespacio se ha convertido en el nuevo ámbito donde se desarrollan diferentes situaciones, actividades y conflictos que hasta el siglo pasado solo se presentaban en el ámbito Físico, como lo son: programas de capacitación, el comercio, las relaciones sociales, nuevas guerras y espionaje cibernético.

Una nueva sociedad virtual converge ante la posibilidad de vivir en un mundo más interconectado y con la necesidad de minimizar tiempo y costos para el acceso a la información y el conocimiento, realizar trámites y consumir servicios, sin importar las fronteras; sin embargo, los medios y mecanismos digitales no están maduros, situación que los delincuentes y adversarios aprovechan para crear amenazas que evolucionan aceleradamente, volviéndose cada día más sofisticadas y con herramientas de mayor alcance al público, permitiendo que algunas de las situaciones o métodos de delitos o ataques del mundo físico migren al mundo digital generando consecuencias de mayor impacto.

Según Castañeda (2018) en su publicación en el periódico la Republica, en el reciente estudio realizado por el Ponemon Institute, en colaboración con Accenture, el costo financiero del Cibercrimen para las empresas a nivel mundial, aumentó en 27,4% en 2017, con respecto al costo financiero de los ciberataques en 2016, lo que se ve reflejado en que el costo mundial promedio por cada ciberataque sea de US$11 millones, donde el 72% de las infracciones son causadas por fallas humanas (Ponemon Institute, 2017); lo que ha generado que las empresas a nivel mundial hayan aumentado sus inversiones en materia de Ciberseguridad para protegerse de los diferentes ataques.

En el informe sobre Ciberseguridad 2016 del CONPES 3701, el Observatorio de Ciberseguridad en América Latina y el Caribe reportó que el Cibercrimen le cuesta al mundo aproximadamente US$ 575.000 millones anuales, lo que representa el 0,5 por ciento del Producto Interno Bruto global. En América Latina y el Caribe, este tipo de delitos cuestan alrededor de US$ 90.000 millones anuales. (García, Revista Militar Digital, 2016).

Teniendo en cuenta lo anterior y ante la incapacidad de algunos Estados de poder reaccionar eficiente y coordinadamente ante estas nuevas amenazas, se han establecido por parte de organizaciones a nivel mundial buenas prácticas en la implementación de políticas y equipos de respuesta a incidentes informáticos que ayuden a las diferentes organizaciones de todo el mundo a crear estrategias con el fin de fortalecer las capacidades de prevención, detección y reacción ante este tipo de amenazas, lo que ha permitido minimizar las vulnerabilidades de sus plataformas tecnológicas y mitigar posibles ataques cibernéticos hacia sus infraestructuras.

Colombia no ha sido ajena a estos eventos y ante el aumento acelerado de usuarios de internet que según cifras de We Are Social y Hootsuite para 2018 , paso del 54% de penetración de usuarios de internet durante 2011 a superar el 63% durante 2018 según informe de Digital In (Monterrosa, 2018), creó la necesidad a nivel del gobierno de Colombia de establecer una estructura de Ciberdefensa y Ciberseguridad nacional que contrarrestara a su vez el incremento de los incidentes y delitos contra las infraestructuras cibernéticas gubernamentales y de carácter privado, lo que dio a conocer el grado de vulnerabilidad del País ante amenazas cibernéticas, en los diferentes usos de este medio como con posibles fines terroristas, espionaje, sabotaje a infraestructuras críticas y hurto por medios electrónicos, entre otros. De esta forma, fue creado

en 2011 el CONPES 3701 "*Lineamientos de política para Ciberseguridad y Ciberdefensa*", el cual creo 4 instancias para fortalecer las capacidades de prevención, detección, monitoreo, mitigación y respuesta ante ataques cibernéticos, ellas fueron:

- La Comisión Intersectorial: encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica (hardware, software y comunicaciones), información pública y Ciberseguridad y Ciberdefensa.
- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT: Organismo coordinador a nivel nacional en aspectos de Ciberseguridad y Ciberdefensa.
- El Comando Conjunto Cibernético de las Fuerzas Militares – CCOC: Encargado de prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales.
- El Centro Cibernético Policial – CCP: Instancia encargada de la Ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos.

(Consejo Nacional de Política Económica y Social (CONPES 3701), 2011)

Estas instancias ejecutaron una serie de actividades para cumplir con las misiones particulares encomendadas en busca de contrarrestar las amenazas en contra de la seguridad y defensa nacional en el ámbito cibernético, de igual forma y con el fin de medir el avance de la estrategia se crearon en su momento unos indicadores que fueron evaluados durante el 2015, dando como resultado un 79% de cumplimiento de las actividades estipuladas en el Plan de Acción del

documento CONPES, según lo indicó Departamento Nacional de Planeación (DNP), mediante reporte con corte a junio de 2015 .

En respuesta al porcentaje de avance de la estrategia planteada en el CONPES 3701, en el año 2016 Colombia en acompañamiento con el Banco Interamericano de Desarrollo - BID, la Organización de Estados Americanos - OEA y otras instituciones de carácter privado y público, estructuraron el Documento CONPES 3854 "*Política Nacional De Seguridad Digital"* (Marzo de 2017), es documento cambio su enfoque para incluir la gestión de riesgo como elemento fundamental en la seguridad digital, a su vez, busca dar continuidad a la estrategia planteada desde 2011 al establecer nuevos lineamientos y directrices de seguridad digital que fortalezcan la investigación, la educación, la cooperación, la regulación, el desarrollo y la innovación.

Ahora bien, con relación a la instancia de Coordinación Nacional en materia de Ciberseguridad y Ciberdefensa - COLCERT, el CONPES 3854, en su sección de diagnóstico, establece que el grupo colCERT, ente coordinador en materia de Ciberseguridad y Ciberdefensa a nivel nacional "*tiene un alcance limitado en cuanto a detección y respuesta*" (Consejo Nacional de Política Económica y Social, República de Colombia, 2016) (p.34), y recomienda al Ministerio de Defensa el "*fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica de colCERT*" (p.51). De igual manera, afirma que se mantiene la necesidad de integrar los esfuerzos logrados por cada uno de los actores a nivel País, para obtener un beneficio general y fortalecer la Ciberseguridad y Ciberdefensa a nivel nación. Para solucionar lo enunciado, la política establece, dentro de su plan de acción y seguimiento - PAS, la siguiente tarea al colCERT: "*elaborar el plan de fortalecimiento de las*

capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del colCERT, como punto focal nacional para la gestión de incidentes digitales en Colombia".

Para el cumplimiento de la tarea asignada al COLCERT, se requiere diseñar, desarrollar e implementar una estrategia que consolide sus competencias operativas y de servicios, las cuales le permitan afianzar las tareas de coordinación, contacto y monitoreo para la seguridad digital en Colombia, dotándolo de la infraestructura, herramientas, mecanismos, procesos y personal necesarios y razonables, para lograr un CERT nacional, en sus distintas dimensiones en el menor tiempo posible. La satisfacción de esta necesidad se constituye en el objeto principal de esta monografía la cual busca, identificar y proponer las recomendaciones necesarias para lograr que el Equipo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, fortalezca sus capacidades de coordinación y gestión de incidentes de seguridad informática para la protección de la infraestructura crítica del Estado Colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la Seguridad y Defensa Nacional; para lo cual, se retomarán los lineamientos y prácticas de organismos internacionales que han sido estandarizadas y probadas alrededor del mundo, como lo son el Instituto Nacional de Estándares y Tecnología - NIST, la Agencia Europea de Seguridad de las Redes y de la Información – ENISA, la organización de Estados Americanos – OEA, el Foro de respuesta a incidentes y equipos de seguridad – FIRST y el Centro Criptológico Nacional de España CCN.

Esta monografía se encuentra dividida en tres secciones, inicialmente se realizará una contextualización acerca de las principales características del Ciberespacio, sus bondades,

amenazas y estadísticas del Cibercrimen a nivel internacional y nacional, adicionalmente se indica los aspectos a mejorar en la arquitectura de Ciberseguridad de Colombia y los lineamientos bajo los cuales se soportará la propuesta de la presente monografía; la segunda sección se presenta el marco de referencia donde se menciona el marco conceptual y teorías de referencia que se emplean para el Ciberespacio, así como para los organismos CERT creados a nivel mundial para afrontar las amenazas cibernéticas, de igual forma, se describe la doctrina principal que ha surgido a nivel internacional para la implementación de estos organismos y el soporte legal bajo el cual soportan sus diferentes actividades. En la última sección, se realiza una descripción de las capacidades actuales del colCERT a nivel estratégico, de servicios y las herramientas técnicas utilizadas para la prestación de sus servicios, producto de un diagnóstico basado en los lineamientos del Instituto Nacional de Estándares y Tecnología – NIST y el Centro Criptológico Nacional de España, finalmente se expone la estrategia propuesta para reducir las debilidades del CERT nacional.

De la situación planteada, se desprende el siguiente interrogante: ¿Qué estrategia debe implementar el colCERT para fortalecer las capacidades a nivel de escalamiento, coordinación, servicios y gestión de incidentes en seguridad digital nacional, que aporte a su modelo Ciberseguridad y Ciberdefensa nacional?

Objetivos

Objetivo General

Proponer las recomendaciones necesarias para lograr que el Equipo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, fortalezca sus capacidades de coordinación y gestión de incidentes de seguridad informática para la protección de la infraestructura crítica del Estado Colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la Seguridad y Defensa Nacional.

Objetivos Específicos

1. Identificar las Capacidades técnicas, de gestión y de operación actuales del colCERT involucrando las múltiples partes interesadas.
2. Realizar un diagnóstico de las capacidades en hardware, software y servicios actuales del colCERT.
3. Proponer una estrategia operacional y de prestación de servicios acorde a las mejores prácticas implementadas por CERT y organizaciones internacionales.
4. Plantear la estructura organizacional interna que debe adoptar el colCERT para el mejoramiento de los servicios prestados.

Metodología

Tipo de Investigación: Deductivo

La metodología de investigación de la presente monografía tiene un enfoque deductivo el cual relaciona tres momentos: 1) Axiomatización (1er principio) se parte de axiomas; verdades que no requieren demostración, 2) Postulación se refiere a los postulados, doctrinas asimiladas o creadas y 3) Demostración, referido al acto científico propio de los matemáticos, lógicos, filósofos.

A pesar de sus limitaciones, es de utilidad para la investigación, ofrece recursos para unir la teoría y la observación, además de que permite a los investigadores deducir a partir de la teoría los fenómenos que habrán de observarse (Dávila Newman, 2006).

Es así como partiendo del precepto estandarizado por la Universidad de Carnegie Mellon referente a que los CERT son un Equipo de Respuesta ante Emergencias Informáticas, conformado por un personal de expertos encargado de la coordinación de todas las áreas, individuos y procesos para la implementación de medidas reactivas y proactivas que permitan preparar a un País ante incidentes de seguridad de la información, se realiza un análisis de las principales prácticas internacionales y estándares, incluyendo las diferentes normas de regulación de la NIST, ENISA, OEA, entre otras que caracterizan a los CSIRT y CERTs; para posteriormente hacer un análisis comparativo del estado actual del colCERT y proponer una estrategia que permita fortalecer las capacidades operativas, logísticas y humanas del CERT Nacional.

Será deductivo, dado que se evaluará y analizará un conjunto de buenas prácticas a nivel internacional para la creación de CERT/CSIRT que faciliten la realización de un diagnóstico interno del colCERT con el fin de evidenciar las debilidades de la organización, para proponer una estrategia que permita fortalecer las capacidades técnicas, operativas y humanas del CERT nacional. Se utilizará la técnica de análisis de contenido, ya que se identificaran y estudiarán las diferentes guías y protocolos de creación de equipos de respuesta y extraer de ellos la información relevante o las características principales con relación al objetivo de estudio de la presente monografía; a su vez, se utilizará la técnica de la entrevista, en la que se busca realizar un diagnóstico de las capacidades actuales a nivel estratégico, de servicios y herramientas tecnológicas implementadas en el colCERT.

La Monografía emplea fuentes de información primaria como la entrevista para identificar el estado actual de la organización, y fuentes secundarias como libros o artículos que interpretan otros trabajos o investigaciones que ayuden a demostrar la gestión del Equipo de Respuestas CERT.

Esta aproximación metodológica desde los estándares responde a la estricta designación dada por el CONPES de "Elaborar el plan de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del colCERT, como punto focal nacional para la gestión de incidentes digitales en Colombia" (Consejo Nacional de Política Económica y Social, República de Colombia, 2016), que permita a la organización estar en las mismas condiciones de sus homólogos, buscando de esta forma "elaborar un plan para desarrollar las capacidades necesarias para implementar un esquema de gobernabilidad

participativa de múltiples partes interesadas, y definir los niveles de escalamiento para el reporte de incidentes digitales. El plan incluirá un análisis detallado de las capacidades actuales, así como insumos de revisiones externas que permitan orientar las acciones requeridas en cada uno de los frentes. Este plan, además deberá considerar aspectos de orden presupuestal, y plantear estrategias para gestionar recursos provenientes de fuentes diferentes al Gobierno nacional, como, por ejemplo, alianzas con gremios, instituciones privadas, el desarrollo de actividades mediante un portafolio de servicios que genere ingresos, entre otros" (Consejo Nacional de Política Económica y Social, República de Colombia, 2016).

Al respecto, se proponen unas actividades y objetivos como parte de la estrategia que ayude a cumplir con el "fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica de colCERT" sugerido en el CONPES 3854 de 2016; así mismo, se proponen unos niveles de maduración para la implementación de los servicios ofertados por el equipo de respuesta, un método de evaluación de la madurez y finalmente se recomienda una estructura interna que apalanque la gestión de la estrategia.

Contexto

Desde la aparición en 1988 del primer malware de la historia denominado Morris (Morris worm), el cual infectó casi 10% de las 66,000 computadoras que en aquel entonces conformaban internet (entonces ARPANET). Fue establecido como respuesta a la situación de crisis en ese mismo año por parte de la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA), el primer Equipo de Respuesta ante Emergencias Informáticas (CERT, por su sigla en inglés), concepto que luego cambia en algunos Países como los de la Unión Europea a CSIRT (Computer Security Incident Response Team/Equipo de Respuesta a Incidentes de Seguridad Informática).

Desde entonces, a nivel internacional se ha ido incrementando la necesidad de establecer estos equipos llegando alrededor de 462 inscritos en el Foro Global de Respuesta a Incidentes y Equipos de Seguridad (FIRST), que cooperan en contrarrestar las diferentes amenazas que surgen como consecuencia de la creciente explotación del Ciberespacio para el desarrollo de nuevos negocios, espacios de contacto y oferta de servicios por parte de las diferentes entidades del orden nacional hacia sus clientes finales, para lo cual han promovido la implementación de nuevos controles de seguridad que brinden una protección a los activos de información que procesan, almacenan y transportan información de las personas con el fin de brindar una confianza hacia los clientes en el mundo digital, lo que ISACA (Information Systems Audit and Control Association), denomina como Ciberseguridad.

Este concepto que nace con el fin de adoptar las medidas necesarias para brindar un Ciberespacio más seguro, que de acuerdo a lo indicado por Martin C. Libicki "está compuesto de tres capas clásicas: la física, que está formada por el hardware de todo tipo que empleamos para albergar e interactuar con la información; la semántica, constituida por esos mismos datos; y la sintáctica, que está conformada por los programas y protocolos que nos permiten gestionar estos últimos, a las cuales se les debe implementar estas medidas para salvaguardar la integridad, confidencialidad y disponibilidad de la información que viaja a través de los componentes de cada capa" (Ágreda, 2012).

La Ciberseguridad implica un nuevo modelo de seguridad a nivel global, exploratoria y que implica conocer la totalidad de los escenarios que se van a ver afectados por la existencia y la utilización del Ciberespacio. Teniendo en cuenta estas características y los diferentes fenómenos emergentes del Ciberespacio, la Ciberseguridad busca proporcionar seguridad o mitigar las amenazas y vulnerabilidades que surgen producto de este nuevo entorno; esto a través de un trabajo coordinado y sistemático en donde la cooperación internacional juega un papel fundamental en el establecimiento de políticas y estrategias que articulen capacidades normativas, técnicas, formativas y de infraestructura para la seguridad y lucha contra la delincuencia cibernética.

A nivel internacional, existe un importante desarrollo en materia de Ciberseguridad y Ciberdefensa. Al año 2013 según un estudio de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), concluyó que más de 35 Países contaban con algún tipo de estrategia o política de Ciberseguridad, de igual forma Países como Holanda, Estonia, Estados Unidos y

China han demostrado capacidades considerables a nivel técnico, humano y de procesos, que han facilitado por parte de diferentes Países a nivel internacional la evolución doctrinaria, técnica y normativa a través de diversos foros, como Naciones Unidas, OEA, Unión Europea, entre otros, tanto desde una perspectiva de seguridad internacional como de seguridad interna en cada País. (European Union Agency for Network and Information Security, (2015-2018).

De igual forma el Banco Interamericano de Desarrollo (BID, 2016) a través de un análisis de 49 indicadores de alto impacto en materia de Ciberseguridad y Ciberdefensa, demuestra que muchos Países en Latinoamérica son vulnerables a ataques cibernéticos potencialmente devastadores. Cuatro de cada cinco Países no tienen estrategias de Ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética y de igual forma, la gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos.

Ahora bien, pese a estos esfuerzos a nivel mundial por establecer políticas, controles y en general proponer buenas prácticas para que las entidades garanticen una seguridad digital, se ha presentado según el estudio del costo del Cibercrimen realizado por Ponemon Institute y Accenture para este año, un aumento del costo financiero por concepto de los ciberataques del 27.4 por ciento en 2017, con respecto al costo financiero de los ciberataques en 2016 (Carlos Castañeda, 2018). Sin embargo, este costo financiero varía según la modalidad del ciberataque pero, a nivel general, los incidentes que más impactan las entidades son originados por malware, ataques de denegación de servicios (DoS), código malicioso, fuga de información a través de empleados activos o que se han retirado de la operación, diferentes tipos de ingeniería social

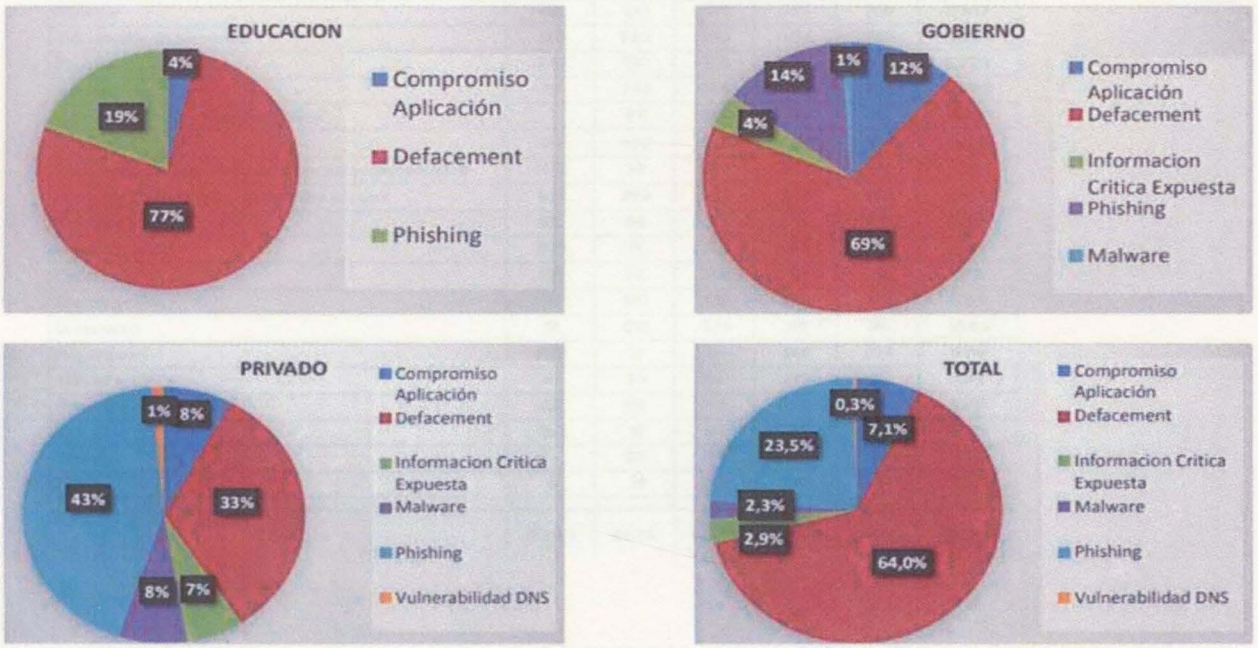
(Tailgaiting, Dumpster Diving, Baiting, Phishing, entre otros), el ransomware- o secuestro de plataformas o información, el robo físico de dispositivos electrónicos y las llamadas botnet que es una red de equipos que han sido infectados por malware para ser utilizados para ejecutar un ataque en conjunto contra un objetivo.

Así mismo, lo corrobora el estudio realizado por la empresa McAfee (2017) en el tercer informe anual sobre seguridad en la nube. Donde indica que "al ser cada día más utilizadas las tecnologías relacionadas con la nube en las empresas causan que los delincuentes informáticos estén más interesados en penetrar las redes corporativas. El 83% de las organizaciones reconoció que tuvieron al menos un incidente, siendo los más frecuentes las filtraciones de datos, que acapararon el 30%; el robo de datos de aplicaciones implementadas en la nube, que acaparó el 26%; un control incompleto sobre el acceso a los datos sensibles con un 25%; estructuras IT en la sombra que suministraban aplicaciones desde fuera del campo visible de la estructura legítima de la empresa, que acapararon un 23%; y otro 23% que reconoció la falta de profesionales especializados en la gestión de la seguridad de las aplicaciones en la nube. A todo esto, se suma que alrededor del 20% de las empresas ha recibido un ataque avanzado contra sus infraestructuras cloud" (Mcafee, 2017).

En lo concerniente a los ataques cibernéticos que se han presentado en Colombia, Equipo de Respuesta a Incidentes Informáticos colCERT, desde sus inicios a la actualidad ha atendido alrededor de 50000 incidentes reportados a través de sus canales de contacto página web http://www.colcert.gov.co, correos electrónicos contacto@colcert.gov.co y malware@colcert.gov.co y su línea telefónica desde las diferentes fuentes de información y ha

participado de varias mesas de trabajo a nivel sector defensa y empresarial con el fin de prestar asesoría en materia de Ciberseguridad. Dentro de las estadísticas de incidentes atendidos por tipo de sector para 2017 se encuentran:

Ilustración 1 Estadísticas de incidentes atendidos por el colCERT 2017.



Nota. Recuperado de: "Estadísticas, panorama 2017", Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, (23 de noviembre, 2017). Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf)

Por otra parte, el Centro Cibernético de la Policía, a su vez tiene referenciada la siguiente estadística de delitos informáticos denunciados, lo cuales según los resultados se puede observar que para el 90% de los delitos por cada modalidad durante el periodo comprendido entre 2014 al 2018, han tenido un incremento durante cada vigencia (Policía Nacional, 2018).

Ilustración 2. Estadísticas de delitos cibernéticos en Colombia durante el último cuatrienio

POLICÍA NACIONAL
Dirección de Investigación Criminal e INTERPOL
24 de julio. de 2018

CENTRO CIBERNÉTICO POLICIAL

Estadística de incidentes informáticos
SEGURIDAD DIGITAL

Modalidad	2014	2015	2016	2017	2018	TOTAL
Estafa - compra/venta de productos/servicios en Internet	1239	935	912	1273	886	5305
Malware	62	261	771	735	1118	2947
Suplantación de Identidad	140	532	783	1164	768	3447
Phishing	240	502	725	849	611	2927
Vishing	87	293	503	617	593	2093
Amenazas a través de redes sociales	1	211	300	390	310	1212
Smishing	187	408	365	292	330	1582
Publicación de imágenes/videos con pornografía infantil	N/R	78	259	212	172	721
Injuria y/o Calumnia a través de redes sociales	331	282	222	372	439	1646
Sextorsión	152	90	251	375	215	1083
Ingeniería social	N/R	75	169	162	187	593
Cyberbullying	216	44	162	314	117	853
Carta nigeriana	171	139	130	184	120	744
Defacement	31	312	620	32	69	1064
Ransomware	N/R	14	84	446	284	828
Skimming	47	50	84	175	51	407
Grooming	26	44	69	281	80	500
Spoofing	N/R	10	64	86	71	231
Turinet	16	33	38	111	43	247
DDOS	3	71	19	20	7	120
Total	2949	4516	6530	8090	6471	28556

Nota. Estadística proporcionada por el Centro Cibernético Policial, a través de su correo caivirtual@correo.policia.gov.co

Por otro lado, y teniendo en cuenta estas tendencias del Cibercrimen a nivel mundial, desde 2011 Colombia ha adoptado buenas prácticas a través de la generación de políticas de gobierno y la creación de una estructura organizacional para prevenir y contrarrestar ataques cibernéticos, iniciando con la creación de 4 organismos a nivel estatal como lo fueron: la Comisión Intersectorial dependiente de la Presidencia de la Republica, la cual dicta lineamientos al Grupo de Respuesta a Emergencias Cibernéticas de Colombia ministerio de Defensa Nacional, el Comando Conjunto Cibernético en el Comando General de las Fuerzas Militares encargados de

ejecutar las acciones necesarias para la Ciberdefensa de Colombia y el Centro Cibernético Policial a cargo de la Policía Nacional, encargado de la investigación y judicialización de los delitos cibernéticos (Consejo Nacional de Política Económica y Social (Consejo Nacional de Política Económica y Social (CONPES 3701), 2011).

Sin embargo, con el fin de evaluar la efectividad de las actividades realizadas por cada una de estas instancias, para el año 2014, el Estado colombiano a través de la creación de una "Misión Nacional de Asistencia Técnica en Seguridad Cibernética" y el Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo perteneciente a la Secretaria de Seguridad Multidimensional de la OEA, realizó un estudio del grado de cumplimiento de los objetivos planteados en el CONPES 3701 y como resultado de este ejercicio resultaron diferentes recomendaciones y actividades a ejecutar entre las que se encuentra:

"Solicitar al Ministerio de Defensa Nacional:

a. Con apoyo del coordinador nacional de seguridad digital, elaborar y ejecutar los planes de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del colCERT, del CCP y del CCOC, (diciembre de 2019).
b. Realizar la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales (a partir de enero de 2017)." (Consejo Nacional de Política Económica y Social, 2016)

De esta forma, se estructuro dentro de la misma Política Nacional un Plan de Acción que dentro de sus actividades contempla aquellas enfocadas a mejorar estas falencias identificadas para el colCERT, proponiendo acciones de mejora que a la fecha no han sido desarrolladas en su totalidad por parte de los miembros de la organización, pero aun, el colCERT adolece de una perdida de enfoque que lo desnaturaliza según su concepción en el CONPES 3701 de 2011. Para solucionar esto es necesario adelantar un documento que guie la transformación del colCERT hacia su rol natural de coordinador de las capacidades cibernéticas de la nación.

Esta necesidad identificada en el CONPES 3854 de 2016, constituye la identificación del problema a solucionar a través de la ruta de trabajo en la presente monografía que busca proponer la estrategia que ayude al fortalecimiento de las capacidades del colCERT, para lo cual se analizarán las diferentes metodologías aprobadas a nivel mundial en el establecimiento de los Equipos de Respuesta a Incidentes Informáticos, como lo son:

1. Instituto Nacional de Estándares y Tecnología - NIST,
2. la Agencia Europea de Seguridad de las Redes y de la Información - ENISA
3. la organización de Estados Americanos – OEA
4. Foro de respuesta a incidentes y equipos de seguridad – FIRST

Estas buenas prácticas ayudaran a determinar el tipo de servicios que debería prestar el CERT e identificar que capacidades operativas, técnicas y de gestión de incidentes, de tal forma que a través de ellas podamos proponer la infraestructura, hardware, software, talento humano, procesos y procedimientos a implementar.

Marcos de Referencia

En esta sección y de acuerdo con el momento número uno (Axiomatización) de metodología planteada inicialmente, se abordará los conceptos básicos que identifican el Ciberespacio, sus características, sus propiedades, tipos de ataques y atacantes, características y nuevos conceptos que nacieron a raíz de este nuevo ámbito de interacción social. Posteriormente y alineado con el momento dos (Postulación) se referencian las teorías, guías y procedimientos que se tuvieron en cuenta para proponer la estrategia de fortalecimiento del CERT, indicando a su vez las buenas prácticas que se proponen, como base de esta teoría que permitirán proponer unos niveles de implementación de los servicios y el marco legal a nivel internacional y nacional bajo los cuales deben operar los mismos. Finalmente, con el propósito de evidenciar los puntos a fortalecer en el CERT nacional, se realizará un diagnóstico del grupo de Respuesta a Incidentes bajo el método de investigación inductivo y la técnica de entrevista, la cual será aplicada al actual coordinador del colCERT quien cuenta con la experticia e idoneidad necesaria para realizar el levantamiento de información requerido y estructurar la estrategia a proponer.

Marco Conceptual y teorías de referencia

Existe un nuevo campo de desarrollo social, económico, cultural y de guerra, llamado el Ciberespacio, del cual se ha identificado que cuanto mayor es su nivel de desarrollo, mayor dependencia a nivel social se tiene de los sistemas de información y de las comunicaciones que lo componen, por consiguiente, cualquier amenaza que pueda llevar a su indisponibilidad, impactara directamente sobre el normal desarrollo de las operaciones de las organizaciones o la

cotidianidad de las personas. De acuerdo con lo anterior, Adrianna Llongueras Vicente (2013) realiza una evaluación sobre lo que el Ciberespacio representa para la seguridad nacional de un Estado, indicando:

El Ciberespacio es un elemento de poder dentro la seguridad nacional, es a través de este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI; en este mundo virtual hasta los actores más modestos pueden ser una amenaza para las grandes potencias forjándose y desarrollándose el concepto de las operaciones militares centradas en redes (Vicente, 2011).

Esta afirmación evidencia, en el poder que a través del Ciberespacio cualquier Estado puede ejercer o demostrar hacia otro durante el ejercicio de una guerra convencional, explotando las vulnerabilidades del oponente con el fin de lograr comprometer sus infraestructuras o simplemente exponiendo información sensible (Vargas, 2014).

A su vez, con el crecimiento descontrolado de Internet en la actual era del conocimiento, la proliferación de redes corporativas internas y externas, entre otros; conforman el escenario ideal para que personas inescrupulosas ejecuten acciones que impactan la integridad, confidencialidad o disponibilidad de la información y servicios en el llamado Ciberespacio, el cual, se ha convertido en un entorno virtual donde convergen y se interconecta un conjunto de medios y procedimientos, que basados en Tecnologías de la Información y comunicación proporcionan servicios desde y hacia cualquier ubicación geográfica, en donde los usuarios intercambian información en tiempo real con menos recursos y sin necesidad de desplazamientos físicos. Entre las características del Ciberespacio están las siguientes (Arreola, 2016):

- Anonimato: Teniendo en cuenta que no se requiere de interacción física y esto facilita la creación de perfiles o identidades a la medida o falsas para el usuario final.
- Trascendencia de los límites físicos entre las naciones: La interacción entre las personas y el consumo de los servicios puede desarrollarse sin límites geográficos.
- Información al alcance de todos: La información está disponible en un ambiente compartido, en donde puede ser consultada cuando y donde se requiera, por lo cual se logra generar una construcción colectiva de conocimiento.
- Flexibilidad de acceso a los servicios: La conexión con los servicios alojados en este entorno está disponible 7x24x365 días.

Por otra parte, de acuerdo con el Instituto Español de Estudios Estratégicos, "el Ciberespacio constituye un escenario táctico, estratégico y operativo, diferente de los espacios terrestre, marítimo, aéreo y exterior, que ha sido calificado en la doctrina, como uno de los Global Commons (Carrillo, 2015). Desde esa categorización, el discurso ha progresado y se ha perfeccionado como muestra la construcción teórica realizada por Gómez de Ágreda. A partir de esa propuesta inicial, el autor avanza en la comprensión de la naturaleza de Ciberespacio cuestionando doblemente el recurso a aquella categoría: en un primer momento, constata las características singulares del Ciberespacio respecto de los otros Global Commons para marcar sus diferencias; y, después, procede a identificar la «esencia» del Ciberespacio como el elemento verdaderamente distintivo. Como advierte certeramente Gómez de Ágreda, "su esencia se encuentra en el modo en que altera las realidades de los otros dominios, su capacidad para interactuar con las otras realidades y modificar la percepción de estas y su naturaleza como aglutinante catalizador que provoca alteraciones en los demás entornos y en la comprensión de

estos. Esa naturaleza singular del Ciberespacio desborda la idea de Global commons y este concepto, a su vez, se muestra incapaz de aprehender esa naturaleza singular." (Instituto Español de Estudios Estratégicos (IEEE), Carrillo, 2015)

Adrianna Llongueras Vicente realiza una clasificación de los ataques que pueden llegarse a presentar en la red, catalogándolos como ataques de alta y baja intensidad. El ataque de alta intensidad lo define como aquel que tiene como objetivo herramientas o procesos militares o infraestructuras críticas y adicionalmente al ejecutarse este tipo de ataque va a generar una acción bélica departe del Estado objetivo. El ataque de baja intensidad es aquel que se presenta más frecuentemente y va enfocado a ataques de denegación de servicio DoS, ataques a información bancaria, ataque de desfiguración de sitios web (defacement), ataque de DNS, correos basura (spam), robo o suplantación de identidad y robo de dinero por medios electrónicos (Llongueras, 2011).

De igual forma María José Caro Bejarano en su artículo alcance y ámbito de la seguridad nacional en el Ciberespacio (Bejarano, 2010), clasifica los tipos de atacantes que se encuentran en el Ciberespacio:

- Atacantes patrocinados por Estados
- Servicios de Inteligencia y Contrainteligencia
- Terrorismo, extremismo político e ideológico
- Ataques de delincuencia organizada
- Ataques de perfil bajo

Aunado a lo anterior y teniendo en cuenta que el Ciberespacio ha sido llamado el quinto dominio de la guerra sumándose a las ya existentes tierras, mar, aire y el espacio; se han creado nuevos conceptos como lo son:

-Ciberguerra que, de acuerdo con la descripción de Gaitán Andres, es la utilización de todas las herramientas electrónicas e informáticas para derrumbar los sistemas electrónicos y de comunicación del enemigo y mantener operativos los propios. (Gaitán, 2012)

-Ciberseguridad que consiste en la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados (Fojón & Sanz, 2010).

-Crimen Cibernético es el acto criminal cometido mediante la utilización de computadoras como herramientas principales para cometer el delito. Suele también generalizarse que existe crimen cibernético si computadores han sido objeto, sujeto o instrumento del ilícito. (Uzal, 2012)

-Cibernético o Ciberterrorismo puede ser resumida como Crimen Cibernético pero realizado por motivaciones religiosas, sociales o políticas. (Uzal, 2012)

-Ciberdefensa: la seguridad de esa información que camina involucrada en este Ciberespacio aplicada a la Defesa Nacional. Tiene la principal finalidad de planear, coordinar, integrar, sincronizar, conducir y ejecutar actividades relacionadas a la protección de las redes de computadores del área de Defesa, como también, aquellas acciones cibernéticas provenientes de otras naciones que comprometan las estructuras

críticas del País y sus servicios esenciales. (La estrategia de Argentina y Brasil para la DefensaCibernética, un análisis por los niveles de la conducción, 2015).

Teniendo en cuenta todas estas tendencias, los Estados a nivel mundial han adoptado estrategias entre las que se encuentran la creación de Equipos de Emergencias a Incidentes informáticos – CERT o equipos de respuesta a incidentes de seguridad informática CSIRT, los primeros liderados por EEUU a través de CERT Coordination Center (CERT/CC) y los segundos son aquellos comúnmente manejados por la Unión Europea.

"Estos equipos son los responsables de implementar medidas preventivas y reactivas ante incidencias de seguridad, así como la gestión de respuesta a incidentes en caso de la ocurrencia de catástrofes naturales o desastres provocados por el hombre que afectan los servicios e infraestructuras de información críticas a través de la explotación de vulnerabilidades cibernéticas" (Muñoz, 2015).

En la actualidad, se encuentran inscritos en el Foro de Respuesta a Incidentes y Equipos de Seguridad FIRST, cuatrocientos veintinueve (429) equipo CSIRT nacionales en todo el mundo, sin embargo, dependiendo de la región se utilizan diferentes nombramientos y abreviaturas de los equipos de respuesta ante incidentes informáticos, nombrándose de la siguiente forma:

- CERT o CERT/CC (Computer Emergency Response Team): Abreviatura utilizada en Estados Unidos.
- CSIRT (Computer Security Incident Response Team): Abreviatura utilizada en Europa.

- CIRT (Computer Incident Response Team): Abreviatura utilizada en Países como Australia, Alemania, Japón, Noruega y Estados Unidos.
- SERT (Security Emergency Response Team): Abreviatura utilizada en África.
- IRT (Incident Response Team): Abreviatura utilizada en equipos pequeños que se encuentran dentro de una organización.

De igual forma, tal y como lo menciona la Organización de Estados Americanos tipos en su documento "Buenas prácticas para establecer un CSIRT Nacional", suelen clasificarse en los siguientes tipos:

- CSIRT Académicos
- CSIRT Comerciales
- CSIRT de infraestructuras críticas
- CSIRT Gubernamentales
- CSIRT Nacionales
- CSIRT del Sector Militar
- CSIRT de proveedores
- CSIRT del sector de pequeñas y medianas empresas (PYME)

Cada uno con funciones diferentes de acuerdo a la estructura política, cultura, marco jurídico y capacidad financiera de cada País, y están integrados por una mezcla de expertos en seguridad de Tl y profesionales de distintas especialidades y sectores económicos. Adicionalmente con esta clasificación se tiene un campo de acción especifico que facilita la especialización de competencias técnicas específicas para responder a incidentes cibernéticos de nivel nacional, las

cuales aportan a las capacidades de un Estado para identificar, prevenir, mitigar y combatir las amenazas cibernéticas.

Alineado a lo anterior, a continuación se mencionan los lineamientos establecidos, probados y apropiados por diferentes organismos a nivel mundial como buenas prácticas, los cuales permiten la definición de estrategias y políticas a la hora de crear un CERT y para el presente caso de estudio aquellas que debe tener uno nacional; éstas se constituyen, junto con el direccionamiento del gobierno colombiano, en la base para el fortalecimiento del colCERT el cual es el objetivo de la presente monografía.

Tabla 1
Lineamientos para establecimiento de un CERT

Título de la Fuente	Tipología de la fuente (web, RSS, base de datos, ferias, etc.)	Descripción general	¿Cómo aporta la fuente a mi proyecto?
Organización de los Estados Americanos (OEA) - Buenas prácticas para establecer un CSIRT NACIONAL	Web	Analiza el proceso de gestión de un proyecto para la creación y la puesta en marcha de un CSIRT nacional, incluidos distintos criterios y consideraciones necesarias para definir su constitución, misión, visión, alcance, servicios, tiempos, y aspectos legales e institucionales u organizacionales. Esto incluye un examen de los requerimientos de recursos humanos, tanto en términos de contratación como de	El documento presenta una propuesta para la creación de un CSIRT a partir de los marcos existentes de la marcos y metodologías existentes de CSIRT, como aquellos desarrollados por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y GÉANT. También se

Título de la Fuente	Tipología de la fuente (web, RSS, base de datos, ferias, etc.)	Descripción general	¿Cómo aporta la fuente a mi proyecto?
		formación continua, que son necesarios para establecer el personal de un equipo nacional de respuesta a incidentes. Asimismo, la guía presenta descripciones detalladas de infraestructura, que incluye hardware, software y procedimientos técnicos.	analizan directrices para la adhesión y la participación en determinados organismos internacionales, como el Foro de Equipos de Respuesta a Incidentes y de Seguridad (FIRST).
Centro Criptológico Nacional España - GUÍA DE CREACIÓN DE UN CERT / CSIRT	Web	Facilita la visión global de todas las implicaciones (no sólo tecnológicas) que conlleva la puesta en marcha de estos equipos de respuesta, tanto en su diseño como en el desarrollo y posterior funcionamiento, especialmente entre las administraciones públicas. A lo largo de este documento, se desarrolla en sus distintos capítulos: la estrategia general, las experiencias y ámbitos de actuación actuales de los CERT a nivel nacional, la normativa, buenas prácticas y legislación aplicable, la formación e D8 información necesaria, y las herramientas que pueden ser usadas.	El documento presenta una propuesta para la creación de un CSIRT a partir de los marcos existentes de la marcos y metodologías existentes de CSIRT, como aquellos desarrollados por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

Título de la Fuente	Tipología de la fuente (web, RSS, base de datos, ferias, etc.)	Descripción general	¿Cómo aporta la fuente a mi proyecto?
ENISA - Como Crear un CSIRT Paso a Paso	Web	Describe el proceso de creación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) desde todas las perspectivas pertinentes, como la gestión empresarial, la gestión de procesos y el punto de vista técnico. Este documento recoge dos de los productos escritos en el apartado 5.1 del Programa de trabajo de la ENISA para 2006.	El documento indica las recomendaciones paso a paso se deben seguir para la creación de un CSIRT, desde la definición de los servicios básicos, plan comercial para su oferta y establecimiento de procedimientos operativos y técnicos.
NIST Cybersecurity Framework	Web	El marco de trabajo es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de Ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la seguridad cibernética entre los interesados internos y externos de la organización	El marco propone actividades de Ciberseguridad y tendientes a considerar los riesgos de Ciberseguridad como parte de los procesos de gestión de riesgos de la organización. El documento consta de tres partes: el Marco básico, el perfil del marco y los Niveles de implementación del marco. El Framework indica referencias formativas que son comunes a través de los sectores de infraestructura crítica

Título de la Fuente	Tipología de la fuente (web, RSS, base de datos, ferias, etc.)	Descripción general	¿Cómo aporta la fuente a mi proyecto?
			(Funciones, Categorías y Sub categorías), proporcionando la orientación detallada para el desarrollo de perfiles individuales de la organización.
ENISA CSIRT Capabilities How to assess maturity? Guidelines for national and governmental CSIRTs	Web	Brinda una herramienta de orientación para los CSIRT nacionales y gubernamentales, que están considerando alcanzar el siguiente nivel de madurez y una buena comprensión de sus capacidades. Este documento ofrece recomendaciones para los CSIRT sobre cómo mejorar y madurar en sus procesos de negocio y gestión de incidentes con el fin de estar mejor preparados para proteger a sus clientes.	Este documento ofrece recomendaciones para los CSIRT sobre cómo mejorar y madurar en sus procesos de negocio y gestión de incidentes con el fin de estar mejor preparados para proteger a sus clientes.
Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) –	Web	Describe el modelo propuesto para la creación de un Equipo de Respuesta a Incidentes de Seguridad de la Información - CSIRT colombiano (por las siglas en inglés de Computer Security Incident Response	El documento analiza los principales aspectos de la creación de un CSIRT, recomendando desde la construcción de su misión y objetivos, hasta como crear una

Título de la Fuente	Tipología de la fuente (web, RSS, base de datos, ferias, etc.)	Descripción general	¿Cómo aporta la fuente a mi proyecto?
Diseño de un CSIRT de Colombia para la estrategia gobierno en línea		Teams).	propuesta de funcionamiento. Incluye también los procesos, procedimientos, indicadores y estructura organizacional que debería tener este equipo de respuesta.

Fuente: Elaboración propia.

A su vez, se presentan en la siguiente tabla publicaciones que permiten reforzar y a su vez ser un referente que complemente y apoye el diagnóstico e identificación de oportunidades en materia de las capacidades, estructura, organización y servicios en el modelo de gestión de la Ciberseguridad y Ciberdefensa para estructurar el CERT internacional.

Tabla 2.

Otras publicaciones que referencian la maduración de Servicios de un CERT

Título de la fuente	Tipología de la fuente (web, RSS, base de datos, ferias, etc.)	Descripción General	¿Cómo aporta la fuente a mi proyecto?

Universidad Nacional abierta y a distancia - Organizaciones CERT o CSIRT's Alrededor del Mundo	Web	En la actualidad existen múltiples organizaciones que usan el nombre CERT - Computer Emergency Response Team (Equipo de Respuesta a Emergencias de Computación) o CSIRT (término genérico de significado equivalente). En la fuente se presentan algunas de estas organizaciones, servicios y experiencias que han fortalecido la seguridad en cada uno de los Países donde operan	Presenta una referenciación del estado del arte y buenas prácticas implementadas por diferentes CERT para el mejoramiento de sus servicios.
ccn-cert.cni.es - GUÍA DE CREACIÓN DE UN CERT / CSIRT	Web	La guía es un instrumento eficaz que facilita una visión global de todas las implicaciones (no sólo tecnológicas) que conlleva la puesta en marcha de estos equipos de respuesta, tanto en su diseño como en el desarrollo y posterior funcionamiento, especialmente entre las administraciones públicas.	Es un documento de buenas prácticas generado por una de las organizaciones pioneras en el establecimiento de equipos de repuesta a nivel mundial. Genera un conjunto de lineamientos que permitan establecer y generar un nivel de madurez de los servicios que presta a la comunidad
Good Practice Guide for Incident Management	Web	En el documento se describen las buenas prácticas y proporciona información práctica y directrices para la gestión de la red y la seguridad de la información con énfasis en la gestión de incidentes. El área de enfoque principal de la guía es el proceso de gestión de	Es documento que genera una guía para el adecuado tratamiento de un incidente de seguridad informática, el cual es el proceso básico que debe atender un CERT.

		incidentes - el servicio básico llevado a cabo por la mayoría de los CERT - que implica la detección y registro de incidentes, seguido de triage (clasificación, priorización y asignación de incidentes), resolución de incidencias, cierre y post análisis.	
cert.org - ¿Qué habilidades son necesarias cuando dotación de personal Su CSIRT?	Web	En esta página web, se describe un conjunto mínimo de conocimientos básicos que los miembros del personal del CSIRT deberían tener. Si se quiere construir un equipo de seguridad equipo de respuesta a incidentes (CSIRT) con administradores de incidentes capaces, se necesita gente con un cierto conjunto de habilidades y conocimientos técnicos, y con habilidades que les permitan responder a incidentes, realizar tareas de análisis, y comunicarse de manera efectiva con su circunscripción y otros contactos externos.	Este enlace proporciona una guía de las competencias que se deben potencializar dentro de las diferentes áreas que componen el equipo de respuesta a Incidentes.
elizabethphillips.co.uk - Computer Security Incident Response Teams(CSIRTs) An Overview	Web	En este documento se presenta la función y el propósito de la seguridad informática de un equipo de Respuesta a Incidentes (CERT), los servicios que prestan, y también varios ejemplos de tales equipos nacionales y multinacionales	La fuente proporciona la información concerniente al estado del arte de diferentes equipos de incidentes informáticos a nivel internacional. De igual forma

		existentes, así como a las organizaciones que se presentan fomentan la cooperación y coordinación de tales equipos. Luego, el documento presenta estudios de casos como ejemplos de tales equipos nacionales.	referenciarían aquellos organismos que apoyan y cooperan con la labor de los CERT.
recibe.cucei.udg.mx - Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT)	Revista	En este artículo se describe una propuesta creada para proteger la información y la infraestructura de un equipo de respuestas ante incidentes de seguridad (CSIRT), se aborda una propuesta de los aspectos de seguridad que debe tener un CSIRT abarcando las áreas de Telecomunicaciones, Equipo hardware y Sistemas SIEM (Security Information and Event Management).	Este es un artículo que presenta información muy puntual con respecto a capacidades técnicas mínimas que debe implementar un CERT para brindar un buen servicio.
sites.oas.org - Buenas prácticas para establecer un CSIRT nacional	Web	El presente documento analiza el proceso de gestión de un proyecto para la creación y la puesta en marcha de un CSIRT nacional, incluidos distintos criterios y consideraciones necesarias para definir su constitución, misión, visión, alcance, servicios, tiempos, y aspectos legales e institucionales u organizacionales. Esto incluye un examen de los requerimientos de recursos humanos, tanto en términos de	La fuente proporciona un paso a paso y aborda de manera específica cada una de las capacidades técnicas, operativas y a nivel de competencias del personal que desde su inicio debe implementar un CERT con el fin de no presentar a futuro algún tipo de obstáculos o inconvenientes a nivel

contratación como de formación continua, que son necesarios para establecer el personal de un equipo nacional de respuesta a incidentes	estructural u organizacional.

Fuente: Elaboración propia.

Teniendo en cuenta estos referentes anteriores, se mencionan a continuación algunos de los aspectos principales en el establecimiento del CERT, de acuerdo a su enfoque y misionalidad, como lo son los servicios que se pueden llegar a prestar a través del equipo, lo cuales pueden dividirse en dos categorías: actividades en tiempo real directamente relacionados con la principal tarea de respuesta a incidentes, y actividades proactivas no en tiempo real, de apoyo de la tarea de respuesta a incidentes. La segunda categoría y parte de la primera categoría consisten en servicios que son opcionales en el sentido de que no todos los CSIRT los ofrecerán, dependiendo de su enfoque o actividad dentro de la organización. Estos servicios pueden ser:

Servicios Preventivos.

"Aquellos servicios que proveen asistencia y atención para ayudar a preparar, proteger y asegurar un componente de sistema en anticipación a futuros ataques, problemas o eventos. Llevar a cabo este tipo de servicios reducirá directamente el número de incidentes en el futuro". (Proyecto Diseño de modelo SGSI para la estrategia de Gobierno en Línea, 2008)

Servicios Reactivos.

"Aquellos servicios que se provocan o se desencadenan por un evento o requerimiento. Este tipo de servicios, son un componente clave para un trabajo de atención de incidentes" (Ministerio de Comunicaciones, 2008).

Manejo de instancias.

"Incluye el análisis de cualquier fichero u objeto encontrado en un sistema que pueda intervenir en acciones maliciosas, como restos de virus, gusanos, secuencias de comandos, troyanos, etc. También incluye el tratamiento y la difusión de la información resultante entre los proveedores y otros interesados, con el fin de evitar que el software malicioso se siga extendiendo y mitigar los riesgos" (Ministerio de Comunicaciones, 2008).

Gestión de la seguridad de la información.

Son servicios establecidos y muy conocidos, diseñados para mejorar la seguridad general de una organización. Estos servicios están diseñados para tener en cuenta los comentarios recibidos y las lecciones aprendidas basándose en los conocimientos adquiridos al responder a incidentes, vulnerabilidades y ataques. Lo anterior hace que se oferten productos que permitan a terceros ayudar a mejorar toda la seguridad de una organización, identificar riesgos, amenazas y debilidades del sistema. Son servicios generalmente no técnicos pero preventivos en naturaleza, contribuyendo indirectamente la reducción en el número de incidentes. (Ministerio de Comunicaciones, 2008).

Dentro de esta clasificación son varios los servicios que se pueden llegar a ofrecer por parte del CERT o CSIRT o SOC, dependiendo de su nivel de madurez y experticia en la ejecución de sus servicios. La adecuada selección de los servicios y su forma progresiva de implementación para alcanzar una exitosa imagen, credibilidad y confianza con los clientes finales y el nivel directivo, son una decisión crucial dentro de la madurez del CERT. A continuación, se presenta una breve visión general de todos los servicios conocidos que pueden llegar a prestar estos equipos, tal como se definen en el «Manual del CSIRT» publicado por el CERT/CC y que pueden llegar a bridar una visión más general de como evaluar el nivel en el que se encuentran de acuerdo a su nivel de madurez, ellos son:

Tabla 3.
Servicios de un CERT

Alertas y advertencias	Comunicados	Análisis de instancias
Tratamiento de incidentes	Observatorio de tecnología	Respuesta a las instancias
Análisis de incidentes	Evaluaciones o auditorías de la seguridad	Coordinación de la respuesta a las instancias
Apoyo a la respuesta a incidentes		Gestión de la calidad de la seguridad

Coordinación de la respuesta a incidentes	Configuración y mantenimiento de la seguridad	Análisis de riesgos
Respuesta a incidentes in situ	Desarrollo de herramientas de seguridad	Continuidad del negocio y recuperación tras un desastre
Tratamiento de la vulnerabilidad	Servicios de detección de intrusos	Consultoría de seguridad
Análisis de la vulnerabilidad	Difusión de información relacionada con la seguridad	Sensibilización
Respuesta a la vulnerabilidad		Educación / Formación
Coordinación de la respuesta a la vulnerabilidad		Evaluación o certificación de productos
Análisis de artefactos		
Respuesta ante artefactos		
Coordinación de la respuesta de artefactos		

Fuente: ENISA

Con el fin de medir el nivel de madurez de los Equipos de Respuesta ya certificados o brindar una guía para aquellos que se encuentren actualmente en este proceso, para el segundo semestre de 2017, ENISA ha publicado una actualización de su modelo de madurez de gestión de

incidentes de seguridad (SIM3) comúnmente utilizado en Europa, lo que hace más fácil para cualquier equipo CSIRT autoevaluar su madurez en términos de SIM3, este documento tiene por objetivo ser una herramienta de orientación para los CSIRT nacionales y gubernamentales que están considerando alcanzar el siguiente nivel de madurez y una buena comprensión de sus capacidades, ENISA también publica una herramienta de evaluación, donde los equipos de respuesta pueden medir la efectividad de las políticas, procedimientos y procesos implementados en el CSIRT (European Union Agency for Network and Information Security, (2017).

Una vez realizada la evaluación con este modelo, el CERT dará una visión del estado de los servicios que presta actualmente clasificándolos en básico, intermedio y certificables, de acuerdo con el enfoque o el trabajo que haya realizado el equipo en temas estratégicos, técnicos u operacionales, de tal forma que, si el equipo ha fortalecido más las capacidades operacionales o técnicas, entonces en la evaluación presentará fallas en el establecimiento de procedimientos o estrategias. Si el equipo está más centrado en los procedimientos y la política, se verá evidenciada una falla en la falta de experiencia y herramientas.

"Un proceso de certificación ideal sería para un equipo bien equilibrado, por ejemplo, para un equipo operativo con alguien lo suficientemente experimentado como para encargarse de los procedimientos. Una combinación de capacidades resulta en una experiencia de certificación más fluida" (European Union Agency for Network and Information Security, (2018).

Al mismo tiempo, ya teniendo identificado y con un nivel aceptable de madurez los servicios que se van a ofrecer por parte del CERT, se debe realizar la adquisición de herramientas de

hardware o software que soporten, automaticen o apoyen las tareas a realizar para brindar al cliente un buen servicio; a continuación, se exponen algunos de los elementos que se deben tener en cuenta en cada etapa de acuerdo al servicio que se proyecte implementar:

Tabla 4.

Herramientas tecnológicas básicas de un CERT

TIPO DE EQUIPO	ELEMENTOS
Equipos y medios de conectividad	- Routers. - Switches. -Sistema de Almacenamiento (SAN) - Cableado Estructurado. - Enlace de Internet con una velocidad adecuada y bloque de direcciones IP válidas. - Dispositivos de seguridad. (Antivirus, IDS, IPS) Firewall. - Detección de Intrusos. - Correo electrónico, WEB, NTP, DNS. - Registro de bitácoras de sistemas. - Archivos. - Intranet. - Acceso Remoto (VPN). - Backup. - Ambiente de Pruebas. - Voz sobre IP (VoIP)
Estaciones de Trabajo y Equipos Portátiles.	- Estaciones de trabajo. - Dispositivos móviles como portátiles, celulares, tablets, lectores de código de barras. - Accesorios: pen drive, CDs, DVDs, Discos

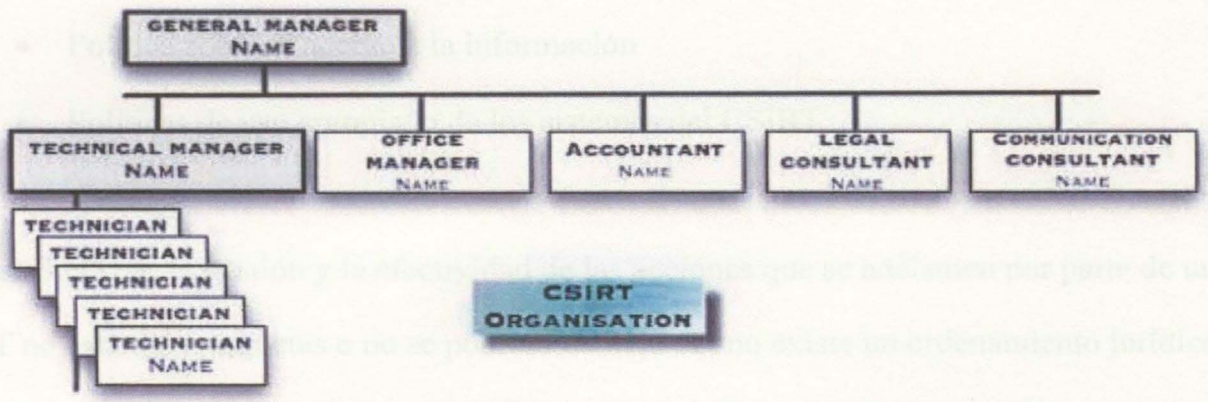
Equipos para la seguridad en ambiente físico.	Duros Externos, Herramientas, etc. - Caja Fuerte a prueba de fuego para almacenar documentos y copias de seguridad. - Infraestructura de protección contra incendios. (Prevención, extinción y alarma.) - Sistema de refrigeración y aire acondicionado compatible con las especificaciones de los equipos adquiridos. - Infraestructura de protección contra interrupciones en el suministro de energía eléctrica. (Estabilizadores, nobreaks, grupos de generadores compartidos con las instalaciones del órgano que acogerá al CSIRT.)
Software	- Servicios de correo electrónico, Web, NTP y DNS. - Aplicativos de Criptografía y Firma Digital. - Aplicativos para el análisis forense - Utilización de programas de virtualización de servidores y estaciones de trabajo para usos internos y de Laboratorio. - Sistema de Seguimiento de Incidentes - Correo Electrónico Seguro - Sistemas de Comunicaciones Seguras - Listas de Control de Acceso - HoneyPot - Gestor de Contraseñas - Anti Sniffers - Herramientas Criptográficas - Aplicaciones de aseguramiento de protocolos y servicios - VPN - Antivirus

	- Herramientas de análisis de Malware
	- Herramientas de análisis Forense
Otros	- Proyectores
	- Impresora Multifuncional. (Impresora, fax y escáner.)
	- Dispositivos para la realización de copias de seguridad: grabadores de CD, DVD y Cintas Magnéticas.
	- Trituradora de papel.
	- Material de Oficina.

Fuente: Elaboración propia.

Así mismo, una adecuada estructura organizacional de un CERT, se convierte en un punto de control y gestión clave a la hora de la atención de incidentes, es por esto que el documento como crear un CSIRT paso a paso de ENISA, propone la siguiente estructura organizacional interna del CSIRT:

Ilustración 3. Organigrama CSIRT (Propuesto por ENISA)



Nota. Recuperado de "cómo crear un CSIRT paso a paso" de Producto WP2006/5.1(CERT-D1/D2), 2006, Recuperado de: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport.

Por lo que se refiere a la estandarización de procedimientos, por parte de la Organización de Estados Americanos OEA, en su documento *"Buenas Prácticas para establecer un CSIRT nacional"* recomienda que se deben establecer lineamientos, procedimientos o guías que definan como mínimo las siguientes políticas y procedimientos (Organización de Estados Americanos - OEA, 2016):

- Política de clasificación de información
- Política de protección de datos
- Política de retención de información
- Política de destrucción de información
- Definición de incidentes de seguridad y política de eventos
- Política de divulgación de información
- Política sobre el acceso a la información
- Políticas de uso apropiado de los sistemas del CSIRT

Para finalizar, la gestión y la efectividad de las acciones que se adelanten por parte de un CERT no estarían completas o no se podrían realizar sin no existe un ordenamiento jurídico que las soporte, a nivel Colombia se han establecido diferentes herramientas jurídicas e iniciativas gubernamentales, que han permitido que los organismos de Ciberdefensa y Ciberseguridad creados mediante el CONPES 3701 de 2011 puedan ejercer sus funciones de una manera más

dinámica y eficiente, mejorando la calidad de la utilización del Ciberespacio en Colombia, entre ella se destacan las siguientes (Consejo Nacional de Política Económica y Social (CONPES 3701), 2011):

- Ley 527 de 1999 - Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
- Ley 599 DE 2000 - Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."
- Ley 962 de 2005 - Habeas data financiera, y seguridad en datos personales;
- Ley 1150 de 2007 - Seguridad de la información electrónica en contratación en línea;
- Ley 1266 de 2008 Habeas data financiera, y seguridad en datos personales;
- Ley 1341 de 2009 - Tecnologías de la Información y aplicación de seguridad;
- Ley 1453 de 2011 - Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal.

- Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales;
- Ley 1712 de 2014 - Transparencia en el acceso a la información pública;
- Decreto 032 de 2013 - Por la cual se crea la Comisión Digital y de Información Estatal
- Decreto 2364 de 2012 - Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones;
- Resolución 3066 de 2011 Comisión de Regulación de Comunicaciones - Por la cual se establece el Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones.
- Resolución 76434 de 2012 - Se imparten instrucciones relativas a la protección de datos personales.
- Circular 052 de 2007 (Superintendencia Financiera de Colombia) - Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.
- Documento CONPES 3701 de 2011 - Lineamientos de Política para Ciberseguridad y Ciberdefensa
- Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital
- Directiva Permanente 2014-18 de 2014 – Políticas de Seguridad de la Información para el Sector Defensa.
- Documento diseño de un CSIRT de Colombia para la estrategia gobierno en línea, Ministerio de Comunicaciones

(Consejo Nacional de Política Económica y Social (CONPES 3701), 2011).

De la normatividad colombiana cabe resaltar la ley La ley 1273 de 2009 o ley de delitos informáticos, la cual estableció un nuevo bien jurídico tutelado llamado "de la protección de la información y los datos", y en dicha norma se encuentran tipificados nueve tipos penales que van dirigidos a la protección de la información, los datos y el patrimonio económico, los cuales son:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos
- Daño informático
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales
- Hurto por medios informáticos y semejantes
- Transferencia no consentida de activos

Por otra parte, a nivel estratégico específicamente para el colCERT, el equipo de respuesta se encuentra adelantando durante el 2018 diferentes mesas de trabajo con la Comisión de Regulación de Comunicaciones, cuyo objetivo es modificar el artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y así obtener un respaldo por parte de este organismo para que los Proveedores de Servicios de Internet (ISP), realicen el reporte de incidentes de seguridad de la información al colCERT y con ello tener mayor información y conocimiento del entorno para afrontar las amenazas cibernéticas. El proyecto de Resolución puede ser consultado en

https://www.crcom.gov.co/uploads/images/files/Proyecto%20de%20Resoluci%C3%B3n%20seguridad%20digital_publicar2018.pdf.

También, para el año 2018 se sancionó la ley 1928 de 2018, en materia de cooperación internacional en la lucha contra la ciberdelincuencia, por la cual se aprueba el "Convenio sobre la ciberdelincuencia" celebrado por el Consejo de Europa en Budapest en el año 2001, el cual es el primer tratado internacional que hace frente a los delitos informáticos y de internet, enfocándose en fortalecer la cooperación internacional y establecer un marco de regulación a los delitos cibernéticos.

De igual forma, en el ámbito internacional se han establecido una serie de documentos normativos que coadyuvan a construir unas reglas base para el uso aceptable del Ciberespacio, así como unos parámetros que rijan las relaciones, la convivencia y respeto por los derechos humanos, pese a las diferencias políticas existentes entre un Estado y otro para los niveles de libertad de acceso y publicidad de la información a través de este medio, entre la normatividad existente se destacan:

- Política de Ciberdefensa OTAN - Plan de Acción para la Ciberdefensa, en él se indican las tareas y actividades específicas para las propias estructuras de la OTAN y las fuerzas defensivas de sus aliados.
- Manual de Tallin - Documento que examina cómo poder aplicar las normas existentes de derecho internacional a la nueva Ciberguerra.
- Directiva (UE) 2016/1148 del parlamento europeo y del consejo - Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

- El mencionado anteriormente Tratado No.185 Convención sobre ciberdelincuencia – convenio Budapest del 23/11/2001, tratado abierto que aborda los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Al mismo tiempo realiza una clasificación de los delitos informáticos, en cuatro grupos así:
  - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
  - Delitos informáticos
  - Delitos relacionados con el contenido
  - Delitos relacionados con infracciones de la propiedad intelectual y derechos afines (OEA, 2001).

Estructura y capacidades del colCERT

Diagnóstico colCERT

En esta sección se presenta el diagnóstico realizado al CERT nacional de Colombia, el cual fue ejecutado a través de la metodología de investigación inductiva que según Francis Bacon (1561-1626), citado por (Rodríguez Jiménez & Pérez Jacinto, 2017), "*fue el primero que propuso la inducción como un nuevo método para adquirir conocimientos. Afirmaba que para obtener conocimiento es imprescindible observar la naturaleza, reunir datos particulares y hacer generalizaciones a partir de ellos. Según Bacon, las observaciones se hacían sobre fenómenos particulares de una clase y luego a partir de ellos se hacían inferencias de la clase*

entera". De igual forma, indica que en el método inductivo se llevan a cabo una serie de pasos: a) observación; b) formulación de hipótesis; c) verificación d) tesis; e) ley y f) teoría; los cuales se desarrollan en el transcurso del documento a través del desarrollo de cada capítulo, iniciando con el contexto y marco de referencia enfocadas a desarrollar las etapas a y b de la investigación, siguiendo con el presente capítulo que busca abordar la etapa c y d que permitan proponer una teoría a través de la estrategia que lleve a cumplir con los objetivos propuestos.

Para realizar el diagnóstico del colCERT, se utilizará la técnica de la entrevista de tipo estructurada que de acuerdo a lo relacionado con (Folgueiras, 2016), con el apoyo de una encuesta que esta previamente diseñada para ser desarrollada de forma fija y secuencial. De esta forma, se aplicó dicha técnica al señor Ingeniero Wilson Arturo Prieto Hernández, Asesor de Ciberseguridad del equipo de respuesta, el cual tiene más de 9 años de experticia laborando en este equipo y es el punto de contacto en la atención de incidentes reportados a nivel nacional por las empresas prestadoras de servicios y adicionalmente realiza las conferencias de buenas prácticas en Ciberseguridad y presentación del CERT nacional.

Adicionalmente, es pertinente indicar que la siguiente información suministrada durante la entrevista fue de carácter general, toda vez que por políticas de seguridad no se puede revelar al público en general la estructura interna, procedimientos o políticas internas que se administran del CERT nacional, por lo cual fue suministrado por parte del funcionario un enlace en donde se podría encontrar la información que es pública del equipo de respuesta; el cual es:

(https://caivirtual.policia.gov.co/sites/default/files/colcert_sensibilizacion_gestion_de_incidentes.pdf)

El Equipo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT es un grupo adscrito a la Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional y tiene como responsabilidad central asignada mediante el CONPES 3701 de 2011, la de organismo de Coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual está enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional, tales como el Centro Cibernético Policial (CCP), el Comando Conjunto Cibernético (CCOC) y el CSIRT de la Policía Nacional. Sus principales funciones son:

- Colaboración activa en la resolución de incidentes
- Asistencia técnica sector público y privado
- Coordinación en la gestión y respuesta de incidentes
- Asistencia ante emergencias cibernéticas
- Desarrollo de capacidades operativas
- Proveer información estratégica de inteligencia
- Asesoramiento y apoyo en Ciberseguridad y Ciberdefensa
- Gestión y Monitoreo de Infraestructuras Críticas de Colombia (Policía Nacional, 2018).

En cuanto a los servicios que ofrece a nivel nacional, el CERT brinda el apoyo a empresas públicas y privadas en los siguientes servicios proactivos, reactivos y de gestión:

Tabla 5.

Gestión y Respuesta a Incidentes

Proactivos	Reactivos	Gestión
Reducir los riesgos de seguridad y su impacto, evitar incidentes cibernéticos	Responder a una amenaza o incidente que pudo haber sufrido una infraestructura o un sistema de información	Mediante los cuales se pretende mejorar todos los conceptos de Ciberseguridad en los ámbitos de formación y sensibilización
• Informes sobre vulnerabilidades presentes en una infraestructura o sistema de información • Gestión de Incidentes • Auditorias y evaluaciones de seguridad • Apoyo en inteligencia cibernética • Apoyo técnico para la mitigación y resolución del incidente • Trabajo colaborativo con los operadores de internet y administradores de dominio	• Gestión de Incidentes • Alertas sobre nuevas vulnerabilidades • Análisis de código malicioso (muestras de malware) • Envió y recepción de información sobre ataques con los homólogos internacionales	• Sensibilizar a entidades tanto públicas como privadas en temas de ciberseguridad • Coordinación de acciones para la identificación, priorización y catalogación de Infraestructuras Críticas. • Talleres de gestión de Incidentes • Eventos de Ciberseguridad

Nota. Recuperado de: "copyright – colCERT", Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, (23 de noviembre, 2017). Recuperado de https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf)

Dentro de la gestión de incidentes que realiza el grupo, se tiene una clasificación de los ciber incidentes con el fin de aplicar el adecuado tratamiento de estos de acuerdo con su tipo, esta es:

Tabla 6.

Clasificación de los ciber incidentes

Clase de incidente	Descripción	Tipo de ciberincidente
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o	Virus, Gusanos, troyanos, spyware, rootkit, ransomware, herramientas para acceso remoto RAT

	usuario y con finalidades muy diversas	
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	Denegación [Distribuida] del Servicio DoS / DDoS, Fallo (Hardware/Software), Error humano, Sabotaje.
Obtención de información	Proceso de recolección de información en búsqueda de nuevas amenazas, brechas de seguridad o mitigación de las mismas.	Identificación de vulnerabilidades (scanning), Sniffing, Ingeniería social, phishing
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una	Compromiso de cuenta de usuario, Defacement (desfiguración), CrossSite Scripting (XSS), Cross-Site Request Forgery (CSRF) Falsificación

	organización.	de petición entre sitios cruzados, Inyección SQL, Spear Phishing, Pharming (DNS), Ataque de fuerza bruta, Inyección de archivos Remota, Explotación de vulnerabilidad software, Explotación de vulnerabilidad hardware
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información, Modificación y borrado no autorizada de información, Publicación no autorizada de información, Exfiltración de información

Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes	Suplantación / Spoofing, Uso de recursos no autorizado, Uso ilegítimo de credenciales, Violaciones de derechos de propiedad intelectual o industrial.
Contenido Abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (Correo Basura), Acoso/extorsión/ mensajes ofensivos, Pederastia / racismo/ apología de la violencia/delito, etc.
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	Abuso de privilegios por usuarios, Acceso a servicios no autorizados, Sistema desactualizado,

	Otros
Otros	Otros incidentes no incluidos en los apartados anteriores

Nota. Recuperado de: "Gestión y Respuesta a Incidentes", Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, (23 de noviembre, 2017). Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf)

Actualmente el grupo cuenta con alianzas estratégicas a nivel nacional y mundial que permiten alertar y gestionar los diferentes incidentes a nivel de seguridad informática a nivel Colombia. Entre las alianzas más destacadas están FIRST, OEA, .CO, Microsoft, US-CERT, APWG y ENISA tal y como lo observamos en la siguiente ilustración:

Ilustración 4. Alianzas destacadas del colCERT.

Nota. Recuperado de: "Gestión y Respuesta a Incidentes", Grupo de Respuesta a Emergencias Cibernéticas de Colombia – colCERT, (23 de noviembre, 2017). Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/colcert_-_sensibilizacion_gestion_de_incidentes.pdf)

A nivel de estructura interna el grupo colCERT cuenta con un grupo de funcionarios que se encargan de gestionar los diferentes incidentes y lo relacionado con la documentación e histórico de los procesos a cargo del grupo, sin embargo, esta planta de personal no cubre la totalidad de los requerimientos que se reciben.

Teniendo en cuenta lo anterior y a partir de las buenas prácticas expuestas en el marco teórico, se realizó un diagnóstico de las capacidades actuales, dividiendo las mismas en tres secciones: a nivel Estratégico, de Servicios e Infraestructura tecnológica instalada. De lo cual se obtuvo lo siguiente:

A nivel Estratégico

Para evaluar esta sección se tomó la guía de creación de un CERT / CSIRT, publicada por el Centro Criptológico Nacional de España, lo anterior, teniendo en cuenta que presenta unos criterios de evaluación generales y que nos pueden dar una aproximación a la necesidad actual del colCERT con la información que se obtuvo de la entrevista realizada al Ingeniero Wilson Prieto.

Tabla 7.

Análisis a nivel estratégico del colCERT

CRITERIO	DESCRIPCIÓN	LINEA BASE	BRECHA PARA EL colCERT
Tamaño de la Comunidad a la que se da servicio.	Este es el parámetro principal, puesto que a mayor número de miembros se generarán más peticiones de asistencia en gestión de incidentes y de otro tipo.	Según ENISA, Este tipo de CSIRT no suele tener un grupo de clientes directo, pues se limita a desempeñar un papel de intermediario para todo el País.	Alcance limitado de acuerdo a infraestructura y personal, se cubre tan solo una pequeña parte de la empresa privada y pública
Grado de autoridad sobre los miembros de la Comunidad	Es un parámetro relevante si se considera la posibilidad de gestionar los servicios por propia iniciativa o por imperativo legal, lo que condiciona en	Según el CCN de España, este parámetro puede establecerse como: Autoridad completa: el Equipo puede llevar a cabo todas las acciones necesarias para gestionar los incidentes; los miembros de la Comunidad deben implantar las medidas establecidas por el CERT o	El modo en el que el CERT se relacione con la Comunidad y el grado de autoridad sobre las intervenciones que realice determinará enormemente el

CRITERIO	DESCRIPCIÓN	LINEA BASE	BRECHA PARA EL colCERT
	este último caso la existencia probable de un mayor volumen de incidentes a gestionar.	bien dar facilidades para que su personal las realice. Autoridad compartida: el CERT colabora abierta y directamente con los administradores y gestores TIC de la Comunidad en la gestión directa de los incidentes, facilitando información y tomando las decisiones de manera conjunta. Autoridad nula: no se tiene ningún tipo de autoridad sobre los miembros de la Comunidad y únicamente actúa como asesor y fuente confiable de información. Autoridad indirecta: el equipo del CERT no tiene autoridad directa sobre la Comunidad, pero indirectamente tiene la posibilidad de ejercer presión sobre sus miembros. Este tipo de relación no está	tipo y el nivel de servicios que ofrezca. Actualmente se cuenta con una autoridad compartida.

CRITERIO	DESCRIPCIÓN	LINEA BASE	BRECHA PARA EL colCERT
		explicitada formalmente y se tratan más bien de interrelaciones que han surgido con el paso del tiempo o bien a través de una tercera organización (por ejemplo, la organización patrocinadora que apoya abiertamente al CERT).	
Aptitud operativa / operabilidad	Cubre los requisitos técnicos y operacionales que el equipo debe cumplir. Es crucial cumplir un tiempo de respuesta mínimo en la respuesta a incidentes.	ENISA aconseja que el número mínimo de integrantes para implantar un CERT no baje de 6 a 8 personas ocupadas a tiempo completo. Entre ellos deben figurar un jefe de equipo y un gestor de incidentes senior. El CERT debe estar disponible 24/7/365 tanto para su Comunidad como para cooperar con socios nacionales e internacionales.	No se cumple con la línea base establecida
Catálogo de Servicios	Cubre los servicios que el equipo proporciona a su	Según el CCN de España, se debería mencionar Objetivo, Definición, Funciones, Niveles de	No se tiene estructurado ni publicado

CRITERIO	DESCRIPCIÓN	LINEA BASE	BRECHA PARA EL colCERT
	Comunidad o utiliza para su propio funcionamiento interno.	servicio, Parámetros de calidad, Política de comunicación Prioridades.	
Promoción y comunicación de servicios.	Es el grado de conocimiento por parte de la Comunidad de los servicios que se ofrecen. Este aspecto implica que la dotación del CERT debe ir progresando a medida que aumente su impacto prestando especial atención a la promoción y	Según el CCN de España, el éxito de un CSIRT depende de la confianza y reconocimiento que logre en su Comunidad. Esto requiere hacer énfasis en la promoción de sus actividades y servicios. El plan de comunicación y promoción debería incluir los siguientes aspectos: - Identificación de los medios disponibles. - Mecanismos oficiales de divulgación de información del centro – sala de prensa. - Participación en eventos y foros especializados o Afiliación a organismos internacionales.	Se cuenta con algunos de los criterios mínimos, pero no son ampliamente usados

CRITERIO	DESCRIPCIÓN	LINEA BASE	BRECHA PARA EL colCERT
	comunicación de los nuevos servicios.		
Capacidades de cooperación	Incluye los requisitos relativos al intercambio de información con otros equipos y que no se vean satisfechas con los anteriores criterios. Además de dotar al CERT con equipos tecnológicos y humanos, uno de los	Según ENISA, Algunos retos a los que se enfrentan los CERT en esta mayor coordinación e integración a nivel nacional e internacional, que exigen de grandes esfuerzos y recursos, son: •La normalización de la información intercambiada, y el uso de estándares abiertos. • La utilización de terminologías parecidas en los distintos estados. • El establecimiento de esquemas de respuesta	Se cuenta con unos parámetros para intercambio de información, publicados en la página web, se estandarizó los tipos de incidentes a gestionar y se tiene una política de clasificación de la información avalado por la

CRITERIO	DESCRIPCIÓN	LINEA BASE	BRECHA PARA EL colCERT
	activos más valiosos de los que dispondrá para desarrollar sus funciones en general y específicamente las de cooperación, será el conocimiento de sus miembros	similares. • La clasificación de la información sensible. • El uso de mecanismos seguros de comunicación	alta dirección del Ministerio de Defensa. Sin embargo, no se encuentran adscritos al FIRST.
Organigrama y procedimientos	Según la OEA, Las políticas de un CSIRT, además de servir como guía para sus empleados y la comunidad objetivo, son recursos útiles para	El mayor foro internacional de CSIRT en el mundo, la Organización FIRST, tiene las siguientes políticas obligatorias mínimas para un CSIRT que desee convertirse en un miembro de la comunidad:	Algunos documentos aprobados y otros no controlados en la herramienta de calidad, a su vez hace falta estructurar algunos de ellos.

CRITERIO	DESCRIPCIÓN	LINEA BASE	BRECHA PARA EL colCERT
	los miembros de la comunidad objetivo, ya que detallan cuándo un CSIRT proporciona qué tipo de servicios y cómo mantiene y protege la información que gestiona.	•Política de clasificación de información. •Política de protección de datos. •Política de retención de información. •Política de destrucción de información. •Definición de incidentes de seguridad y política de eventos. •Política de destrucción de información. •Política de divulgación de información - clasificación información. •Política sobre el acceso a la información. •Políticas de uso apropiado de los sistemas del CSIRT.	

Fuente. Elaboración Propia con criterios base de ENISA, OEA y CCN de España

Nivel de Servicios

Para el nivel de servicios se separaron en tres niveles los posibles servicios que puede ofertar un CERT, teniendo en cuenta las recomendaciones de varias organizaciones internacionales como lo son:

La Organización de Estados Americanos – OEA - Documento "Buenas Prácticas para establecer un CSIRT nacional", página 44 en donde indica "los servicios ofrecidos por un CSIRT dependerán de su tamaño, infraestructura, recursos y de las capacidades de los miembros de su equipo. Se pueden dividir en básicos, intermedios y avanzados, y es probable que crezcan a medida que el equipo madure con el tiempo (Organización de Estados Americanos - OEA, 2016).

Ilustración 5. Evolución de los servicios de un CSIRT

Nota. Recuperado de "Buenas Prácticas para establecer un CSIRT nacional" – Organización de Estados Americanos OEA.

La Agencia Europea de Seguridad de las Redes y de la Información – ENISA, en su Documento "CERT community Recognition mechanisms and schemes", página 12 indica "el desarrollo de un CERT ocurre en términos generales como una progresión de tres etapas en la cual pasa de ser establecida a lograr un conjunto completo de capacidades y estabilidad dentro de su comunidad." (Agencia Europea de Seguridad de las Redes y de la Información, 2006)

Ilustración 6. Evolución de los servicios de un CSIRT

CERT MATURITY MODEL			
	Summary	**Characteristics**	**Organisation / Mechanisms**
Tier 1	*Fundamental* (Essential, indispensable)	CERT is being established and trying to earn recognition in the CERT community (based on individual trust building).	ENISA: *A Step-by-Step Approach on How to Set up a CSIRT* (2006) ENISA: *Baseline Capabilities for National / Governmental CERTs – operational aspects* (2009) ENISA: *Map of CERTs* and *Inventory of CERT Activities in Europe* (2005, constantly updated) RARE CERT Task Force[23]: *Guide to Setting up a CERT* (1993) TF-CSIRT/TI: *'Listed' status*
Tier 2	*Baseline* (Steady, Sure-Footed)	CERT has baseline capabilities (operations) in place and its team representative gained trust among the CERT community.	ENISA: *Baseline Capabilities for National/ Governmental CERTs – Policy recommendations* (2010, 2012) IETF: RFC-2350 (2003 updated) TF-CSIRT/TI: 'Accreditation' FIRST: 'Full Membership' APCERT: 'Membership' CERT/CC: *Handbook for Computer Security Incident Response Teams (CSIRTs)* (2003)
Tier 3	*Advanced* (Stable, Well-Balanced)	CERT has a complete set of capabilities in place and has established a	ENISA: *n/g CERT standard capabilities mechanism* (2014) ISO: *ISO 27035* (2011 update)

Nota. Recuperado de "CERT community Recognition mechanisms and schemes" – Agencia Europea de Seguridad de las Redes y de la Información – ENISA.

De acuerdo con lo anterior, lo que se realizó fue un cruce de los niveles de maduración de los servicios de un CERT que cada una de las organizaciones propone y de esta forma organizar los servicios que se pueden ofertar por el equipo de respuesta, los cuales fueron expuestos en el capítulo de "*Marco Conceptual y teorías de referencia*", de la presente monografía. De esta forma se consultó al Ingeniero Wilson Prieto, obteniendo los siguientes resultados:

Tabla 8.

Análisis a nivel de Servicios del colCERT de acuerdo a su evolución

Etapa	*Servicios Reactivos*	*Servicios Proactivos*	*Servicios para la Gestión de Calidad de la Seguridad*	*Actividades que faltan por madurar en cada etapa*
I	✓ Alertas y advertencias ✓Tratamiento de incidentes ✓ Análisis de incidentes Apoyo a la respuesta a incidentes ✓ Coordinación de la respuesta a incidentes Respuesta a incidentes in situ	✓ Comunicados ✓ Servicios de detección de intrusos ✓ Difusión de información relacionada con la seguridad	✓ Análisis de riesgos ✓ Continuidad del negocio y recuperación tras un desastre ✓ Sensibilización	Alertas y advertencias 5%, Tratamiento de incidentes 100%, Análisis de incidentes y Apoyo a la respuesta a incidentes 100%, Coordinación de la respuesta a incidentes

✓ Tratamiento de la vulnerabilidad ✓ Análisis de la vulnerabilidad ✓ Respuesta a la vulnerabilidad ✓ Coordinación de la respuesta a la vulnerabilidad		respuesta a incidentes in situ 10%, Tratamiento de la vulnerabilidad 50%, Análisis de la vulnerabilidad 80%, Respuesta a la vulnerabilidad 20%, Coordinación de la respuesta a la vulnerabilidad 50%, Comunicados 20%, Servicios de detección de intrusos 50%, Difusión de información relacionada con la Seguridad

				50%.
II	✓ Alertas y advertencias ✓ Tratamiento de incidentes ✓ Análisis de incidentes Apoyo a la respuesta a incidentes ✓ Coordinación de la respuesta a incidentes ✓ Respuesta a incidentes in situ ✓ Tratamiento de la vulnerabilidad ✓ Análisis de la vulnerabilidad ✓ Respuesta a la vulnerabilidad	✓ Comunicados ✓ Observatorio de tecnología ✓ Evaluaciones o auditorías de la seguridad ✓ Servicios de detección de intrusos ✓ Difusión de información Relacionada con la seguridad	✓ Análisis de riesgos ✓ Continuidad del negocio y recuperación tras un desastre ✓ Sensibilización ✓ Educación / Formación ✓ Respuesta a las instancias ✓Coordinación de la respuesta a las instancias	Análisis de artefactos 50%, Respuesta ante artefactos 20%, Coordinación de la respuesta de artefacto 20%, Observatorio de tecnología 0%, Evaluaciones o auditorías de la seguridad 100%, Análisis de riesgos 50%, Continuidad del negocio y recuperación tras un desastre 5%,

	✓ Coordinación de la respuesta a la vulnerabilidad ✓ Análisis de artefactos ✓ Respuesta ante artefactos ✓ Coordinación de la respuesta de artefacto			Sensibilización 100%, Educación / Formación N/A, Respuesta a las instancias 50%, Coordinación de la respuesta a las instancias 50%
III	✓ Alertas y advertencias Tratamiento de incidentes ✓ Análisis de incidentes Apoyo a la respuesta a incidentes ✓ Coordinación de la respuesta a incidentes Respuesta a incidentes in situ	✓ Comunicados ✓ Observatorio de tecnología ✓ Evaluaciones o auditorías de la seguridad ✓ Configuración y mantenimiento de la seguridad ✓ Desarrollo de	✓ Análisis de riesgos ✓ Continuidad del negocio y recuperación tras un desastre ✓ Consultoría de seguridad ✓ Sensibilización ✓ Educación / Formación	Configuración y mantenimiento de la seguridad 50%, Desarrollo de herramientas de seguridad 20%, Consultoría de seguridad N/A, Evaluación o certificación de Productos

✓ Tratamiento de la vulnerabilidad ✓ Análisis de la vulnerabilidad ✓ Respuesta a la ✓vulnerabilidad ✓ Coordinación de la respuesta a la vulnerabilidad ✓ Análisis de artefactos ✓ Respuesta ante artefactos ✓ Coordinación de la respuesta de artefactos	herramientas de seguridad ✓ Servicios de detección de intrusos ✓ Difusión de información relacionada con la seguridad	✓ Evaluación o certificación de productos ✓ Análisis de instancias ✓ Respuesta a las instancias ✓ Coordinación de la respuesta a las instancias	0%.

Fuente. Estructuración propuesta, de acuerdo a lineamientos de ENISA y OEA.

Infraestructura Tecnológica

Para esta sección se tomó el equipo básico propuesto en el documento de Buenas Prácticas para establecer un CSIRT nacional de la Organización de Estados Americanos OEA, ampliando un poco más la información de acuerdo a cada uno de los ítem que allí se proponen, a su vez se preguntó acerca del nivel de implementación de cada grupo de equipos o herramientas,

clasificándolo en implementado (se tienen todos los componentes descritos en el ítem), parcialmente implementado (se tienen gran cantidad de los equipos allí descritos instalados en el CERT) y no implementado (existe una total ausencia de los equipos descritos en el ítem); evidenciando lo siguiente (Organización de Estados Americanos - OEA, 2016):

Tabla 9.

Análisis a nivel de Infraestructura Tecnológica del colCERT

Tipo de equipo	Elementos	Grado de implementación
Equipos y medios de conectividad	- Routers. - Switches. -Sistema de Almacenamiento (SAN) - Cableado Estructurado. - Enlace de Internet con una velocidad adecuada y bloque de direcciones IP válidas. - Dispositivos de seguridad. (Antivirus, IDS, IPS) Firewall. - Detección de Intrusos. - Correo electrónico, WEB, NTP, DNS. - Registro de bitácoras de sistemas. - Archivos. - Intranet.	Implementado

	- Acceso Remoto (VPN). - Contingencia y Backup - Ambiente de Pruebas. - Voz sobre IP (VoIP)	
Estaciones de Trabajo y Equipos Portátiles.	- Estaciones de trabajo. - Computadoras portátiles. - Identificación biométrica o por token para ingreso - Duros Externos, Herramientas, etc.	Implementado
Equipos para la seguridad en ambiente físico.	- Caja Fuerte a prueba de fuego para almacenar documentos y copias de seguridad. - Infraestructura de protección contra incendios. (Prevención, detección y alarma.) - Sistema de refrigeración y aire acondicionado compatible con las especificaciones de los equipos adquiridos. - Infraestructura de protección contra interrupciones en el suministro de energía eléctrica. (Estabilizadores, nobreaks,	Implementado

	grupos de generadores compartidos con las instalaciones del órgano que acogerá al CSIRT.) - Controles de acceso biométrico, CCTV	
Software	- Servicios de correo electrónico, Web, NTP y DNS. - Aplicativos de Criptografía y Firma Digital. - Aplicativos para el análisis forense - Utilización de programas de virtualización de servidores y estaciones de trabajo para usos internos y de Laboratorio. - Sistema de Seguimiento de Incidentes - Correo Electrónico Seguro - Sistemas de Comunicaciones Seguras - Listas de Control de Acceso - HoneyPot - Gestor de Contraseñas - Anti Sniffers - Herramientas Criptográficas	Implementado

	- Aplicaciones de aseguramiento de protocolos y servicios - VPN - Antivirus - Herramientas de análisis de Malware - Herramientas de análisis Forense	
Otros	- Proyectores - Impresora Multifuncional. (Impresora, fax y escáner.) - Dispositivos para la realización de copias de seguridad: grabadores de CD, DVD y Cintas Magnéticas. - Trituradora de papel. - Material de Oficina.	Implementado

Fuente: Estructuración propuesta, de acuerdo a lineamientos de ENISA y OEA.

ANALISIS DE BRECHA

De los resultados obtenidos en el diagnóstico y teniendo en cuenta el marco de referencia citado, se puede realizar el siguiente análisis de brecha identificado para cada criterio:

A nivel Estratégico:

a. Actualmente se tiene una cobertura limitada para la atención de incidentes por parte del equipo hacia las entidades públicas y privadas del Estado. Lo anterior, teniendo en cuenta que la difusión de los servicios que se prestan no es eficiente o no se ha empleado un método lo suficientemente efectivo.
b. Se logra evidenciar que el personal que conforma el grupo es muy poco para la cantidad de actividades, clientes y servicios que debería realizar el CERT nacional, de igual forma, no se tiene estructurado un catálogo de servicios que permita dar a conocer las actividades que se realizan o las capacidades instaladas actualmente en el equipo.
c. El colCERT no se encuentra adscrito al FIRST, lo cual no permite establecer un punto de contacto clave para la coordinación ante otros CSIRT a nivel mundial, así como el acceso a información que permita generar alertas tempranas con respecto a nuevas amenazas que se identifican a nivel internacional.
d. Se logra identificar la necesidad de documentar varios de los procedimientos que se ejecutan en el equipo, los cuales permiten dar continuidad de las operaciones, así

como la evaluación periódica de las actividades que se realizan con el fin de detectar su efectividad.

e. Finalmente, el colCERT no tiene estructurado y publicado un catálogo de servicios en donde se evidencien las capacidades actuales y los Acuerdos de Nivel de Servicio (ANS) para las mismas. Este catálogo de servicios según la guía de creación de un CERT/CSIRT publicada por el Centro Criptológico Nacional de España (CCN), debería especificar los siguientes aspectos como mínimo para cada servicio:

- ✓ Objetivo: propósito y naturaleza del servicio.

  Definición: Realizar la descripción del servicio a ofrecer y su alcance el nivel de cobertura que el CERT ofrece (por ejemplo: para análisis de vulnerabilidades ¿Qué tipo de responsabilidad compartida o infraestructura a utilizar?
- ✓ Funciones: qué tipo de responsabilidad asume cada una de las partes para la prestación del servicio.
- ✓ Nivel de Servicio: Grado del nivel del servicio.

  Se definen los Parámetros de calidad que el CERT suministrará a sus clientes y los acuerdos de nivel de servicio que empleará.
- ✓ Política de comunicación: se describe la forma como el CERT se relacionará con cada uno de sus clientes, proveedores o colaboradores que intervienen en la prestación de su servicio; de igual forma, se publica el tipo de información a intercambiar con cada uno.
- ✓ Prioridades: se indica la prelación que otorga el CERT en la atención de los requerimientos. Este aspecto está directamente relacionado con los puntos "Nivel de Servicio" y Parámetros de Calidad". Las consideraciones tenidas en cuenta

constituirán una imagen de lo que debe esperar obtener la Comunidad del CERT a nivel de servicios (ESPAÑA, CONSEJO NACIONAL DE CIBERSEGURIDAD, 2019).

A nivel de servicios

El nivel de madurez de los servicios, de forma general se logró evidenciar que se encuentra alineado al análisis del nivel estratégico que se realizó, lo que da como resultado servicios que se prestan sin gran cobertura a nivel nacional y con unos ANS (Acuerdo de Nivel de Servicios) altos, al no tener el talento humano suficiente para poder ejecutar las diferentes actividades. Así mismo, se requiere realizar un análisis de las capacidades actuales que se tienen a nivel del Sector Defensa y el Sector Académico, con el fin identificar las oportunidades con los aliados estratégicos que pueden proporcionar o compartir la infraestructura física y tecnológica, talento humano y el saber hacer de capacidades individuales instaladas en cada entidad, para apoyar al CERT con el fortalecimiento de alguno de los servicios que por intermedio de él se pueden ofrecer a nivel nacional e internacional.

De igual forma, para la identificación, valoración e implementación de controles o mecanismos que mejoren las capacidades del colCERT y teniendo en cuenta las funciones asignadas desde el CONPES 3701 de 2011 como ente coordinador en la gestión de incidentes a nivel nacional, se propone el empleo de la Guía de implementación del Instituto Nacional de Patrones y Tecnología - NIST, de la cual se pueden destacar las siguientes bases alineadas al objetivo que se busca en la presente monografía:

- Establecer un lenguaje común para gestionar riesgos de ciberseguridad
- Proveer un enfoque priorizado, flexible, repetible, neutral, basado en el desempeño efectivo y en términos de coste-beneficio basado en las necesidades del negocio
- Establecer criterios para la definición de métricas para el control del desempeño en la implementación
- Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones orientadas al desarrollo de estándares (Acosta, 2016).

Es de anotar que de acuerdo con el NIST: "El marco de trabajo es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la seguridad cibernética entre los interesados internos y externos de la organización" (Acosta, 2016).

El Marco de Ciberseguridad NIST aborda dentro de su estructura los controles y buenas prácticas de los siguientes estándares internacionales:

- El CSF está basado y/o hace referencia a los siguientes estándares, directrices y mejores prácticas:
- Control Objectives for Information and Related Technology (COBIT)
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC)

- ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
- ISO/IEC 27001:2013, Information technology --Security techniques --Information security management systems --Requirements
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

Estas directrices permiten las actividades y servicios que puede llegar a ofrecer el CERT, así como sus resultados a todas las partes interesadas de la organización, cubriendo desde el nivel ejecutivo hasta el nivel de implementación/operación, a través de las siguientes funciones establecidas en este marco:

- ✓ Identificar (Identify): Permite determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan este entorno.
- ✓ Proteger (Protect): Permite desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad.
- ✓ Detectar (Detect): Permite desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través de la monitorización continúa.

- ✓ Responder (Respond): Permite la definición y despliegue de actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.
- ✓ Recuperar (Recover): Permite el despliegue de actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente.
- ✓ A su vez, cada una de estas funciones cuenta con categorías y sub-categorías con sus referencias informativas relacionadas (estándares, directrices y prácticas) (Acosta, 2016).

Finalmente, a través de los niveles de implementación que propone el marco, como lo son: Nivel 1 – Parcial (Partial), Nivel 2 – Riesgos informados (Risk Informed), Nivel 3 – Repetible (Repeatable), Nivel 4 - (Adaptive), lo cual se podría alinear a los niveles de maduración del CERT que tiene ENISA de Básico, Intermedio y Certificable.

Infraestructura tecnológica

En este nivel, se propone tomar como referencia aquellos estándares mínimos sugeridos por ENISA para establecer un CSIRT, los cuales se dividen en 6 partes:

-Normas generales relativas al edificio

-Normas generales relativas al equipamiento de TI

-Mantenimiento de los canales de comunicación

-Sistema(s) de localización de registros

-Uso del «estilo corporativo» desde el principio

-Otras cuestiones

De acuerdo con el levantamiento de información, de manera general se plantea en el siguiente capítulo, una estrategia que permita subsanar las falencias identificadas y proponer las recomendaciones para el fortalecimiento de las capacidades bajó los estándares internacionales, dejando la claridad que para el desarrollo de la misma, se debe solicitar los recursos financieros y materiales necesarios en el Plan de Acción y de necesidades del Ministerio de Defensa que permitan asegurar la adecuada implementación de esta estrategia. Esto se ve exacerbado por una clara falencia en el ordenamiento jurídico que apalanquen los esfuerzos de la fuerza pública y organismos encargados de la Ciberdefensa y Ciberseguridad de Colombia; de allí que sea necesario tener una hoja de ruta con una serie de actividades o premisas ejecutadas de forma escalonada que apuntan las capacidades y buenas prácticas para el funcionamiento, identidad y sostenibilidad del CERT nacional que permitan dar a conocer a alta dirección la finalidad de dicho cambio.

Estrategia propuesta

PARTE 1:

Objetivo General de la Estrategia

Constituir al colCERT como el organismo central para la gestión de incidentes cibernéticos de Colombia al 2030 enmarcando en las dimensiones de coordinación, contacto y monitoreo en los niveles de maduración establecidos por la Organización de los Estados Americanos (OEA) para esta clase de equipos de respuesta.

Explicación parte 1: La razón por la cual se propone para el colCERT desarrollar la estrategia al 2030, es porque los objetivos que en ella se proponen implican un desarrollo de capacidades , las cuales están asociadas a recursos materiales y humanos, el recurso humano demanda tiempo en desarrollarse, teniendo en cuenta las competencias específicas que se requieren para la atención de cada servicio, a su vez, se proyectan ciclos de 4 años, considerando que las herramientas tecnológicas a implementar requieren inversión, que se desprende de los planes, programas y proyectos de las instituciones públicas, las cuales tienen periodos de duración de 4 años, con lo cual se hace necesario el apoyo y la inversión en las propuestas de desarrollo a ejecutar por parte del gobierno a nivel nacional, ya que el CERT tiene una cobertura Nacional. El tiempo de implementación se puede ver afectado de acuerdo al nivel de gestión, seguimiento y control de cambios que se tenga a la estrategia por parte del líder, para su despliegue, lo cual se ajustará a medida que se desarrollen las dimensiones de coordinación, contacto y monitoreo, las cuales también deben ser contempladas, teniendo en cuenta:

- *Coordinación:*

De acuerdo con las prácticas internacionales de ENISA (Agencia Europea de Seguridad de las Redes y de la Información, 2006) *y OEA,* (Organización de Estados Americanos - OEA, 2016) El papel de un CERT Nacional como organismo de coordinación, es una dimensión clave para la gestión de incidentes y debe estar contemplado dentro de las funciones de su creación. Los resultados de esta coordinación se ven reflejados en el establecimiento de modelos de

colaboración y alianzas tanto dentro del propio Estado, como entre el sector público y privado (Centro Criptológico Nacional de España, 2011).

Adicionalmente, teniendo en cuenta la magnitud, complejidad y las necesidades derivadas de los requerimientos, amenazas, retos y oportunidades procedentes de la utilización del Ciberespacio, el valor de la coordinación es importante en la articulación de esfuerzos y en el fortalecimiento de la seguridad colectiva, porque el Ciberespacio es un entorno que cambia constantemente y nadie tiene las capacidades completas. (Mateus, 2014).

- *Contacto:*

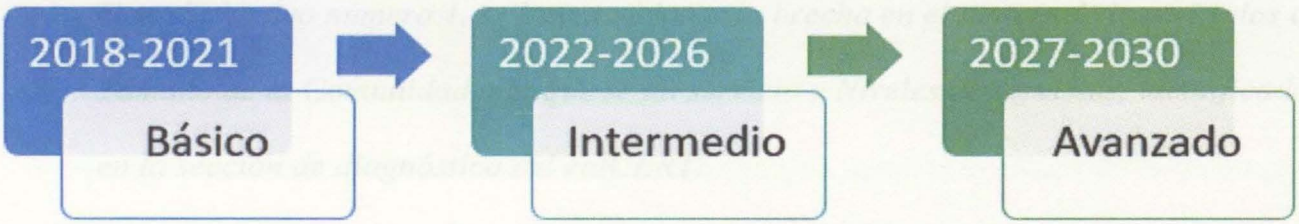
Un CSIRT Nacional sirve como punto de contacto central de seguridad de un País en lo que respecta a incidentes de seguridad informática y políticas relacionadas con la seguridad, lo que permite centralizar la información para evaluar los riesgos existentes y dimensionar las necesidades en la gestión de incidentes y protocolo de escalamiento de los mismos ante homólogos nacionales e internacionales. Adicionalmente, el contar con una única instancia de coordinación, se evitan la duplicación de esfuerzos para el desarrollo de nuevas capacidades ya que a través del CERT Nacional, según lo indica la experiencia que tienen Países como España en su documento "*guía de creación de un CERT / CSIRT*" (Centro Criptológico Nacional de España, 2011).

- *Monitoreo:*

Con el monitoreo el CERT logra identificar las últimas técnicas y herramientas disponibles de manera pública (monitorizar foros, conocer herramientas, etc), para detectar nuevas vulnerabilidades conocidas, técnicas de ataque y defensa que aporten a la gestión de incidentes.

Así mismo, para cada uno de los tres periodos establecidos en la escala de maduración se proponen niveles de madurez asociados a aquellos servicios que como indica ENISA debería ofrecer un CERT para la prevenir, mitigar y contrarrestar los diferentes riesgos y amenazas que surgen desde el ámbito cibernético. Estos niveles y servicios serán detallados en el parte 3 de la presente estrategia.

Ilustración 7. Escala de Maduración Propuesta



Fuente: Elaboración Propia.

PARTE 2:

Objetivos específicos de la Estrategia:

1. Identificar los servicios a desarrollar por el colCERT en cada nivel de madurez establecido por la OEA y ENISA.
2. Establecer las líneas de acción para el cumplimiento de los niveles de madurez para cada una de las dimensiones del colCERT (coordinación, contacto y monitoreo)

3. Establecer criterios de evaluación para el grado de implementación y aseguramiento de las dimensiones para cada uno de los servicios clasificados de acuerdo a los niveles de madurez.
4. Proponer una estructura organizacional interna para el colCERT para la prestación de los diferentes servicios ofrecidos por el equipo de respuesta en su último nivel de madurez.

Explicación parte 2:

1. *Con el objetivo número 1, se busca mejorar la brecha en el tiempo de los criterios de Tamaño de la Comunidad a la que se da servicio y Niveles de servicios, identificadas en la sección de diagnóstico del colCERT.*
2. *Con el objetivo número 2, se busca mejorar la brecha en el tiempo de los criterios de Aptitud operativa / operabilidad e Infraestructura tecnológica, identificada en la sección de diagnóstico del colCERT.*
3. *Con el objetivo número 3, se busca mejorar la brecha en el tiempo de los criterios de Grado de autoridad Promoción y comunicación de servicios sobre los miembros de la Comunidad y capacidades de cooperación, identificada en la sección de diagnóstico del colCERT.*
4. *Con el objetivo número 4, se busca mejorar la brecha en el tiempo de los criterios de Organigrama y procedimientos y Catálogo de Servicios, identificada en la sección de diagnóstico del colCERT.*

PARTE 3:

Despliegue del objetivo específico No 1: Identificar los servicios a desarrollar por el colCERT en cada nivel de madurez establecido por la OEA y ENISA.

Los niveles de maduración determinan los tipos y capacidades desarrolladas por el organismo, los cuales se verán reflejados en los servicios que brindará a sus clientes atendidos alineados al cumplimiento de los siguientes hitos:

- Nivel Básico

Para este nivel se propone la consolidación de unos servicios que permitan dar reconocimiento y publicidad al CERT nacional, consiguiendo ampliar la cobertura de prestación de servicios en las entidades privadas y públicas a nivel nacional, lo que puede llevar al establecimiento de alianzas estratégicas o convenios para el intercambio de las capacidades. De esta forma y teniendo en cuenta las capacidades que se tienen actualmente en el grupo como se pudo evidenciar en el diagnóstico, el CERT debería estar en la capacidad de ofrecer los siguientes servicios:

Tabla 10.

Servicios de Nivel Básico para el CERT

Servicios reactivos	Servicios proactivos	Gestión de la calidad de la seguridad

Alertas y advertencias	Comunicados	
Tratamiento de incidentes	Servicios de detección de intrusos	Análisis de riesgos
Análisis de incidentes	Difusión de información relacionada con la seguridad	Continuidad del negocio y recuperación tras un desastre
Apoyo a la respuesta a incidentes		Sensibilización
Coordinación de la respuesta a incidentes		
Respuesta a incidentes in situ		
Tratamiento de la vulnerabilidad		
Análisis de la vulnerabilidad		
Respuesta a la vulnerabilidad		

Fuente: Estructuración propuesta, de acuerdo a lineamientos de ENISA y OEA.

- Nivel Intermedio

El objetivo de este nivel, es implementar servicios que requieren la coordinación a nivel nacional e internacional de los diferentes organismos con capacidades en prevención, respuesta, monitoreo o respuesta de incidentes cibernéticos, permitiendo la integración de esfuerzos y capacidades de estas entidades, que conduzcan a un fortalecimiento de la Ciberdefensa,

Ciberseguridad e investigación de delitos cibernéticos, como también el mejoramiento de la credibilidad y confianza ante la alta dirección del Estado, de tal forma que el CERT tenga participación en las decisiones estratégicas y asignación de recursos para futuras vigencias. Por consiguiente, El CERT debería estar en la capacidad de ofrecer los siguientes servicios:

Tabla 11.

Servicios de Nivel Intermedio para el CERT

Servicios reactivos	Servicios proactivos	Manejo de instancias
Alertas y advertencias		Respuesta a las instancias
Tratamiento de incidentes	Comunicados	Coordinación de la respuesta a las instancias
Análisis de incidentes	Observatorio de tecnología	Gestión de la calidad de la seguridad
Apoyo a la respuesta a incidentes	Evaluaciones o auditorías de la seguridad	
Coordinación de la respuesta a incidentes	Servicios de detección de intrusos	Análisis de riesgos
Respuesta a incidentes in situ	Difusión de información relacionada con la seguridad	Continuidad del negocio y recuperación tras un desastre
Tratamiento de la vulnerabilidad		Sensibilización
Análisis de la vulnerabilidad		
Respuesta a la		

vulnerabilidad		
Coordinación de la respuesta a la vulnerabilidad		
Análisis de artefactos		

Fuente: Estructuración propuesta, de acuerdo a lineamientos de ENISA y OEA.

- Nivel Avanzado

Una vez se cuente con la infraestructura tecnológica, alianzas y nivel de participación política en el Estado para el CERT, el objetivo de este nivel es implementar los servicios que proporcionen al equipo su consolidación en Colombia y que adicionalmente generen ingresos que permitan la sostenibilidad de las capacidades en el tiempo. El CERT debería estar en la capacidad de ofrecer los siguientes servicios:

Tabla 12.

Servicios de Nivel Avanzado para el CERT

Servicios reactivos	Servicios proactivos	Manejo de instancias
Alertas y advertencias	Comunicados	Análisis de instancias
Tratamiento de incidentes	Observatorio de tecnología	Respuesta a las instancias
Análisis de incidentes	Evaluaciones o	Coordinación de la
Apoyo a la respuesta a	auditorías de la	respuesta

incidentes	seguridad	a las instancias
Coordinación de la respuesta a incidentes	Configuración y mantenimiento de la seguridad	Gestión de la calidad de la seguridad
Respuesta a incidentes in situ	Desarrollo de herramientas de seguridad	Análisis de riesgos
Tratamiento de la vulnerabilidad	Servicios de detección de intrusos	Continuidad del negocio y recuperación tras un desastre
Análisis de la vulnerabilidad	Difusión de información relacionada con la seguridad	Consultoría de seguridad
Respuesta a la vulnerabilidad		Sensibilización
Coordinación de la respuesta a la vulnerabilidad		Educación / Formación
Análisis de artefactos		Evaluación o certificación de productos
Respuesta ante artefactos		
Coordinación de la respuesta de artefactos		

Fuente: Estructuración propuesta, de acuerdo a lineamientos de ENISA y OEA.

Con los tres modelos de madurez que se proponen, se busca implementar y evaluar el desempeño de los servicios ofrecidos por el CERT, teniendo la premisa que la oferta de estos

dependerá de su tamaño (Infraestructura física), Infraestructura tecnológica, recursos y de las capacidades del talento humano.

Antes de pasar a cada nivel se debe realizar una identificación del estado del arte de los servicios y su madurez de acuerdo con las siguientes premisas.

Ilustración 8. Diagrama propuesto para Medir el nivel de Madurez de los servicios del CERT.

Fuente. Elaboración Propia.

En el diagrama propuesto se plasman los tres niveles de servicios que puede ofrecer un CERT, los cuales ya están estandarizados en la guía de ENISA (básico, intermedio, avanzado) , de igual forma se plasma el análisis que NIST recomienda realizar a las actividades de Ciberseguridad, resultados esperados y referencias aplicables de acuerdo a la estructura de la organización y los servicios que se desean prestar (Identificar, proteger, detectar, responder y recuperar); por último se propone el modelo de evaluación de ENISA para medir la madurez del CERT en cada uno de los niveles planteados (básico, intermedio, certificable).

Explicación parte 3: Los servicios ofertados por el CERT, dependen de su nivel de maduración y fueron tomados de las buenas prácticas y recomendaciones dadas por la Organización de Estados Americanos OEA y de la agencia europea de seguridad de las redes para la creación de CSIRT, estos niveles fueron mencionados en la sección "niveles de servicio" de la presente monografía. Sin embargo, se propone aplicar el método de identificación, análisis y evaluación de los servicios a partir de tres marcos de referencia como lo son NIST y ENISA, para lo cual se indica a continuación como contribuye cada una para lograr estos objetivos:

a) ENISA: como se mencionó en el marco de referencia del presente documento, en lo referente a las buenas prácticas en la implementación de un CERT para los servicios preventivos, reactivos, de manejo de instancias Gestión de la seguridad de la información que se pueden llegar a implementar por parte de este organismo nacional. Se tomaron como base y se realizó una división de acuerdo al objetivo que se buscaba en cada nivel de madurez, el cual iba a enfocado a:

- Nivel Básico: Reconocimiento del colCERT a nivel nacional y establecimiento de alianzas estratégicas o convenios.
- Nivel Intermedio: Afianzar los niveles de cooperación nacional e internacional en materia de Ciberdefensa, Ciberseguridad y delitos informáticos, así como mayor participación en las decisiones del Estado en la temática que abarca el CERT.
- Nivel Avanzado: Sostenibilidad propia de las capacidades del CERT (Agencia Europea de Seguridad de las Redes y de la Información, 2006).

b) NIST: los objetivos del marco de trabajo en su implementación en una organización podrían catalogarse en los siguientes puntos:

- Describir la postura actual de Ciberseguridad
- Describir el estado objetivo de Ciberseguridad
- Identificar y priorizar oportunidades de mejora en el contexto de un proceso continuo y repetible
- Evaluar el progreso hacia el estado objetivo
- Comunicación entre las partes interesadas internas y externas sobre el riesgo de Ciberseguridad (Acosta D. , 2017).

Para lo cual se emplean cinco actividades fundamentales:

- Identificar (Identify): Permite determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de Ciberseguridad que afectan este entorno.
- Proteger (Protect): Permite desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de Ciberseguridad.
- Detectar (Detect): Permite desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de Ciberseguridad a través de la monitorización continúa.
- Responder (Respond): Permite la definición y despliegue de actividades para reaccionar frente a un evento de Ciberseguridad identificado y mitigar su impacto.

- Recuperar (Recover): Permite el despliegue de actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente (Acosta D. E., 2016).

En lo que respecta a la forma de evaluar el nivel de madurez de un CERT, ENISA proporciona una guía que brinda una visión general completa sobre los parámetros a evaluar para medir el grado de madurez del modelo de gestión de incidentes en un CERT - CSIRT, lo que abarca las políticas, recursos humanos, herramientas para realizar la gestión de incidentes y procesos que soportan la misma. Además, dispone una herramienta de encuesta en línea para una autoevaluación de madurez, la cual se puede encontrar en https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey (ENISA, 2015 - 2019).

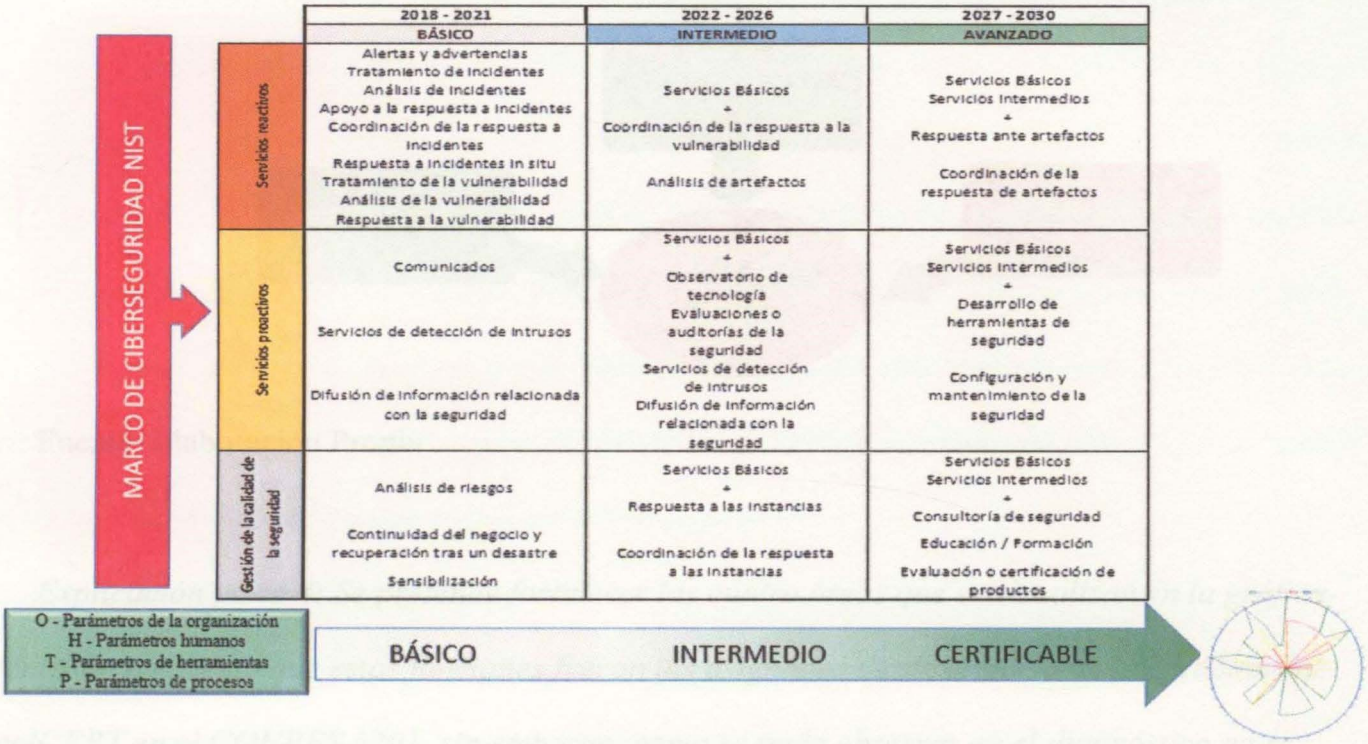
Es de anotar que con el modelo de evaluación que se adaptó inicialmente, de acuerdo a las recomendaciones del Centro Criptologico Nacional de España, se encontraron a nivel general los puntos de mejoramiento bajo los cuales debía ir enfocada la estrategia, pero con el modelo de evaluación de ENISA que se propone en este punto, el grupo colCERT puede realizar una evaluación más específica e identificar falencias de fondo de la organización, la cuales pueden ser asumidas a nivel interno del equipo de respuesta y de esta forma enfocar los esfuerzos para cada oportunidad de mejora.

Así pues, la evolución en la escala de maduración para los servicios propuestos en cada nivel (básico, intermedio, avanzado), se logrará establecer conforme sus capacidades en estructura,

personas, procesos y tecnologías se vayan estructurando y consolidando; para lo cual, se realizó el diseño del siguiente diagrama como una guía de manera que se integren todos los conceptos y metodologías que se han tratado, de tal forma que se aclaran los criterios propuestos en la presente monografía para el despliegue de las actividades a realizar en los periodos de tiempo establecidos (cuatrienios); encontrando:

- NIST como herramienta rectora en la identificación de los controles, políticas, procesos y procedimientos faltantes o aquellos por afianzar dentro de la actual operación y organización interna del colCERT. Esta se utilizará para formar una base operativa, normativa y de gestión de servicios sólida, en busca de fortalecer al grupo para la prestación de los diferentes servicios a sus clientes internos y externos de forma adecuada y eficaz.
- OEA y ENISA como entidades que, a través de su experiencia y conocimiento, han establecido una serie de criterios y lineamientos para establecer un CERT y los servicios que debería ofrecer.
- Finalmente, se toma la herramienta de ENISA para realizar la evaluación de la evolución de cada nivel de madurez, de tal forma que una vez se implementen los servicios dentro del CERT, se ejecute un análisis del nivel de cumplimiento de los parámetros de organización, Talento Humano, Herramientas y procesos implementados, con el fin de que cuando el resultado sea certificable se continúe al próximo nivel y por ende a la implementación de los servicios que hacen parte del mismo.

Ilustración 9. Diagrama propuesto para Medir el nivel de Madurez de los servicios del CERT.



Fuente. Elaboración Propia.

PARTE 4:

Despliegue de los objetivos especifico No 2 y 3: Establecer las líneas de acción para el cumplimiento de los niveles de madurez para cada una de las dimensiones del colCERT (coordinación, contacto y monitoreo) y Establecer criterios de evaluación para el grado de implementación y aseguramiento de las dimensiones para cada uno de los servicios clasificados de acuerdo con los niveles de madurez.

El objetivo dos está dividió en tres secciones que corresponden cada una de las dimensiones, cuyas iniciativas serán desarrolladas a continuación.

Ilustración 10. Focos para Fortalecer en el colCERT, Visión 2030

Fuente: Elaboración Propia

Explicación parte 4: Se pretende fortalecer las cuatro áreas que se visualizan en la gráfica, teniendo en cuenta que estas funciones fueron las asignadas desde el inicio de la creación del colCERT en el CONPES 3701, sin embargo, como se pudo observar en el diagnóstico no se encuentran totalmente desarrolladas debido a su baja cobertura a nivel nacional o a las falencias en infraestructura, recursos humanos o financieros.

Coordinación

Es la capacidad que va a tener el CERT de articular esfuerzos, tecnología y procesos a nivel nacional con el fin de prevenir, detectar, mitigar y responder ante incidentes cibernéticos a nivel Nacional; a nivel de coordinación se busca lograr los siguientes objetivos:

a. Desarrollo de capacidades propias o articulación de las capacidades de la empresa privada, entidades públicas y académicas, con facilidad y enfoque especializado en las capacidades que cada una desarrolla.

Explicación. De acuerdo con los niveles de madurez de los servicios y de acuerdo al análisis que se realice de los requerimientos (financieros y de infraestructura física o tecnológica) para implementar cada uno de ellos, se puede identificar la opción más viable y sostenible en el tiempo de tener una capacidad propia instalada en el CERT o realizar una alianza estratégica o convenio para dotar el equipo con el servicio requerido.

b. Creación de una red interdisciplinar para abarcar requerimientos técnicos, legales y operativos de la gestión de incidentes a nivel nacional.

Explicación: Si bien el CERT cuenta con herramientas tecnológicas y fuentes de información externas que permiten generar alertas tempranas en cuanto a amenazas cibernéticas, en el campo de la Ciberseguridad se requiere trabajar en conjunto y desde diferentes disciplinas para contrarrestar y mitigar estas amenazas en pro del beneficio común de la sociedad.

c. Liderar la ejecución de las actividades de los diferentes actores a nivel Colombia para la gestión de los incidentes y reporte de los mismos.

Explicación: El CERT necesita operar de una manera estructurada, gradual y estratégica durante las situaciones de crisis o que se presenten incidentes cibernéticos, de tal forma que se genere la articulación de acciones conjuntas entre los diversos grupos de interés y con el

liderazgo de una instancia con poder de decisión que represente la voluntad y las directrices del Estado.

Con el fin de evaluar la efectividad y la madurez del colCERT, en lo relacionado con la línea de coordinación y de acuerdo a lo propuesto por parte de la Organización de Estados Americanos y el BID en su documento *"Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe?"* (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2016), se propone contemplar los siguientes niveles de maduración de esta capacidad de la siguiente forma:

a) Como CERT a nivel nacional

✓ Inicial

No existe un centro de mando y control de la seguridad cibernética, o se está considerando crearlo a nivel nacional.

✓ Formativo

La función de mando y control está en manos, de manera informal, de la capacidad nacional de respuesta a incidentes o alguna otra entidad, sin una autoridad formal de coordinación.

✓ Establecido

Se identifica y existe una organización de mando y control, pero sin que haya recolección, procesamiento ni análisis automatizados; existe un mando y control ejecutivo oficial para el Ciberespacio como un asunto estratégico nacional; se cuenta con una visión general de las capacidades de seguridad actuales, pero sin conocimiento de la situación.

✓ Estratégico

Se ha establecido un centro de mando y control con automatización mejorada, proporcionando un conocimiento básico de la situación nacional; se hace la selección de objetivos del centro de mando y control como parte de la planeación de recursos y el desarrollo de políticas estratégicas.

- ✓ Dinámico

Hay un centro de mando y control de Ciberespacio nacional completamente desarrollado, que recibe y correlaciona la información de las organizaciones con la capacidad de respuesta a incidentes, organizaciones públicas/privadas, los LSP ("Layered Service Providers" en inglés), la infraestructura crítica de la información, organizaciones de defensa e inteligencia, y que está altamente automatizado, lo que proporciona conocimiento avanzado de la situación; el conocimiento de la situación activa está coordinado con la oficina ejecutiva nacional.

b. Como organismo central a nivel nacional en la atención de incidentes informáticos

- ✓ Inicial

La responsabilidad de la respuesta a incidentes puede haber sido asignada, o no, de manera informal a un miembro del personal dentro de cada agencia y ministerio del gobierno.

- ✓ Formativo

Se han identificado y publicitado directores de incidentes en cada agencia y ministerio a nivel nacional; los canales de comunicación entre estos directores siguen siendo ad hoc e incoherentes.

- ✓ Establecido

Se ha establecido y publicado una respuesta nacional a incidentes coordinada, con procesos claros y funciones y responsabilidades definidas; se preparan líneas de comunicación para situaciones de crisis.

- ✓ Estratégico

Ahora las capacidades técnicas van más allá de la coordinación de la respuesta e incluyen análisis de incidentes y apoyo; se establecen servicios proactivos y servicios de gestión de calidad de la seguridad en las organizaciones subnacionales y sectoriales.

- ✓ Dinámico

La respuesta a incidentes se adapta al entorno de amenazas; la coordinación nacional de varios niveles entre todos los niveles y sectores es fundamental para la respuesta a incidentes; existe coordinación entre las organizaciones regionales e internacionales de respuesta a incidentes.

Por otra parte, se debe tener en cuenta que esta capacidad debe identificar, establecer y mantener mecanismos y criterios de intercambio de información que permitan el intercambio de herramientas, conocimiento y/o información para la acción entre los gobiernos, academia y los sectores industriales. De esta forma se logrará fomentar la coordinación en la respuesta a incidentes, facilitar el intercambio en tiempo real de información de amenazas e inteligencia, y ayudar a mejorar la comprensión de cómo los sectores se convierten en objetivo, qué información se pierde y qué métodos se puede utilizar para defender los activos de información. Han surgido al menos cuatro modelos diferentes de intercambio de información para abordar las amenazas cibernéticas y para ayudar a las entidades a asegurar sus activos de información a saber: un modelo (1) impulsado por el gobierno; (2) impulsado por la industria; (3) impulsado por una asociación sin fines de lucro; e (4) impulsado por una asociación híbrida académica, gubernamental, y de la industria.

Monitoreo

Es la capacidad que va a tener el CERT de anticipar la materialización de un riesgo que puede generar un impacto considerable a nivel de las infraestructuras críticas de la nación. Este es el servicio más básico que debe ofrecer este organismo, conlleva la implementación de herramientas, mecanismos o sistemas que ayuden a detectar eventos de seguridad, y a su vez obtener la trazabilidad de sus eventos a través de la correlación los mismos, obteniendo informes de forma efectiva; de igual forma implica la utilización de herramientas de escaneo y búsqueda de vulnerabilidades en la red de clientes atendidos.

En este sentido, esta capacidad puede ser desarrollada desde dos puntos de vista, la implementación de sistemas o herramientas propias o el uso de sensores de propiedad de terceros o de tipo de fuente abierta.

De acuerdo a lo anterior, este monitoreo se puede dividir en dos partes:

a) Servicios de monitoreo de infraestructuras tecnológicas y alertas a nivel externo e interno, los cuales van a permitir generar reportes y alertas de seguridad para todos los clientes atendidos a nivel nacional.

Explicación: Al tener un contexto de lo que pasa o se manifiesta alrededor de las diferentes infraestructuras tecnológicas de las entidades e incluso de los Proveedores de servicios de Internet, se logra una capacidad de detección y comportamiento de amenazas que permite al CERT la generación de estrategias y tácticas coordinadas para el fortalecimiento de la Ciberdefensa nacional.

b) Servicios de monitoreo de tecnología, escaneo de vulnerabilidades y artefactos maliciosos que permitan reforzar la investigación y desarrollo en el CERT.

Explicación: con la generación de capacidades de análisis para nuevas Amenazas Persistentes Avanzadas - APT, se logran consolidar servicios que pueden ser ofrecidos no solo a nivel nacional sino internacional, lo cual da origen a nuevas oportunidades de negocio que permiten ingresos para la sostenibilidad del CERT.

A nivel de monitoreo se busca lograr los siguientes objetivos:

- Identificación de tendencias tecnológicas relacionadas con nuevas amenazas.
- Producción de información que permita generar iniciativas de monitoreo y alerta que apalanque y soporte la toma de decisiones estratégicas y mejore procesos de atención y gestión de incidentes
- Monitoreo en activo y en profundidad que permita detectar vulnerabilidades o amenazas de forma temprana para disminuir el riesgo de impactar la continuidad del negocio en cada uno de los clientes atendidos.
- Generación de alertas tempranas a través de boletines, anuncios, directrices o recomendaciones para prevenir o mitigar brechas de seguridad a mediano o largo plazo.
- Generación de lecciones aprendidas que permitan mejorar tiempos de respuesta, metodología y protocolo de atención de incidentes.

Contacto

Es la capacidad que va a tener el CERT de brindar y establecer los canales y protocolos necesarios para atender y reportar la gestión de incidentes cibernéticos a nivel Nacional; a nivel de contacto se busca lograr los siguientes objetivos:

a) Servir como punto central de contacto para la colaboración nacional e internacional en la atención y respuesta ante incidentes cibernéticos, así como en el liderazgo en temas de Ciberseguridad y Ciberdefensa a nivel nacional.

Explicación: El ser el punto central de contacto a nivel nacional e internacional, da al colCERT un nivel de control, trazabilidad y coordinación más sólido y eficiente de la estrategia de Ciberseguridad y Ciberdefensa del Estado colombiano.

b) Crear un repositorio de información de incidentes, un organismo especializado en el análisis de incidentes y un coordinador de respuesta a incidentes a nivel nacional.

Explicación: Con el repositorio de información de incidentes se logra tener una base de conocimiento ante el comportamiento de amenazas detectadas, lo cual permite disminuir el tiempo de respuesta ante incidentes que guarden características comunes y que puedan llegar afectar infraestructuras críticas de la nación.

c) Establecimiento del protocolo de escalamiento y reporte de incidentes, ante los diferentes organismos de Ciberseguridad y Ciberdefensa a nivel nacional.

Explicación: La definición de este protocolo permite establecer reglas y niveles de autoridad e intervención, por parte de los diferentes actores dentro del modelo de Ciberseguridad y Ciberdefensa que lidera y coordina el colCERT.

En la estrategia de Ciberseguridad y Ciberdefensa nacional, el CERT dentro de su función de coordinación para los incidentes informáticos debe realizar la clasificación de la información como punto único de contacto, para lo cual se establecen unos canales de comunicación con los usuarios a atender donde se les define un protocolo a través del cual se especifica los servicios que se brindarán, horario de operación y pautas sobre cómo y qué se debe informar. Adicionalmente se encuentran disponibles informes y referencias en línea para ayudar a todos sus usuarios en este reporte y como tomar contacto con el CERT nacional.

De acuerdo a lo anterior, el CERT debe crear un mecanismo de distribución de alertas y buenas prácticas de seguridad actuando como un facilitador o un punto de contacto principal para reunir a estas diversas organizaciones y a su vez actuar como un punto principal de distribución para replicar las estrategias de mitigación a una comunidad especifica o general que así lo requiera. Esto permite que el equipo sirva como un repositorio de información sobre incidentes, un centro para el análisis de incidentes y un coordinador de respuesta a incidentes a nivel nacional o internacional.

Con el fin de evaluar la efectividad y de madurez del colCERT en lo relacionado en la línea de contacto y de acuerdo a lo propuesto por parte de la Organización de Estados Americanos y el BID en su documento *"Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe?"*,

se propone contemplar los siguientes niveles de maduración de esta capacidad de la siguiente forma:

- ✓ Inicial

No se reconoce la necesidad de una política de divulgación responsable en las organizaciones del sector público y privado.

- ✓ Formativo

Está vigente un marco de divulgación de vulnerabilidades, lo que incluye un plazo de divulgación, una resolución prevista y un informe de reconocimiento; se demuestra cierta capacidad de compartir detalles técnicos de la vulnerabilidad con otras partes interesadas que pueden distribuir la información de manera más amplia, a través de mayor cooperación público-privada.

- ✓ Establecido

Las organizaciones han desarrollado la capacidad de recibir y difundir información sobre la vulnerabilidad; proveedores de servicios y de software aceptan los informes de error y de vulnerabilidad y los abordan y se comprometen informalmente a abstenerse de adelantar acciones legales en contra de una parte que revela información responsablemente.

- ✓ Estratégico

Se publica un análisis de los detalles técnicos de la vulnerabilidad y se difunde información de asesoramiento de acuerdo a las funciones y responsabilidades; se establecen procesos de divulgación responsable de vulnerabilidades, incluidos los plazos para todos los interesados implicados (proveedores de productos, clientes, proveedores de seguridad y público); puede

haber regulaciones para ordenar reportes de vulnerabilidades por parte de los operadores y propietarios de infraestructuras críticas.

- ✓ Dinámico

Las políticas de divulgación responsable son revisadas y actualizadas de forma continua en base a las necesidades de los grupos de interés afectados; los mecanismos de divulgación responsable se sincronizan a nivel internacional; los procesos nacionales e internacionales para la revisión y la reducción de los plazos se encuentran en operación.

Financiamiento

Para efectos del cumplimiento de los objetivos de esta estrategia, y teniendo en cuenta el histórico de asignación de recursos para el tema de Ciberseguridad y Ciberdefensa dispuesto en los documentos CONPES 3701 y CONPES 3854, así como el histórico de contrataciones estatales expuesto en el portal de contratación de SECOP II del Estado Colombiano, se propone solicitar la asignación del mismo presupuesto relacionado en el CONPES 3854, con la siguiente distribución:

Tabla 23

Presupuesto Planteado para desarrollo de la estrategia

	2018 - 2021	2022 - 2026	2027 - 2030
	BÁSICO	INTERMEDIO	AVANZADO
HERRAMIENTAS TECNOLÓGICAS	4.392	2.583	2.782
CAPACITACIÓN	2.000	3.000	3.000
PERSONAL	1.000	2.000	2.000
TOTAL	**7.392**	**7.583**	**7.782**

Fuente: Elaboración propia

Es pertinente indicar, que la distribución de los recursos a nivel de herramientas tecnológicas obedece a la adquisición de nuevas herramientas para educación, integración de bases de datos, análisis de malware, sensores de Detección de Intrusos, entre otros, a su vez, se contempla el sostenimiento de su operación durante los periodos de desarrollo de la estrategia; para lo concerniente a la capacitación, se propone especializar a los funcionarios en capacidades específicas como análisis de malware, Computer Hacking Forensic Investigator-CHFI, Certified Ethical Hacker- CEH, auditor ISO 27001, Certified Security Analyst –ECSA, Security Specialist –ECSS, Administración en continuidad de Negocios BCLS2000 + CBCP, entre otros que desarrollen las competencias necesarias para ofrecer los servicios de cada nivel de madurez. Finalmente, para lo relacionado con la planta de personal, se propone la contratación de personal experto en modelamiento y análisis matemático, Administración de sistemas Linux y Unix, Ingenieros de Software.

PARTE 5:

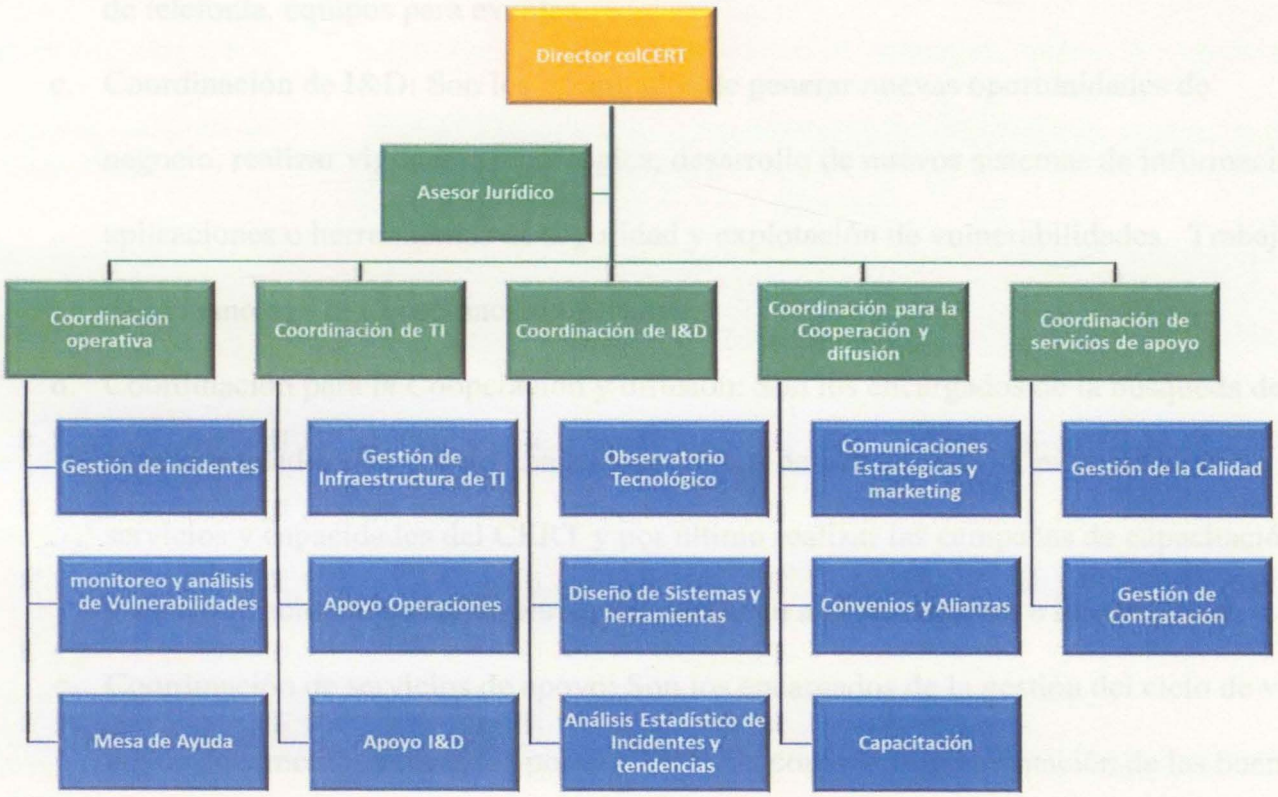
Despliegue del objetivo específico No 4: Proponer una estructura organizacional interna para el colCERT para la prestación de los diferentes servicios ofrecidos por el equipo de respuesta en su último nivel de madurez.

Es la estructura organizativa que debe adoptar el colCERT para gestionar y cumplir con los requerimientos del grupo de clientes atendido con unos Acuerdos de Nivel de Servicio (ANS) acordes a sus necesidades, así como la posibilidad de generar nuevas oportunidades de negocio

para el equipo o simplemente establecer alianzas estratégicas que permitan la consecución de las actividades propuestas para el cumplimiento de los objetivos trazados al 2030.

Para elaborar la propuesta de estructura operativa del CERT se tuvo en cuenta las recomendaciones y criterios establecidos en el documento de "Buenas Prácticas para establecer un CSIRT nacional" de la OEA, también el documento "Como crear un CSIRT PASO A PASO" de ENISA y la "GUÍA DE CREACIÓN DE UN CERT / CSIRT" del CCN – CERT, para proponer una estructura operativa que se adapte a las necesidades del colCERT para la prestación y correcto despliegue de los servicios en el nivel básico, intermedio y avanzado.

Ilustración 11. Propuesta de Estructura Operativa a implementar en el colCERT



Fuente: Elaboración Propia con recomendaciones de OEA, ENISA y CCN CERT

En la anterior estructura se pueden observar 5 roles principales y un asesor jurídico que orientan y apoyan a la alta dirección en temas administrativas, comerciales y de prestación de servicios. De esta forma, se busca que cada rol cumpla con las siguientes funciones a nivel general:

a. Coordinación operativa: Realiza todo el ciclo de atención de los incidentes de seguridad, desde la atención del usuario final y posterior categorización, correlación, priorización, asignación, análisis, solución y seguimiento de los incidentes de seguridad que llegan al CERT.
b. Coordinación de TI: Realiza el apoyo, administración y soporte técnico y operativo a todos los servicios internos del CERT, mantenimiento de equipos de cómputo, mantenimiento del centro de datos, página Web, correo electrónico, intranet, sistema de telefonía, equipos para eventos.
c. Coordinación de I&D: Son los encargados de generar nuevas oportunidades de negocio, realizar vigilancia tecnológica, desarrollo de nuevos sistemas de información, aplicaciones o herramientas de seguridad y explotación de vulnerabilidades. Trabaja de la mano con el Coordinación operativa.
d. Coordinación para la Cooperación y difusión: Son los encargados de la búsqueda de nuevas unidades de negocio, manejo de medios de comunicación, publicidad de los servicios y capacidades del CERT y por último realizar las campañas de capacitación y sensibilización a las entidades que lo requieran a nivel nacional e internacional.
e. Coordinación de servicios de apoyo: Son los encargados de la gestión del ciclo de vida de los documentos generados por el CERT, así como la implementación de las buenas prácticas de las normas de calidad (ISO 9001), Seguridad de la Información (ISO

27001), Continuidad (22301) y Gestión de Incidentes (27035). De igual forma es el grupo que realiza la gestión de la contratación de bienes y servicios para el grupo.

De acuerdo a lo anterior y teniendo en cuenta los diferentes servicios que se quieren consolidar o implementar en el CERT de Colombia, se sugiere la distribución de estos servicios para cada rol de la siguiente forma:

Tabla 14.
Distribución de servicios de acuerdo a roles propuestos

ROL	SERVICIO O ACTIVIDAD A EJECUTAR
Asesor Jurídico	Apoyo administrativo
	Coordinación Operativa
Gestión de Incidentes	Tratamiento de incidentes, Análisis de incidentes, Apoyo a la respuesta a incidentes, Respuesta a incidentes in situ
Monitoreo y Análisis de Vulnerabilidades	Alertas y advertencias, Tratamiento de la vulnerabilidad, Análisis de la vulnerabilidad, Respuesta a la vulnerabilidad, Servicios de detección de intrusos
Mesa de Ayuda	Coordinación de la respuesta a incidentes, Coordinación de la respuesta a la vulnerabilidad
	Coordinación de TI
Gestión de Infraestructura de TI	Configuración y mantenimiento de la seguridad
Apoyo Operaciones	Análisis de artefactos, Análisis de Instancias, Respuesta a las instancias, Respuesta ante artefactos
Apoyo I&D	Coordinación de la respuesta a las instancias, Coordinación de la respuesta de artefactos
	Coordinación de I&D
Observatorio Tecnológico	Observatorio de tecnología
Diseño de Sistemas y herramientas	Desarrollo de herramientas de seguridad
Análisis Estadístico de Incidentes y tendencias	Apoyo en el análisis de tendencias y correlación de eventos
	Coordinación para la Cooperación y difusión

Comunicaciones Estratégicas y Marketing	Comunicados, Difusión de información relacionada con la seguridad
Convenios y Alianzas	Análisis de riesgos, Continuidad del negocio y recuperación tras un desastre, Servicios de detección de intrusos, Consultoría de seguridad
Capacitación	Sensibilización, Educación / Formación
	Coordinación de Servicios de Apoyo
Gestión de la Calidad	Evaluaciones o auditorías de la seguridad, Evaluación o certificación de productos, Apoyo administrativo
Gestión de Contratación	Apoyo administrativo

Fuente: Elaboración Propia.

Seguimiento y evaluación de resultados

Para el cumplimiento de estos hitos es importante tener unos indicadores o focos de evaluación de la estrategia, los cuales pueden plantearse a partir del asentamiento de las siguientes capacidades o mecanismos a nivel organizacional:

1. Capacidades técnicas y administrativas requeridas para la efectiva y holística coordinación de las iniciativas de prevención, respuesta y recuperación de incidentes cibernéticos.
2. Mecanismos de gobernanza implementados que promuevan el reconocimiento de los servicios prestados y a su vez que faciliten la cooperación en la red y el desarrollo, empleo y fortalecimiento armónico y conjunto de los miembros que hacen parte de la estructura de Ciberseguridad y Ciberdefensa del País.
3. Mecanismos de sostenibilidad adquiridos por el colCERT para garantizar la prestación de los servicios en Ciberdefensa y Ciberseguridad a sus clientes.

Explicación: Se proponen estas tres capacidades a nivel organizacional, teniendo en cuenta que Países que son potencia en materia de Ciberseguridad y Ciberdefensa como lo es Estados Unidos, según el estudio realizado por Javier Candau, Instituto Español de Estudios Estratégicos, (2011), centra sus esfuerzos en 5 aspectos principales a saber:

1. *Sistema de respuesta nacional de seguridad en el Ciberespacio.*
2. *Programa de reducción de amenazas y vulnerabilidades.*
3. *Formación y concienciación en el Ciberespacio.*
4. *Asegurar el Ciberespacio gubernamental.*
5. *Cooperación nacional e internacional (*Aguilar, 2011).

Lo que lleva a que se proponga el desarrollo de estas tres características en Colombia.

Conclusiones

1. El desarrollar el presente trabajo, permitió identificar que el grupo colCERT ha establecido desde 2011 una serie de estrategias, planes y programas para contrarrestar las diferentes amenazas cibernéticas que han surgido con el paso de los años, como producto de ello, han establecido algunas alianzas estratégicas y han logrado implementar una serie de herramientas tecnológicas para la detección, mitigación y contención de ataques, como lo son Firewall, HoneyPot, Sandbox, correlacionador de eventos, entre otras, sin embargo, se aconseja realizar una evaluación a las políticas que el CERT nacional tiene implementadas, ya que estas directrices deben definir el alcance de la organización y apalancar los recursos político-administrativos que apoyen la difusión y mantenimiento de los servicios que se ofrecen y ofrecerán.

2. A través del diagnóstico realizado a las capacidades de nivel estratégico, de servicios y herramientas implementadas en el colCERT y al compararlas con los lineamientos internacionales de OEA, ENISA y NIST para el establecimiento de un CERT, se logra identificar que la metodología de OEA permitirá estructurar y fortalecer las capacidades de gestión de incidentes y organización interna para el mejoramiento de la calidad y cobertura de los servicios a nivel nacional. Adicionalmente en el diagnóstico, se ha identificado la necesidad de contar con recursos adicionales para mantener el CERT, estos recursos pueden ser producto de la retribución económica por la prestación de algunos de sus servicios al público en general, con lo que se lograría una sostenibilidad y optimización de los recursos, también se aconseja realizar un análisis de capacidades en

ciberdefensa y ciberseguridad, en los diferentes sectores económicos para establecer convenios o alianzas estratégicas, que coadyuven con la sostenibilidad y ampliación de los servicios prestados por el equipo de respuesta.

De igual forma, a través de la metodología de NIST, ENISA y CCN –CERT, se logran identificar oportunidades de mejora y brechas de seguridad en cuanto al Grado de autoridad sobre los clientes atendidos, catálogo de servicios y promoción de sus capacidades a nivel nacional e internacional, también se identifica la necesidad de crear algunos roles para asignar funciones específicas, que generen mayor valor al grupo en su objetivo de lograr posicionar al CERT como la instancia de coordinación nacional e internacional definida mediante CONPES 3701.

3. Se recomienda al colCERT implementar la estrategia presentada en este documento, la cual está enfocada en recomendar un modelo de identificación, análisis y evaluación de los procesos y servicios del grupo colCERT, basado en las metodologías de ENISA, OEA y NIST, para fortalecer y/o generar capacidades operacionales que permitan mejorar la imagen, credibilidad y confianza del grupo a nivel directivo y nacional. Lo anterior, a través de la implementación de los controles propuestos, capacidades de respuesta y atención de incidentes, análisis de información y correlación de eventos que apalanquen la Ciberseguridad y Ciberdefensa en Colombia.

Por otra parte, a través de NIST, se podrán identificar las oportunidades de mejora a los servicios que actualmente se ofrecen por parte del CERT a sus clientes, de igual forma, al

integrar el modelo de evaluación de ENISA, se logrará medir el grado de maduración de los servicios en cada uno de los niveles propuestos (Básico, Intermedio, Avanzado, para lograr impactar tres ejes de consolidación del CERT que son: reconocimiento, talento humano, infraestructura y asignación de recursos. Estos se constituirán en la base estratégica bajo la cual se logre fortalecer la parte operativa, gerencial y de imagen institucional para el CERT nacional.

Adicionalmente, con el fin de generar una fuente de ingreso adicional que afiance la sostenibilidad en el tiempo del CERT, se debe evaluar con el grupo legal del Ministerio de Defensa Nacional, la figura jurídica que permita al equipo de respuesta la compensación económica de algunos de los servicios ofertados a sus clientes finales, generación de alianzas estratégicas con universidades o empresas privadas cumpliendo a su vez con la normatividad colombiana.

4. Un punto fundamental dentro de la estrategia de fortalecimiento del colCERT, es el ajuste de la estructura operacional del mismo, con lo que se recomienda se implementen los roles propuestos, los cuales irán acompañados de herramientas tecnológicas de acuerdo al tipo de servicio a cubrir y a los estándares de la industria para cada especialidad, como por ejemplo análisis de malware, análisis de vulnerabilidades e informática forense. Por esto, se propone una estructura operativa con la asignación de una serie de servicios para cada rol, lo que generará una especialización en la ejecución de las actividades y funciones, logrando una mejor calidad de los servicios y un reconocimiento favorable ante los clientes internos y externos.

Bibliografía

Acosta, D. (11 de Enero de 2017). *Deacosta.com*. Obtenido de https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/

Acosta, D. E. (23 de 12 de 2016). *ISEC Auditors*. Obtenido de https://blog.isecauditors.com/2016/12/guia-rapida-para-entender-marco-trabajo-de-ciberseguridad-del-NIST.html

Agencia Europea de Seguridad de las Redes y de la Información. (22 de Diciembre de 2006). *cómo crear un CSIRT paso paso*. Obtenido de ENISA: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish

Agencia Europea de Seguridad de las Redes y de la Información. (22 de Diciembre de 2006). *enisa.europa.eu*. Obtenido de ENISA: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish

Agencia Europea de Seguridad de las Redes y de la Información. (2015 - 2019). *enisa.europa.eu*. Obtenido de https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Ágreda, Á. G. (21 de 02 de 2012). *IEEE.es*. Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO17_CiberespacioConflicto_Agreda.pdf

Aguilar, L. J. (21 de Febrero de 2011). *ieee.es*. Obtenido de http://www.ieee.es/en/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html

Arreola, A. (2016). Ciberespacio, el campo de batalla de la era tecnológica. *Revista cientifica ESDEGUE*.

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. (2016). *digital-iadb.leadpages.co*. Obtenido de https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

Bejarano, M. J. (12 de 2010). *IEEE.* Obtenido de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Campos, L. M. (16 de Octubre de 2015). *cefadigital.edu.ar.* Obtenido de http://www.cefadigital.edu.ar/bitstream/123456789/462/1/TFI%20ECS%202015%20Q5C1E4_61.pdf

Carrillo, M. R. (17 de 11 de 2015). *IEEE.* Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-CIberseguridad_Margarita-Robles.pdf

Castañeda, C. (10 de 02 de 2018). *El costo financiero de los ciberataques está al alza*. Obtenido de larepublica: https://www.larepublica.co/internet-economy/el-costo-financiero-de-los-ciberataques-esta-al-alza-2598128

Centro Criptológico Nacional de España. (Septiembre de 2011). *CCN-CERT Centro Criptológico Nacional*. Obtenido de 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-sep11.pdf

Ministerio de Comunicaciones Republica de Colombia, M. d. (2008). Obtenido de http://www.vive.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/3._Diseno_de_un_CSIRT_Colombiano.pdf

Consejo Nacional de Política Económica y Social (CONPES 3701). (14 de Julio de 2011). *MINTIC.* Obtenido de MINTIC: https://mintic.gov.co/portal/604/w3-article-3510.html

Consejo Nacional de Política Económica y Social, República de Colombia. (11 de 04 de 2016). *colaboracion.dnp.gov.co.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Dávila Newman, G. (2006). *El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y.* Libertador: Revista Laurus.

ESPAÑA, CONSEJO NACIONAL DE CIBERSEGURIDAD. (9 de Enero de 2019). *Ministerio del Interior España*. Obtenido de Sitio Web del Ministerio del interior de España: http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf/19676087-0253-4c58-bbb0-2fc58a5fd63b

Fojón, E., & Sanz, V. Á. (2010). Ciberseguridad en España: una propuesta para su gestión . *Real Instituto Elcano*, 1-8.

Folgueiras, P. (30 de 05 de 2016). *Diposit Digital de la Universidad de Barcelona.* Obtenido de http://diposit.ub.edu/dspace/bitstream/2445/99003/1/entrevista%20pf.pdf

Gaitán, R. A. (8 de Junio de 2012). *La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las tic en la guerra regular.* Obtenido de Revista Estudios en Seguridad y Defensa: https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/194/279

García, C. (. (22 de Septiembre de 2016). *Revista Militar digital.* Obtenido de Revista Militar digital: https://dialogo-americas.com/es/articles/cyberdefense-and-cybersecurity-colombia

Jordan, J. (2013). Manual de Estudios Estratégicos y Seguridad Internacional. En J. Jordan, *Manual de Estudios Estratégicos y Seguridad Internacional* (págs. 329-348). Granada: Plaza y Valdés.

Comité Interministerial sobre Ciberseguridad,. (marzo de 2015).. Obtenido de http://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

Mateus, J. M. (12 de Septiembre de 2014). *IEEE*. Obtenido de Instituto español de Estudios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO100-2014_Globalizacion-CIberseguridad-Estrategia_JMMolinaMateos.pdf

Mcafee. (09 de 2017). *mcafee*. Obtenido de https://www.mcafee.com/enterprise/es-es/assets/reports/rp-quarterly-threats-sept-2017.pdf

Monterrosa, H. (03 de 02 de 2018). *La Republica*. Obtenido de https://www.larepublica.co/internet-economy/mas-de-60-de-los-colombianos-son-internautas-2595957

Muñoz, M. (28 de 3 de 2015). *Revista Iberica de Sistemas y tecnologias de la información.* Obtenido de http://www.scielo.mec.pt/pdf/rist/nspe3/nspe3a02.pdf

Nacional, C. S. (02 de 2012). *Subdirección General de Publicaciones y Patrimonio Cultural.* Obtenido de https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

OEA. (23 de Noviembre de 2001). *Convenio sobre la Ciberdelincuencia.* Obtenido de Organization of American States: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Organización de Estados Americanos - OEA. (Abril de 2016). *Buenas Prácticas para establecer un CSIRT nacional*. Obtenido de OAS : https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Policía Nacional. (24 de Julio de 2018). *caivirtual.policia.gov.co*. Obtenido de caivirtual: https://caivirtual.policia.gov.co/

Proyecto Diseño de modelo SGSI para la estrategia de Gobierno en Línea. (04 de 12 de 2008). *vive.gobiernoenlinea.gov.co.* Obtenido de www.vive.gobiernoenlinea.gov.co/apc-aa.../3._Diseno_de_un_CSIRT_Colombiano.doc

Pública, S. d. (marzo de 2015). *Comité Interministerial sobre Ciberseguridad.* Obtenido de http://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

Rodríguez Jiménez, A., & Pérez Jacinto, A. (2017). Métodos científicos de indagación y de construcción del conocimiento . *esc.adm.neg. No. 82*, 22.

Social, C. N. (14 de 07 de 2011). *Ministerio de Tecnologías de la Información y las Comunicaciones*. Obtenido de MIntic: https://mintic.gov.co/portal/604/articles-3510_documento.pdf

Tecnosfera. (31 de 07 de 2018). *El tiempo*. Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cifras-sobre-telecomunicaciones-e-internet-en-colombia-2017-250026

Uzal, R. (Noviembre de 2012). *cefadigital.* Obtenido de cefadigital: http://www.cefadigital.edu.ar/bitstream/123456789/57/1/VC%207-2012%20UZAL.pdf

Vargas, E. M. (2014). *Universidad Militar Nueva Granada.* Obtenido de https://repository.unimilitar.edu.co/bitstream/10654/12259/1/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf

Vicente, A. L. (09 de 2011). *Academia.edu.* Obtenido de http://www.academia.edu/6182513/La_Ciberguerra_la_guerra_inexistente

ACCENTURE. (Enero de 2018). Costo de estudio del crimen cibernético 2017. Obtenido de: https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017