

**DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS
A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN
NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN**



LUZ JENNY GONZÁLEZ PEÑA. CÓDIGO: 100160524
CESAR AUGUSTO MONROY ROJAS. CÓDIGO: 100194478

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
MAESTRÍA EN GERENCIA DE PROYECTOS
BOGOTÁ D. C., COLOMBIA
2024

**DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE
RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE
EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN**



**LUZ JENNY GONZÁLEZ PEÑA. CÓDIGO: 100160524
CESAR AUGUSTO MONROY ROJAS. CÓDIGO: 100194478**

**TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE MAGÍSTER EN GERENCIA
DE PROYECTOS**

DIRECTOR: SEBASTIÁN ALBERTO PELÁEZ GÓMEZ

**INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
MAESTRÍA EN GERENCIA DE PROYECTOS
BOGOTÁ D. C.
Junio de 2024**

TABLA DE CONTENIDO

RESUMEN.....	8
INTRODUCCIÓN	10
1. TÍTULO DE LA PROPUESTA	13
2. PLANTEAMIENTO DEL PROBLEMA.....	14
2.1. Formulación del Problema	16
3. OBJETIVOS.....	17
3.1. Objetivo General	17
3.2. Objetivos Específicos	17
4. JUSTIFICACIÓN.....	18
5. MARCO REFERENCIAL	20
5.1. Marco Conceptual y Teórico.....	20
5.1.1. <i>Incidentes de Seguridad Informática 2023 en Colombia</i>	21
5.1.2. <i>Tipos de Incidentes 2023</i>	24
5.1.3. <i>Incidentes Específicos en Entes y Organizaciones del Sector Público de Colombia 2021 – 2024</i>	25
5.1.4. <i>Política y Estrategia de Seguridad Cibernética: 2016 - 2020</i>	26
5.1.5. <i>Modelos para el Manejo de Riesgos</i>	29
5.1.5.1. COBIT.....	29
5.1.5.2. ITIL (Biblioteca de Infraestructura de Tecnologías de Información).....	30
5.1.5.3. ISO 27001.	30
5.1.5.4. CSIRT.....	30
5.1.6. <i>Servicios de un CSIRT</i>	32
5.1.7. <i>Ámbitos de un CSIRT</i>	32
5.2. Marco Tecnológico	33
5.2.1. <i>RTIR</i>	33
5.2.2. <i>Herramientas CRM</i>	33
5.2.3. <i>Herramientas para Verificación de la Información</i>	34
5.2.4. <i>Herramientas de Encriptación</i>	34
5.2.5. <i>Herramientas de Obtención de Datos Volátiles de Memoria</i>	34
5.2.6. <i>Kali Linux</i>	34
5.3. Marco Legal	35
5.3.1. <i>Contexto Regulatorio</i>	35
5.3.2. <i>Ley 527 de 1999</i>	35
5.3.3. <i>Ley 594 de 2000</i>	35

5.3.4.	<i>Ley 679 de 2001</i>	36
5.3.5.	<i>Ley 962 de 2005</i>	36
5.3.6.	<i>Ley 1150 de 2007</i>	36
5.3.7.	<i>Ley 1273 de 2009</i>	36
5.3.8.	<i>Ley 1341 de 2009</i>	36
5.3.9.	<i>CONPES 3701 de 2011</i>	37
5.3.10.	<i>Ley 1437 de 2011</i>	37
5.3.11.	<i>Ley 1480 de 2011</i>	37
5.3.12.	<i>Decreto Ley 019 de 2012</i>	37
5.3.13.	<i>Ley 1581 de 2012</i>	38
5.3.14.	<i>Ley 1712 de 2014</i>	38
5.3.15.	<i>Resolución 8934 de 2014</i>	38
6.	METODOLOGÍA	39
6.1.	Fase I: Simplificación de la Información	39
6.2.	Fase II: Estructuración de los Servicios del CSIRT	40
6.3.	Fase III: Estructura Orgánica del CSIRT	40
6.4.	Fase IV: Políticas y procedimientos operacionales del CSIRT.....	40
7.	CRONOGRAMA	41
8.	DESARROLLO DE LA INVESTIGACIÓN	42
8.1.	Fase I: Simplificación de la Información	42
8.1.1.	<i>Descripción del Modelo SIM3</i>	42
8.1.2.	<i>Premisas Básicas</i>	45
8.1.3.	<i>Equipo Evaluador</i>	45
8.1.4.	<i>Organización</i>	47
8.1.5.	<i>Recursos Humanos</i>	47
8.1.6.	<i>Herramientas</i>	47
8.1.7.	<i>Procesos</i>	48
8.1.8.	<i>Resultados</i>	48
8.2.	Fase II: Definir el Catálogo de Servicios del CSIRT para el Ministerio de Educación Nacional y el Sector Educación	50
8.2.1.	<i>Servicios Proactivos:</i>	50
8.2.2.	<i>Servicios Reactivos</i>	52
8.3.	Fase III: Establecer la Estructura Organizacional y Perfiles que Integran el CSIRT para el Ministerio de Educación Nacional y el Sector Educación	53
8.3.1.	<i>Horarios Iniciales de Atención</i>	59

8.3.2.	<i>Autoridad</i>	59
8.3.3.	<i>Responsabilidad</i>	59
8.3.4.	<i>Dimensionamiento del CSIRT</i>	60
8.4.	Fase IV: Documentar las Políticas y Procedimientos Operacionales para la Puesta en Funcionamiento del CSIRT del Ministerio de Educación Nacional y el Sector Educación	64
8.4.1.	<i>Misión</i>	64
8.4.2.	<i>Visión</i>	64
8.4.3.	<i>Comunidad Objetivo</i>	64
8.4.4.	<i>Políticas y Procedimientos</i>	65
8.4.4.1.	Política de Clasificación de Información.	65
8.4.4.2.	Política de Divulgación de Información.....	65
8.4.4.3.	Política de Gestión de Incidentes.	65
8.4.4.4.	Procedimiento de Gestión de Incidentes.	65
8.4.4.5.	Política de Seguridad de Datos y Protección de Datos.	65
8.4.4.6.	Procedimientos de <i>Back Ups</i> y Respaldos de la Información.....	66
9.	REFERENCIAS	67
10.	ANEXOS.....	71
	Anexo 1. Entrevistas cuadrante Organización	71
	Anexo 2. Entrevistas cuadrante Recursos Humanos	82
	Anexo 3. Entrevistas cuadrante Herramientas	89
	Anexo 4. Entrevistas cuadrante Procesos.....	98

LISTA DE TABLAS

Tabla 1. Ciudades colombianas afectadas por ciberdelitos.....	23
Tabla 2. Ciberataques en Colombia.....	25
Tabla 3. Ámbitos de los CSIRT.....	32
Tabla 4. Parámetros de los cuadrantes.....	43
Tabla 5. Niveles de acción.....	45
Tabla 6. Equipo evaluador.....	46
Tabla 7. Organización CSIRT MEN y Sector Educación.....	53
Tabla 8. Perfiles y competencia recurso humano.....	54
Tabla 9. Dimensionamiento del CSIRT.....	60

LISTA DE FIGURAS

Figura 1. Tipo de CSIRT.....	20
Figura 2. Denuncia cibercrimitos en Colombia.....	21
Figura 3. Interceptación de datos informáticos 2022.....	23
Figura 4. Tipos de incidentes en Colombia.....	24
Figura 5. CSIRT Colombia en el grupo FIRST.....	27
Figura 6. Cronograma.....	41
Figura 7. Nivel de madurez del MEN para implementación de CSIRT.....	49

RESUMEN

El desarrollo de actividades económicas, educativas, culturales y recreativas, entre otras, se afianza cada vez más en el uso de las Tecnologías de la Información y las Comunicaciones TIC alrededor de todo el mundo. Es así como este contexto posibilita nuevos modelos de economía y formas de interacción, pero a su vez propicia la aparición de amenazas cibernéticas que se traducen en la existencia de un riesgo latente de materialización de ataques cibernéticos que pueden ocasionar una grave afectación en todos los niveles de la sociedad mundial. El presente estudio propone la estructuración de un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) para el Ministerio de Educación Nacional y el sector Educación de Colombia, contemplando la incorporación de todos los elementos que brinda la NIST SP800-61 (*Guía de manejo de incidentes de seguridad informática*) del Instituto Nacional de Estándares y Tecnología (NIST, por su abreviatura en inglés) (NIST, 2008) y la Guía Práctica para CSIRT-volumen 2 de la Organización de los Estados Americanos (OEA, 2023).

De acuerdo con lo establecido en el Boletín Técnico de Encuesta de Tecnologías de la Información y las Comunicaciones en Empresas (Departamento Administrativo Nacional de Estadística, 2022), en el 2020, el 17,2% de las empresas del sector comercio contaron con un área o dependencia encargada de coordinar la implementación de las TIC internamente y el 40,1% lo hicieron externamente. Para las empresas de industria, los respectivos porcentajes fueron 17,3% y 33,8%. En cuanto a las empresas del sector de servicios, se encuentra que los subsectores con mayor porcentaje de empresas con área interna encargada de las TIC fueron a) Educación superior privada, b) Desarrollo de sistemas informáticos y procesamiento de datos, y c) Administrativas y de apoyo de oficina con porcentajes de 59,4%, 56,8% y 52,0%, respectivamente.

Adicionalmente, el CONPES 3854 (2016) convierte a Colombia en el primer país de Latinoamérica y uno de los primeros en el mundo, en incorporar plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social para las empresas que sean víctimas de estos (CONPES, 2020). Para el Ministerio de Educación Nacional como cabeza de sector y sus entidades adscritas que brindan apoyo a la formulación, coordinación y evaluación de las políticas

públicas a nivel de educación que promueven el desarrollo competitivo, equitativo y sostenible del sector estudiantil, la inexistencia de un CSIRT que se haga responsable de coordinar y respaldar la respuesta a un evento o incidente de ciberseguridad se traduce en la incapacidad de garantizar el bienestar de sus activos de información, toda vez que la información es el activo más importante para cualquier institución o empresa. Ante dicha problemática surge el siguiente interrogante: ¿Cuáles son los lineamientos y políticas pertinentes para la conformación de un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) en el sector de educación en Colombia? Desde un punto de vista teórico, se analizan fundamentos relacionados con la temática propuesta y con cada uno de los objetivos, esto con el fin de poder dar un lineamiento apropiado al tema seleccionado.

La metodología de la investigación se desarrolla a partir de una investigación aplicada que permita mostrar las actividades propias del CSIRT para el Ministerio de Educación Nacional, con la descripción de los diferentes campos de aplicación, la definición de los roles del personal que integrará el equipo con sus respectivas funciones, el diseño del catálogo de servicios a prestar, el manual de operaciones y, finalmente, la estructura orgánica que tendrá el CSIRT.

PALABRAS CLAVE: CISRT, Cibernéticas, NIST, ciberseguridad, vulnerabilidad, amenaza, ataques, incidentes, seguridad digital, riesgo, activos de información.

INTRODUCCIÓN

En Colombia, la ciberseguridad y ciberdefensa (seguridad digital) han cobrado una gran importancia debido al aumento de amenazas en el ciberespacio. Es por esto que el Gobierno Nacional ha realizado grandes avances en la materia iniciando por la implementación de políticas de acuerdo con lo establecido por el Consejo Nacional de Política Económica y Social, de ahora en adelante denominado CONPES, así:

- CONPES 3701 de 2011: Lineamientos de Política en Ciberseguridad y Ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país (CONPES, 2011).
- CONPES 3854 de 2016: Política Nacional de Seguridad Digital, renovó la política anterior, centrándose no sólo en la defensa y seguridad nacional en el entorno digital, sino que también abarca aspectos como la gobernanza, la regulación, la educación, la investigación y el desarrollo, la innovación y la cooperación internacional. Además, amplía su alcance más allá del Estado, para incluir a todos los ciudadanos, organizaciones y sectores económicos (CONPES, 2016).
- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital, fue la última política emitida en materia de seguridad digital y tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de forma que Colombia sea una sociedad competitiva e incluyente en el futuro digital, así mismo, busca fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país, en este mismo sentido, reconoció que se hace necesario actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías (CONPES, 2020).

En desarrollo de la última política y en el marco del objetivo específico “Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país” (CONPES, 2020), se asignó al Ministerio de Educación Nacional, como entidad cabeza del sector, al Departamento Nacional de Planeación a través de la

Dirección de Estudios Económicos con apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, al Archivo General de la Nacional, una acción con el objeto de que diseñarán, estructurarán y presentarán el proyecto de implementación del Equipos de Respuestas ante Incidentes de Seguridad (en inglés Computer Security Incident Response Team, CSIRT) del Sector de la Educación Nacional.

Al respecto, es importante resaltar que, gracias al desarrollo de los diferentes CONPES, relacionados con ciberseguridad y ciberdefensa en el país, se han logrado identificar infraestructuras críticas cibernéticas (ICC) y se han podido consolidar organizaciones que aportan al fortalecimiento de la seguridad digital como unidades para la gestión de riesgos e incidentes a nivel país correspondiente con esas infraestructuras. Entre estas estructuras existen conceptos que el país viene implementando para obtener servicios de reacción y prevención ante incidentes informáticos como el CSIRT, sistema cuya función se enfoca en controlar y minimizar los daños a los que se enfrenta una entidad cuando acceden de manera malintencionada y fraudulenta para secuestrar su información, suplantar su imagen o buscar un lucro económico con la afectación de la imagen y reputación de una entidad, ofreciendo además el registro y la preservación de evidencias que facilitaran conocer el contexto del ataque y las mitigaciones en aras de retornar su información a la operación requerida por la entidad.

Según lo enunciado y considerando que el Sistema Nacional de Información y Banco de Datos del Sector Educación (SNIBDE) es crucial para el sector educativo colombiano y el país, debido a que alberga activos digitales de alto valor esenciales para el funcionamiento diario, la toma de decisiones y la formulación de políticas públicas educativas, se convierte en un activo de información catalogado como infraestructura crítica cibernética del Estado colombiano.

Por lo anterior, el Ministerio de Educación Nacional requiere desarrollar e implementar un conjunto robusto de medidas que permitan prevenir, identificar y gestionar adecuadamente los riesgos de seguridad digital. Es por eso que la definición de una estrategia que permita implementar el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) para el Ministerio de Educación Nacional y su sector juega un papel fundamental para la protección de sus activos digitales.

El desarrollo de la definición de una estrategia que permita implementar el CSIRT en el Ministerio de Educación Nacional y su Sector pretende identificar gestionar, mitigar los riesgos y las amenazas de ciberseguridad que enfrentan tanto el Ministerio como las instituciones del sector

educativo. Dada la criticidad de los servicios ofrecidos y la sensibilidad de los datos que se manejan, el CSIRT desempeñará un papel fundamental en la generación de capacidades para la protección de la infraestructura crítica a su cargo y del sector en general.

Teniendo en cuenta que desarrollar un CSIRT requiere un enfoque colaborativo y flexible que permita una respuesta ágil en un entorno donde las amenazas cibernéticas evolucionan constantemente, las organizaciones requieren equipos de respuesta altamente eficientes, en consecuencia, resulta esencial garantizar la protección de los activos digitales e infraestructura crítica cibernética del Sector Educación, a través del desarrollo de políticas, procedimientos, protocolos, mecanismos de control y demás medidas que permitan prevenir, identificar y gestionar riesgos de Seguridad Digital. El CSIRT del Sector Educación, tiene como objetivo principal gestionar y mitigar los riesgos y amenazas de ciberseguridad que enfrenta el Ministerio de Educación y las instituciones del sector, lo cual resulta fundamental dada la criticidad de los servicios ofrecidos por éste y la sensibilidad de los datos que se manejan, por lo cual desempeñará un papel fundamental en la generación de capacidades para la protección de la infraestructura crítica del sector educación.

1. TÍTULO DE LA PROPUESTA

Diseñar una estrategia para implementar el Grupo de Respuestas a Incidentes de Seguridad (CSIRT) en el Ministerio de Educación Nacional de Colombia y el Sector de Educación.

2. PLANTEAMIENTO DEL PROBLEMA

En 1988 se creó el primer Centro de Respuesta a Emergencias Cibernéticas (CERT), por las siglas en inglés de *Computer Emergency Response Team*, bajo la dirección de DARPA, en atención de respuesta a uno de los primeros gusanos (*worms*) que afectaron Internet (FIRST, 2015), desarrollado por un estudiante de posgrado de la Universidad Cornell que aprovechó múltiples vulnerabilidades de la época para replicarlo automáticamente a través de las redes e infectó en poco tiempo a un gran porcentaje de los equipos que estaban conectados, este ataque fue publicado desde las redes del Massachusetts Institute of Technology (MIT) con el objetivo de desviar las investigaciones. Este evento, que condujo a una de las primeras investigaciones de incidentes informáticos y condenas por delitos en el mundo de internet, evidenció la necesidad de construir una comunidad de respuesta a incidentes ante futuros ataques. El CERT fue luego asignado al Instituto de Ingeniería de Software de la Universidad Carnegie Mellon y desarrollado como marca propia que sólo puede ser usada por los CERT nacionales y quienes licencien su marca cumpliendo con los criterios definidos para la protección de información.

En este sentido, se han venido desarrollando organizaciones orientadas a la coordinación y gestión de incidentes de seguridad en instituciones, públicas, privadas y académicas a través de todo el mundo, instituciones que se apoyan para la respuesta a estos eventos que son generados en cualquier país del mundo y pueden afectar cualquier sistema de información en el ciberespacio.

Cada organización ha adoptado denominaciones diversas pero cada vez más convergen en los CSIRT. Las capacidades de todos estos centros de respuesta se ven fortalecidas en la medida en la que pertenezcan y aporten a redes nacionales, regionales, continentales y globales de respuesta a incidentes de seguridad cibernética que puedan apoyarlos con información, escalamiento o capacidades para la defensa en entornos complejos y, muchas veces, transnacionales. Por ello, foros como el FIRST (*Forum of Incident Response and Security Teams*), que es la principal asociación global de los CSIRT y cuyo objetivo principal es promover la cooperación y coordinación en la prevención de incidentes a través del mundo. El CSIRT Américas de la Organización de los Estados Americanos y los CERT y CSIRT de carácter nacional en cada uno de los países con sus alianzas multilaterales complementan efectivamente este ecosistema haciéndolo cada vez más unido, con posibilidades de compartir en un entorno de confianza entre diferentes equipos dispersos en las diferentes regiones. En síntesis, la creación de centros de respuesta a incidentes ha sido una

necesidad en el ciberespacio desde sus inicios y requiere enfoques nacionales y sectoriales como el planteado en este documento para el Sector Educación de Colombia.

En el ámbito nacional, desde principios de la primera década del 2000 se comenzó a tener respuesta a incidentes de ciberseguridad, especialmente por parte de la Policía Nacional, entidad que debió atender los primeros delitos por computador. A mediados de esa década, el Ministerio de Defensa Nacional comienza a manifestar interés en la creación de un centro nacional de respuesta a emergencias cibernéticas. La consolidación y formalización de la existencia de un CSIRT en Colombia se consolida en el documento de política económica y social CONPES 3701 de 2011 (CONPES, 2011), donde se dictan los lineamientos de política en ciberseguridad y ciberdefensa para el país y se formaliza la coordinación nacional en materia de gestión de incidentes cibernéticos. Allí se define la creación del ColCERT adscrito al Ministerio de Defensa Nacional como ente coordinador de las acciones necesarias, apoyado por el Centro Cibernético Policial (CCP) que opera en defensa del ciudadano colombiano en el ciberespacio y en el combate contra el cibercrimen. También se establece la creación del Comando Conjunto Cibernético (CCOC) adscrito al Comando General de las Fuerzas Militares como ente responsable de la identificación y defensa de las infraestructuras críticas del país.

Las iniciativas nacionales en la materia continuaron su desarrollo y hacia el 2016 se publica la Política Nacional de Seguridad Digital en el documento CONPES 3854 (CONPES, 2016) donde se trabaja principalmente el desarrollo de pilares en el fortalecimiento del marco legal y regulatorio, la cultura de ciberseguridad y ciberdefensa, la protección de las infraestructuras críticas cibernéticas y la cooperación y diplomacia en el ciberespacio para el fortalecimiento de las capacidades y la gobernanza en la materia en el país, y en el cual se estableció la necesidad del desarrollo de los CSIRT sectoriales.

Además, en julio del 2020 se publica el documento CONPES 3995 (CONPES, 2020) que establece la Política Nacional de Confianza y Seguridad Digital, cuyo objetivo general es:

Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías (CONPES, 2020, p. 3)

Para el cumplimiento de este propósito, se establecieron tres objetivos y un plan de acción. Dicho plan establece que el Ministerio de Educación Nacional, junto con otras importantes instituciones, “coordinará y diseñará una estrategia de formación en capacidades en materia de seguridad digital, en la cual se unifiquen las iniciativas de sensibilización y generación de habilidades en los ciudadanos en Colombia en materia de seguridad digital” (CONPES, 2020, p. 27). Asimismo, se “implementará una estrategia para la creación de hábitos de uso seguro y responsable de las TIC” (CONPES, 2020, p. 28). Por último, el MEN debe liderar el diseño e implementación de una “estrategia que contemple acciones para la generación de hábitos de uso seguro y responsable de las TIC que posibilite generar en la trayectoria educativa completa el desarrollo de competencias y la formación en seguridad y confianza digital” (CONPES, 2020, p. 41). Además, estableció la necesidad de contar con un registro central único de incidentes, el cual aprovechará las capacidades de los diferentes CSIRT sectoriales.

2.1. Formulación del Problema

¿Cuáles son los aspectos técnicos, económicos, sociales, estándares, normas y legislación a tenerse en cuenta para el diseño de una estrategia que permita implementar el Grupo de Respuestas a Incidentes de Seguridad (CSIRT) en el Ministerio de Educación Nacional de Colombia y el Sector Educación?

3. OBJETIVOS

3.1. Objetivo General

Diseñar la estrategia para implementar el Grupo de Respuestas a Incidentes de Seguridad CSIRT en el Ministerio de Educación Nacional de Colombia y el Sector de Educación.

3.2. Objetivos Específicos

- Identificar el nivel de madurez inicial con el que operará el CSIRT de educación.
- Definir el catálogo de servicios del CSIRT para el Ministerio de Educación Nacional de Colombia y el Sector Educación.
- Establecer la estructura organizacional y perfiles que integran el CSIRT para el Ministerio de Educación Nacional de Colombia y el Sector Educación
- Documentar las políticas y procedimientos operacionales para la puesta en funcionamiento del Grupo de Respuestas a Incidentes de Seguridad CSIRT.

4. JUSTIFICACIÓN

Como se ha visto en el contexto internacional y nacional enunciados en la introducción de esta investigación, el Sector Educación ha estado siempre en el centro de los incidentes de ciberseguridad en el mundo, ha sido desde donde se han presentado los primeros incidentes y donde en muchas ocasiones se han probado las primeras técnicas de ataque y defensa. Esto no ha sido ajeno en Colombia, donde desde la década de 1990, muy cerca de la llegada de internet al país en 1994, a través del proyecto de la Red de Ciencia, Educación y Tecnología de Colombia (CETCOL) se conocieron los primeros ataques que afectaron, principalmente, las redes de las universidades que estuvieron involucradas en este proceso de adopción y divulgación de la tecnología de Internet.

En los últimos años ha sido ampliamente visible el aumento del cibercrimen, *ransomware* y el terrorismo digital que afecta a las instituciones del sector y las prácticas en contra de los niños y adolescentes en edad escolar que han pasado por temas como el ciberbullying, *grooming*, sextorsión, *sexting*, *stalking*, así como el aprovechamiento de los canales digitales para afectar su desarrollo y aprovechar su desconocimiento para influenciarlos de manera negativa y facilitar ciberataques en sus hogares e instituciones educativas (CyberTalk, s.f.).

De allí se concluye que la definición de una estrategia para implementar el CSIRT en el Sector Educación debe hacerse asumiendo la complejidad de la realidad de una entidad pública del orden nacional, un dinamizador de políticas educativas y un organismo dotado de una gran complejidad de gestión y operación. Para ello es necesario desarrollar las áreas que permitan el desarrollo de la presente investigación, las cuales se definen en:

1. La acción ministerial, entendida como su misión de dirigir la educación de acuerdo con los principios constitucionales; formulando y adoptando los programas, políticas, proyectos y planes que guían el sector hacia el logro de los propósitos de la educación establecidos en la ley. Trabajar en la integración de la Nación con las entidades territoriales y, en particular, lograr el establecimiento del CSIRT.

2. La gestión y gobernanza, entendida como plasmación del concepto de gobierno basado en la interrelación equilibrada y armónica del Ministerio como órgano rector, el operador y los gestionados (electorado) para lograr un progreso en las funciones encomendadas de forma estable, sostenible y eficiente. Gobernanza, además, que debe buscar el equilibrio entre el cumplimiento de los requisitos legales y la eficiencia.

3. La interacción entre CSIRT y Gobierno. El CSIRT debe canalizar esfuerzos de colaboración en varios ámbitos, como puede ser la articulación de políticas de cooperación (tanto a nivel local como regional, nacional e internacional), la defensa cibernética, la generación de alianzas orientadas a defensa, todo ello desde el compromiso de contribuir a la inteligencia pública y colectiva.

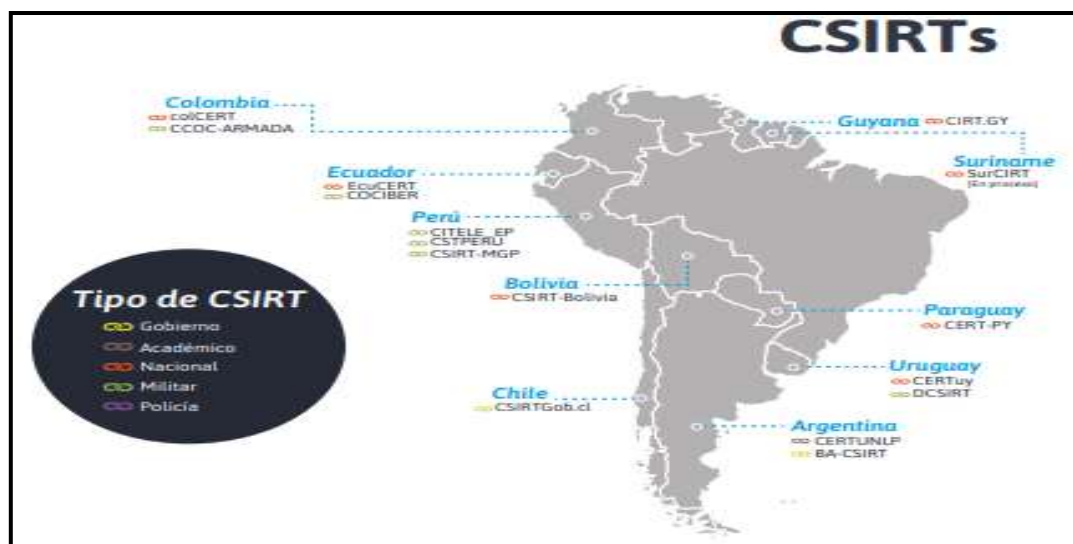
5. MARCO REFERENCIAL

5.1. Marco Conceptual y Teórico

La implementación de Equipos de Respuesta a Incidentes de Seguridad (CSIRT) en la región han tenido una fase de crecimiento ante la necesidad de identificar, proteger, detectar, responder y recuperar las infraestructuras tecnológicas en las entidades públicas y privadas de amenazas cibernéticas que comprometen la integridad, disponibilidad y confidencialidad de la información, afectando de manera directa la reputación de la entidad y, en consecuencia, generando pérdidas económicas incalculables entre otras afectaciones.

Figura 1

Tipo de CSIRT



Fuente: Banco Interamericano de Desarrollo (2020).

Para el caso de Colombia, actualmente cuenta con Equipos de Respuesta a Incidentes de Seguridad (CSIRT), como el ColCERT y CCOC-ARMADA, por lo que se hace necesario avanzar en la implementación de CSIRT, con el fin de proteger la infraestructura tecnológica de las entidades gubernamentales y demás partes interesadas, que están expuestas ante cualquier ataque cibernético.

Por lo anterior, resulta imperativo que el Ministerio de Educación Nacional diseñe e implemente un Equipo de Respuesta a Incidentes de Seguridad, el cual, por su naturaleza, maneja todos los niveles de clasificación de la información que debe pretender por su manejo, cuidado y

tratamiento de los datos personales de los actores y comunidad estudiantil de Colombia, los cuales nos son ajenos a las amenazas cibernéticas.

Por el lado de los sectores los resultados también son sorprendentes. Según un informe de la compañía de ciberseguridad Lumu Technologies (2021), si bien el sector financiero es del que más se suele hacer ruido al momento que sufre un ciberataque, lo cierto es que no hay sector que esté menos expuesto a los delincuentes en la red, señalan, por ejemplo, que sectores como el de la salud han venido presentando un incremento importante en el número de ataques recibidos en los últimos años. Además, todo parece indicar que seguirán siendo blanco de los ciberdelincuentes.

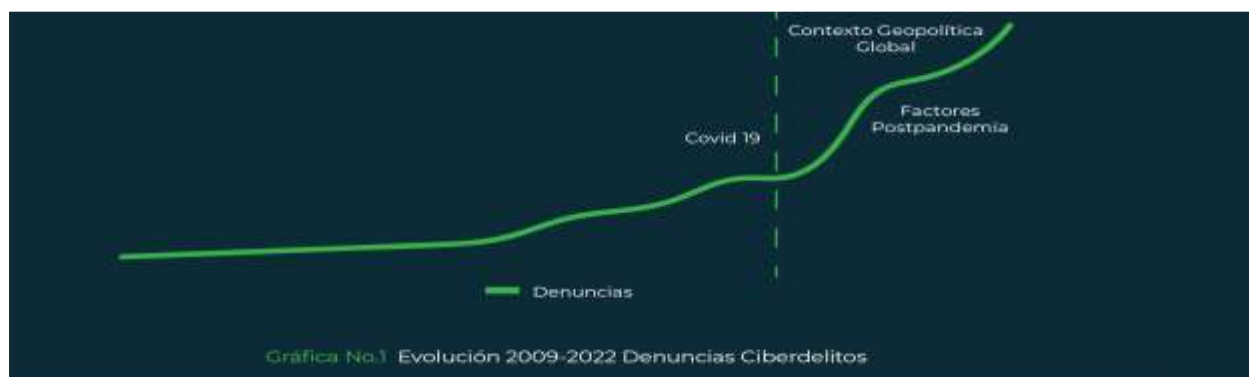
5.1.1. Incidentes de Seguridad Informática 2023 en Colombia

Durante los últimos diez años, el número de casos registrados en el sistema de la Fiscalía General de la Nación creció de manera exponencial, tanto así que, en el 2013, cuando se empezaron a conocer los primeros casos de *ransomware* en Colombia ya se adelantaban campañas de sensibilización para enfrentar el problema de *SpearPhishing*. Durante este periodo se reportaron tan sólo 3.380 casos y en 2023 el registro de estos casos es de 65.794 (CCIT, 2023).

Hasta el momento, el 2022 ha sido el segundo año con mayor crecimiento en las cifras de ciberdelito para Colombia, con un aumento de 14.000 casos respecto a lo reportado en el 2021. Estas cifras fueron superadas en 2020 durante la pandemia del COVID-19 cuando el incremento anual registró más de 22.000 casos en comparación con 2019, lo cual equivale a una variación del 109% (CCIT, 2023).

Figura 2

Denuncias ciberdelitos en Colombia



Fuente: CCIT (2023).

Según la Cámara Colombiana de Informática y Telecomunicaciones (CCIT, 2023), el porcentaje de incremento de los ciberdelitos ha venido creciendo de manera significativa, pues el comportamiento de alza tuvo un punto de inflexión en 2019. A continuación, se destacan algunos factores que ocasionaron estos resultados:

- Incidencia del factor geopolítico en el contexto global: se evidenció que los grupos que conforman el APT C36 (grupo de espionaje de Latinoamérica activo desde 2018) han lanzado ciberataques contra entidades gubernamentales colombianas, como también a corporaciones del sector financiero, la industria petrolera y la fabricación profesional.
- Incremento en el número de servicios de comercio electrónico y servicios de banca digital: el sector Fintech en Latinoamérica indica que las billeteras virtuales vienen creciendo en un 27% cada año, tendencia que se espera sea duplicada para el 2025.
- Concienciación y sensibilización insuficientes como herramienta de detección temprana y prevención de ataques en fases iniciales.
- Percepción de la ciberseguridad como un gasto elevado en la operación de las empresas en Colombia.
- Desactualización de los sistemas y del recurso humano por fuga de talentos de ciberseguridad. Hoy en día la alta rotación en las entidades del Estado del recurso humano con competencia en Seguridad de la Información y Ciberseguridad ocasiona ralentización en el avance de la implantación de sistemas de gestión de seguridad de la información y Grupos de Respuesta a Incidentes de Seguridad.

Continuando con el estudio realizado por CCIT (2023), se puede encontrar que la violación de los datos personales es el tercer delito más reportado, tanto así que en el 2022 se registraron 12.775 casos, valor que aumentó en un 3% respecto al 2021, donde se evidenció que 12.419 de los casos correspondieron a suplantaciones de identidad, robos de identidad y fuga de datos, observado también que estos datos fueron objetos de venta en los mercados de la internet profunda (*deep web*).

La suplantación de sitios web, asociados a modalidades como el *SpearPhishing*, *phishing* y *pharming* son identificados como el cuarto delito con mayor reporte de noticias criminales. En Colombia, estos tipos de suplantación tienen sanciones de tipo penal. Las cifras analizadas indican

un incremento del 4% entre 2021 (12.419) y 2022 (12.775). Asimismo, se identificó que el delito que más creció en Colombia fue la interceptación de datos informáticos: las cifras de 2021 de 1.331 frente al 2022 de 1.927, indican un aumento del 45%. Estos registros de manera indirecta pueden haber estado relacionados con los casos de ciberespionaje empresarial y otras afectaciones a la información comercial.

El estudio realizado por la CCIT (2023) demostró que las ciudades con mayor afectación fueron las siguientes (ver Tabla 1 y Figura 3).

Tabla 1

Ciudades colombianas afectadas por ciberdelitos

CIUDADES COLOMBIANAS AFECTADAS POR CIBERDELITOS	
CIUDAD	% DE AFECTACIÓN IDENTIFICADO
Bogotá	29%
Medellín	8.65%
Cali	6.23%
Barranquilla	3.76%
Cartagena	2.23%
Bucaramanga	1.91%
Ibagué	1.89%
Villavicencio	1.65%
Pereira	1.45%

Fuente: elaboración propia.

Figura 3

Interceptación de datos informáticos 2022



Fuente: elaboración propia.

Las ciudades reportadas en la Figura 3 representan un 65% del total de los casos reportados.

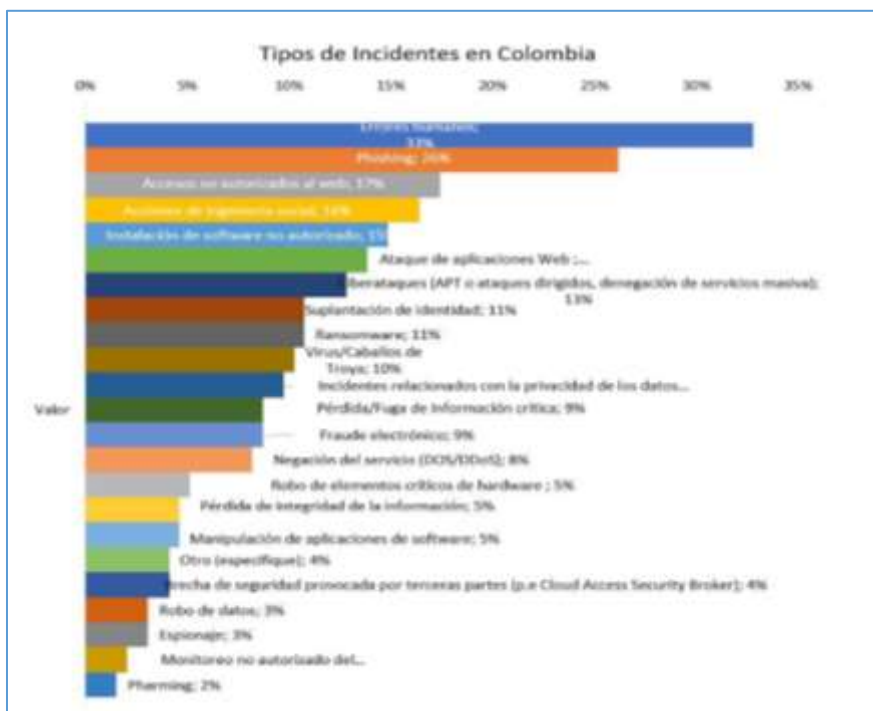
5.1.2. Tipos de Incidentes 2023

El informe XXIII Encuesta Nacional de Seguridad Informática (Almanza, 2023) presenta un conjunto de resultados sobre la situación de la ciberseguridad en Colombia. El 48% de los encuestados afirma haber estado en contacto con algún incidente de seguridad en su empresa, en comparación con el año inmediatamente anterior, donde el 56% lo manifestó. El 36% asevera no tener información al respecto de los incidentes en sus organizaciones, al revisar los detalles se encuentra que el 27% expone haber experimentado entre 1 y 3 incidentes, tanto para los que expresan que han experimentado entre 4 y 7 incidentes, como los que han experimentado más de 7 incidentes el valor es cercano al 11%.

Los tipos de incidentes que se presentaron en las organizaciones son: errores humanos (33%), *phishing* (26%) y los accesos no autorizados a la web (17%) son las tres primeras posiciones del listado.

Figura 4

Tipos de incidentes en Colombia



Fuente: Almanza (2023).

Por tanto, se puede concluir que en la XXIII Encuesta Nacional de Seguridad Informática se evidencia un cambio leve frente a la estadística presentada el año inmediatamente anterior, es decir,

los valores disminuyen un poco más, sin embargo, no son tan significativos para afirmar que existe un cambio de tendencia.

5.1.3. Incidentes Específicos en Entes y Organizaciones del Sector Público de Colombia 2021 – 2024

A continuación, se relacionan los ciberataques más recientes que han generado mayor impacto en la prestación de los servicios en entes y organizaciones pertenecientes específicamente al sector público de Colombia:

Tabla 2

Ciberataques recientes en Colombia

Año	Entidad / organización afectada	Tipo de Ataque
2021	Ministerio de Salud y Protección Social	Secuestro de Información (Ransomware) a los sistemas de apoyo y administrativos
2022	Universidad de Pamplona	Comercio de cuentas de correo electrónico en mercados ciberdelictivos
2022	Invima	Secuestro de Información (Ransomware) – primer ataque (febrero).
2022	Invima	Secuestro de Información (Ransomware) – segundo ataque (octubre).
2022	Famisanar	Secuestro de Información (Ransomware)
2022	Clínica Laura	Secuestro de Información (Ransomware)
2022	Red de Salud Ladera	Secuestro de Información (Ransomware)
2022	Procaps Laboratorios	Secuestro de Información (Ransomware)
2023	Audifarma	Por establecer (gestión en curso).
2022	Grupo Keralty (Sanitas)	Secuestro de Información (Ransomware)
2022	Departamento Administrativo Nacional de Estadísticas (DANE).	Secuestro de Información (Ransomware)
2022	Departamento Nacional de Planeación (DNP)	Secuestro de Información (Ransomware)
2022	Dirección de Impuestos y Aduanas Nacionales (DIAN)	Credenciales de cuentas de usuarios expuestas en la Darkweb
2022	Instituto Colombiano para la Evaluación de la Educación (ICFES)	Credenciales de cuentas de usuarios expuestas en la Darkweb
2023	Superintendencia Nacional de Salud	Secuestro de Información (Ransomware) a infraestructura de nube privada alojada en el proveedor (IFX) afectando servicios de plataforma misionales de la entidad.

2023	Ministerio de Salud y Protección Social	Secuestro de Información (Ransomware) a proveedor (IFX) afectando servicios de plataforma misionales de la entidad.
2023	Rama Judicial	Secuestro de Información (Ransomware) a proveedor (IFX) afectando servicios de plataforma misionales de la entidad
2023	Superintendencia de Industria y Comercio	Secuestro de Información (Ransomware) a proveedor (IFX) afectando servicios de portales de la entidad.
2024	Audifarma	Por establecer (gestión en curso).
2024	Salud Total	Por establecer (gestión en curso).

Fuente: elaboración propia.

5.1.4. Política y Estrategia de Seguridad Cibernética: 2016 - 2020

Colombia es un referente en la región en temas relacionados con creación de políticas y estrategias de ciberseguridad, particularmente en temas como la estrategia nacional de seguridad cibernética, respuesta a incidentes, protección de la infraestructura crítica, manejo de crisis, defensa cibernética y redundancia de comunicaciones. Para el año 2016, se creó una segunda política nacional en materia de seguridad cibernética; después de cinco años de presentada la primera versión a través del CONPES 3701 (2011) donde se dan los lineamientos de política para la ciberseguridad y ciberdefensa, cuyo objetivo general es el de fortalecer las capacidades del Estado para responder a las amenazas en materia de seguridad cibernética y defensa en este campo del país.

Como se enuncia en el párrafo anterior, actualmente en Colombia se cuenta con una Política Nacional de Seguridad Digital, desarrollada en el CONPES 3854 del 2016, la cual busca que los ciudadanos utilicen responsablemente las herramientas digitales y cuenten con las habilidades de identificación y tratamiento de los riesgos en el ciberespacio. Como una de las contribuciones más relevantes de esta nueva política, se halla la figura de un coordinador nacional de seguridad digital, rol ejercido por la Presidencia de la República de Colombia (CONPES, 2016).

Por otra parte, la política de Gobierno Digital propuesta por el Decreto 1008 de 2018 establece “el uso y aprovechamiento de las TIC para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital” (Decreto 1008, 2018, art. 2.2.9.1.1.1).

Asimismo, como ente máximo para tratar temas intersectoriales de seguridad digital, se creó el Comité de Seguridad Digital, liderado por el Coordinador Nacional de Seguridad Digital.

Por otra parte, dentro de sus políticas de gestión y desempeño, el Gobierno Nacional por primera vez incluyó la política de seguridad digital como parte integral de la operación estratégica de las entidades públicas y privadas (Decreto 1499, 2017).

Figura 5

Marcos legales y regulatorios



Fuente: Banco Interamericano de Desarrollo (2020).

De igual forma, el Ministerio de Tecnología y las Comunicaciones (MINTIC, 2014) ha implementado a nivel nacional y territorial un modelo de seguridad y privacidad. Este modelo está diseñado para apoyar la gestión e implementación de buenas prácticas y estándares, con el fin de proteger los activos críticos de la información, la infraestructura tecnológica y los sistemas de información y comunicaciones, promoviendo la mejora continua.

Así, el CONPES 3854 (2016) convierte a Colombia en el primer país de Latinoamérica y uno de los primeros en el mundo, en incorporar plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (CONPES, 2016).

La política de Seguridad Digital establece nuevos lineamientos y directrices en los componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación. El CONPES de Seguridad Digital integra, además, los objetivos de defensa del país en relación con la lucha contra el crimen y la delincuencia en Internet. Para ello se centra en la implementación de cinco frentes de acción específicos:

- Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

La Seguridad y Privacidad de la Información, como componente transversal a la Política de Gobierno Digital, permite alinearse a los componentes de ésta para aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos del Ministerio de Educación.

Asimismo, apoya la confidencialidad en el tratamiento de la información utilizada en los trámites y servicios que ofrece la entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la ley que exceptúa el acceso público a determinada información. Es importante mantener actualizada la normativa y verificar periódicamente la aplicación de las mejores prácticas establecidas en Seguridad de la Información.

Para el logro de estos objetivos, es fundamental contar con el acuerdo y compromiso de todos los involucrados y el respaldo del nivel directivo dentro de las Entidades, siendo conscientes de los beneficios a obtener, con una cultura enfocada a la seguridad y privacidad, pero también del impacto que se afronta por la materialización de riesgos que no se controlan y que se asocian al tema de Seguridad y Privacidad de la información.

Los *Lineamientos de política para ciberseguridad y ciberdefensa* establecidos en el CONPES 3701 de 2011, se enfocan en el fortalecimiento y generación de capacidades en el

Gobierno Nacional, para enfrentar las amenazas en el ámbito cibernético creando con ello las condiciones necesarias para brindar protección en el ciberespacio (CONPES, 2011).

En cumplimiento de lo anterior y bajo un modelo de coordinación intersectorial, como estrategia para enfrentar las amenazas que atentan contra la seguridad y defensa del Estado, se planteó la creación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Centro Cibernético Policial (CECIP) y el Comando Conjunto Cibernético (CCOCI).

En este mismo sentido, el CONPES 3995 de 2020, *Política nacional de confianza y seguridad digital*, menciona dentro de sus objetivos específicos que para fortalecer las capacidades en seguridad digital de los ciudadanos, de todas las entidades públicas que integran el Sistema de Educación Nacional y del sector de la educación, coordinarán la elaboración de lineamientos para los planes de mejora en seguridad digital, en el manejo, gestión e intercambio de información, dada la condición de infraestructura crítica cibernética, con la finalidad de aumentar la confianza digital en el país (CONPES, 2020).

Por último, se encuentra el Decreto 338 (2022), por el cual se establecen lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital, donde será de obligatorio cumplimiento estas disposiciones para las entidades que conforman la Administración Pública, siendo el Ministerio de Educación Nacional, parte de estas entidades.

5.1.5. Modelos para el Manejo de Riesgos

En el ámbito de seguridad informática es posible implementar algunos modelos que permitan el manejo de los riesgos informáticos, con ello se puede reducir el impacto que estos producen sobre los activos de información que por consiguiente ponen en peligro la estabilidad de una organización. Entre estos modelos es posible destacar los que se presentan a continuación.

5.1.5.1. COBIT.

Es un modelo aceptado internacionalmente que tiene como fin controlar las herramientas tecnológicas de la información y los riesgos a las que están expuestas; este modelo proporciona herramientas que permiten la conexión entre los controles, los aspectos técnicos y los riesgos. Es un gran referente como marco de buenas prácticas aplicables a gobierno TI, siendo así un marco de trabajo de alto nivel que puede integrar otros modelos como lo son ITIL e ISO proporcionando

una flexibilidad en su aplicación y enfocándose en el control más que en la ejecución (IT Governance Institute-COBIT, 2017).

5.1.5.2. ITIL (Biblioteca de Infraestructura de Tecnologías de Información).

Mundialmente ITIL es un enfoque altamente aceptado de gerencia de servicios de TI, con un gran número de profesionales certificados ya que proporciona un modelo que tiene como resultado la unión de las mejores prácticas del sector público y privado; además, este modelo se encarga de los procesos que se ejecutan dentro de las organizaciones para la administración y operación de la infraestructura de las tecnologías de información, con el fin de proveer los servicios a los clientes teniendo en cuenta los costos acordes a las estrategias del negocio; las principales características de este enfoque es que es un *framework* no propietario, es independiente de proveedores y tecnología, brinda terminología estándar, además de lineamientos para planteamiento y definición de roles en los procesos (Axelos, s.f.).

5.1.5.3. ISO 27001.

Define requisitos de un SGSI (Sistema de Gestión de la Seguridad de la Información), estableciendo, implantando, documentando y evaluando políticas que permitan la protección de los activos; se basa en un enfoque por procesos con el principio de una mejora continua, por lo cual es altamente compatible y se puede integrar con otros sistemas de gestión existentes en una organización; el eje central de este estándar es la protección de los pilares de la seguridad informática (la confidencialidad, integridad y disponibilidad de la información). Esto lo realiza a través de la investigación referente a los problemas potenciales que pueden afectar la información (evaluación de riesgos), luego propone definir qué hacer para evitar que los problemas lleguen a producirse (mitigación o tratamiento del riesgo) (Escuela Europea de la Excelencia, 2019).

5.1.5.4. CSIRT.

Según la documentación de FIRST (2019), y teniendo como base los riesgos a los que se enfrenta la información, se debe abordar el cómo plantear medidas para evitar que las afectaciones sean graves y que sean recuperables en el caso de que se presenten; para ello se analizará y se pondrá a consideración el termino CSIRT. En el año 1988 se presentó el primer incidente cibernético denominado “Morris”, el cual tenía como intención buscar contraseñas de los ordenadores; como medida se creó CERT en la Universidad Carnegie Mellon, en Pittsburgh, Pensilvania (EE. UU). A partir de aquí, los equipos para manejos de incidentes fueron creciendo,

pero se diferenciaban su propósito, su financiación, su idioma y sus zonas horarias; esto cambió al aparecer un nuevo gusano llamado “wank”, que para contraatacarlo generó que se juntaran y coordinaran esfuerzos desde los diferentes equipos de manejo de incidentes lo que creó y fortaleció la comunidad. América Latina logró tener su primer CSIRT en México, su nombre fue MX-CERT y fue propuesto por el Instituto Tecnológico y Estudios Superiores de Monterrey (ITESM), llegó a ser miembro del grupo FIRST; actualmente Colombia tiene varios CSIRT registrados a FIRST (ver Figura 5).

Figura 5

CSIRT Colombia en el grupo FIRST

Team	Official Team Name	Country
SEC-CERT	Cyber Security Operations Center @ SECURE	US
CERT CERN & CSDC	CERN Center for Security and Cyber Defense (CERT CERN & CSDC)	CH
CSIRT360	Cyber Security Government Centre and Digital Security for Business Technology Group CSIRT360	UK
CERTIFICADO SOC DE COLOMBIA	CERTIFICADO SOC DE COLOMBIA	CO
CSIRT Antioquia	CERT Antioquia	CO
CSIRT Coordinador AVAL	CSIRT coordinador AVAL	CO
CSIRT GUARAL	GUARAL SECURITY INCIDENT RESPONSE TEAM OF GUARAL DIGITAL	EC
CSIRT Cve@	CSIRT Cve@	CO
CSIRT ETS	Computer Security Incident Response Team - Empresa de Telecomunicaciones de Bogotá S.A. ETS	CO
CSIRT SOC Israel	Computer Security Incident Response Team of Israel	IL
CSIRT ALL-THREAT	Multi-vendor computer security incident response team	CO
CERTPOLSK	Response Team Computer Security Incident of the Computer Network	PL
DigOCIRT	DigOC Computer Security Incident Response Team	CO
ETS-CERT	Computer Security Incident Response Team of ETS International	CO
GameSOC-CERT	Game Elements SOC-CERT	CO
ISS-CERT-Helicon	ISS-CERT-Helicon	CO
Shark	Shark	CO
Sharknet CSIRT	Sharknet CSIRT	CO
SOC HELICON	Security Operations Center Helicon Consulting Services	CO

Fuente: FIRST (2019).

Actualmente, un CSIRT es definido como un equipo o unidad de una organización que integra personal altamente calificado en seguridad informática, cuyo objetivo radica principalmente en la prevención y en la respuesta inmediata u oportuna ante los incidentes que comprometan los activos de información o la infraestructura tecnológica, además, refuerza la gestión de la seguridad informática de sus usuarios atendidos, a través de la comunicación y coordinación de su trabajo con una red de CSIRT a nivel local y mundial, incluyendo empresas dedicadas a la protección de seguridad informática (United States-Department of Defense, 2015).

5.1.6. *Servicios de un CSIRT*

Son considerados como servicios reactivos y proactivos; los reactivos requieren de una reacción por petición u ocurrencia, pueden ser análisis de vulnerabilidades, detección de malware, gestión de código malicioso y toda la gestión ante un incidente informático que va desde el análisis, el tratamiento, el apoyo y la investigación del incidente; mientras que los servicios proactivos proponen anticipar ataques ayudando a proteger y asegurar los sistemas con lo que se trata de disminuir los riesgos a futuro (Gorgona, 2018).

5.1.7. *Ámbitos de un CSIRT*

Una de las formas de clasificar un CSIRT es por medio de su ámbito de actuación, lo que permite hacer una agrupación sectorizada de la comunidad o del tipo de organizaciones a quienes presta sus servicios (ENISA, 2006). A continuación, se proporciona un listado de algunos CSIRT clasificados según su tipo de operación (ver Tabla 2).

Tabla 3

Ámbitos de los CSIRT

Ámbitos de CSIRT	Detalle
CSIRT comerciales	Venden el servicio de atención de incidentes a clientes que no quieren o no tienen los recursos para montar un CSIRT propio.
CSIRT de infraestructuras críticas	Prestan servicios a sectores públicos o privados de los cuales dependen los procesos más importantes para el desarrollo y fines de uno o varios sectores de la nación.
CSIRT gubernamentales	Brindan seguridad a la información de los entes gubernamentales
CSIRT nacionales	Asume el papel de coordinador nacional de incidentes informáticos
CSIRT del sector militar	Prestan servicios a los entes e instituciones militares de un país.

CSIRT de proveedores	Son destinados a prestar servicio sobre incidentes a productos específicos
CSIRT del sector PYME	Se centran en ayudar a las PYME y a ciudadanos
CSIRT académico	Atienden universidades, colegios, comunidades académicas

Fuente: elaboración propia.

5.2. Marco Tecnológico

Para el tratamiento de incidentes, un CSIRT necesita algunas herramientas tecnológicas básicas que permitan ejecutar el objetivo principal de la organización, el cual es garantizar que no se presenten incidentes de seguridad y si estos se llegaran a presentar se logren mitigar los daños al máximo, por lo que es de gran importancia contar con instrumentos como los descritos a continuación.

5.2.1. RTIR

En su página oficial, se define RTIR (s.f.) como una herramienta que ayuda a equipos de respuesta a incidentes proporcionando colas y flujos de trabajo, correlacionando datos clave del manejo de incidentes que permiten encontrar patrones y vincular múltiples informes de incidentes con un incidente de causa raíz. Este software permite a un usuario crear una incidencia, con lo que un equipo de soporte hace la respectiva revisión para aprobación, rechazo y trabajos adecuados sobre el incidente. Finalmente, se hace un cierre del caso haciendo un informe detallado de los hechos; cabe destacar que RTIR tiene un licenciamiento *open source* y su uso es gratuito por lo que cada organización puede adaptarlo a sus propias necesidades, constituyéndose como herramienta importante al momento de manejar incidentes.

5.2.2. Herramientas CRM

Customer Relationship Management, o por su nombre traducido “gestión de relaciones con clientes”, permite el manejo estratégico de clientes, logrando un manejo eficiente de éstos dentro de la organización; este software tiene como objetivo principal ganar, analizar, atraer y retener clientes, además con ello se puede mejorar la comunicación dentro de la organización y hacer que el personal sea más productivo y organizado en sus labores (Montoya y Boyero, 2012).

5.2.3. Herramientas para Verificación de la Información

Permiten hacer búsquedas selectivas y actualizadas de información relacionada a un objetivo general; para el caso del manejo de incidentes es correcto usar algunas de estas herramientas, como son *Website checker*, la cual tiene una licencia de uso comercial y permite hacer un constante monitoreo para detectar en tiempo real los cambios realizados sobre una página web; otra herramienta de este tipo es *Whatch that page*, la cual tiene una versión gratuita con algunas limitantes en su funcionalidad y una versión comercial con más funciones habilitadas. Ésta permite enviar correos electrónicos cuando se produzcan cambios en una página web determinada.

5.2.4. Herramientas de Encriptación

Estas herramientas permiten encapsular la información con lo que cualquier dato será cifrado e ilegible ante cualquier visualización, esto gracias a algoritmos que logran desordenar sus componentes, por lo que sólo con las claves correctas y el algoritmo preciso los datos podrán ser legibles. Dentro de estas herramientas está GNUPG, la cual permite cifrar datos y comunicaciones con la administración de claves versátil. Es de código abierto por lo que las organizaciones podrán editar y adaptar a sus necesidades.

5.2.5. Herramientas de Obtención de Datos Volátiles de Memoria

En toda investigación se debe hacer la recolección de datos volátiles, esto con el fin de garantizar un proceso investigativo íntegro preservando la evidencia catalogada como volátil y adicionando a ello *logs* que permitan responder preguntas del caso de forma rápida y eficaz sin realizar *backups* sobre las unidades expuestas, reduciendo así los riesgos de pérdida de datos en un incidente. Entre estas herramientas, se destacan:

- Lime para UNIX / LINUX: se usa desde un dispositivo USB conectado en los sistemas u ordenadores afectados.
- Volatilly: al igual que el anterior se usa desde un dispositivo USB sobre el sistema afectado.
- En Windows hay herramientas como FTK Imager, DumpIT o MemoryDD, los cuales realizan un volcado de la memoria del sistema.

5.2.6. Kali Linux

Es un proyecto de código abierto que es mantenido y financiado por *Offensive Security*, un proveedor de servicios de prueba de penetración y capacitación de seguridad de la información de

clase mundial. Este sistema operativo tiene gran número de herramientas para realizar auditorías informáticas con lo que se puede lograr detección de vulnerabilidades y poder gestionar los riesgos de los sistemas informáticos (Kali Linux, 2019).

5.3. Marco Legal

5.3.1. Contexto Regulatorio

Colombia ha priorizado su participación en escenarios internacionales, además, mediante la Ley 1928 (2018) se aprobó el Convenio sobre la Ciberdelincuencia y depositó su instrumento de adhesión el 16 de marzo de 2020. El delito cibernético está cubierto en la Ley 1273 (2009) que modifica el Código Penal de forma de incluir esta modalidad de delito. Para la protección de datos y privacidad, Colombia cuenta con la Ley 1581 (2012).

Asimismo, el país también tiene una Delegatura de protección de datos personales (Superintendencia de Industria y Comercio, s.f.) que se encarga, entre otros temas, de velar por que se cumpla toda la normativa relacionada con la protección de datos y por divulgar a los usuarios sus derechos con respecto a la protección de datos personales. Esta ley se aplica a las bases de datos públicas y privadas.

Legalmente, la ciberseguridad en Colombia está fundamentada en varios documentos y artículos generados desde el gobierno central y sus ministerios reconociendo tratados internacionales con Interpol y Europol, por lo que es conveniente mencionar a continuación los referentes en cuanto a la seguridad de la información y la ciberseguridad en Colombia.

5.3.2. Ley 527 de 1999

Es un marco legal para generar contratos y negocios por medios electrónicos, este documento se compone de dos capítulos, el primero detalla el valor jurídico y probatorio de los mensajes electrónicos y el segundo capítulo permite observar información acerca de regulación de entes encargados de generar firmas digitales (Ley 527, 1999).

5.3.3. Ley 594 de 2000

Esta ley dentro de sus contenidos establece y regula los principios archivísticos desde el panorama de la seguridad de la información, el tratamiento de los datos y la conservación de estos,

regulando así las buenas prácticas dentro del archivo público que pueden ser llevadas al archivo privado también (Ley 594, 2000).

5.3.4. Ley 679 de 2001

Esta ley le hace frente a lo concerniente con la pornografía infantil, genera responsabilidades a los ISP sobre el contenido que los usuarios podrán mover o manejar en el ciberespacio, en él se establecen lineamientos claros acerca de las prohibiciones y deberes tanto de los usuarios del servicio de internet como los proveedores (Ley 679, 2001).

5.3.5. Ley 962 de 2005

Este marco normativo establece normas en las que se simplifica y racionaliza los tramites que se deben llevar a cabo ante entidades públicas por lo que se debe instaurar atributos sobre la seguridad de la información electrónica que manejan estas entidades del sector público o que prestan servicios públicos (Ley 962, 2005).

5.3.6. Ley 1150 de 2007

Brinda normatividad acerca de la contratación en línea y la seguridad electrónica a aplicar sobre ésta; además vela por la eficiencia y la transparencia sobre el cumplimiento de la ley 80 de 1993, la cual brinda lineamientos acerca de la contratación pública para lo cual se desarrolla el sistema electrónico para la contratación pública, o mejor conocido por sus siglas SECOP (Ley 1150, 2007).

5.3.7. Ley 1273 de 2009

Define la información como bien jurídico tutelado y muestra los diferentes delitos informáticos y las penas a las que se ven expuestos sus infractores, teniendo como principal referente el código penal a quienes usen los sistemas de información y los medios electrónicos o telemáticos para desarrollar conductas determinadas para este artículo como criminales (Ley 1273, 2009).

5.3.8. Ley 1341 de 2009

También conocida como ley de tecnologías de la información y las comunicaciones (TIC), define conceptos y principios sobre la sociedad de las tecnologías de la Información y la aplicación de seguridad, resaltando que las TIC son pilares fundamentales de una sociedad evolutiva por lo

que se debe proveer de protección al usuario y la formación de talento para el fortalecimiento de la infraestructura (Ley 1341, 2009).

5.3.9. CONPES 3701 de 2011

Este documento establece una política de ciberseguridad en el país, define una línea que permite dar respuesta a situaciones de riesgo de seguridad informática a cargo de la policía y las fuerzas militares de la nación. El CONPES 3701 de 2011 está basado en tres acciones principales que se citan a continuación:

- Adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten.
- Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en defensa cibernética y ciberseguridad.
- Fortalecer la legislación en estas materias, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales (CONPES, 2011).

5.3.10. Ley 1437 de 2011

Garantiza los derechos y libertades de las personas, además muestra los criterios y políticas de seguridad sobre plataformas tecnológicas, las cuales se aplican a toda entidad u organismo del sector público, quienes deben utilizar medios electrónicos para hacer valer los derechos de las personas a través de actuaciones y procedimientos administrativos (Ley 1437, 2011).

5.3.11. Ley 1480 de 2011

Esta ley permite proteger al consumidor que realiza sus transacciones y movimientos bancarios o de divisas por medios electrónicos, mediante el establecimiento de criterios que garantizan la seguridad del usuario, de la plataforma que presta el servicio (pasarelas de pago) y de la entidad u organización que recibirá los dineros producto de dicha transacción (Ley 1480, 2011).

5.3.12. Decreto Ley 019 de 2012

Este decreto logra estandarizar los tramites a través de medios electrónicos y establece criterios de seguridad sobre estos procesos, siendo su principal objetivo el eliminar trámites innecesarios en el sector público garantizando el cumplimiento de sus deberes y procurando la

aceptación de los derechos de los ciudadanos a través de la transparencia y la eficiencia en los procesos (Decreto Ley 019, 2012).

5.3.13. Ley 1581 de 2012

Mediante esta ley el gobierno central dicta y establece disposiciones generales acerca de la protección de datos personales de cada ciudadano en cuanto a la información que repose en bases de datos, para la cual el usuario y/o ciudadano tiene derecho a solicitar actualización, información o eliminación total o parcial si él así lo requiere (Ley 1581, 2012).

5.3.14. Ley 1712 de 2014

Gracias a esta ley se promueve el principio de transparencia. En ella se dictan disposiciones generales del derecho que tienen los ciudadanos al acceso a la información pública, así como también las excepciones normativas establecidas por la ley o por la Constitución Política que intervienen en la publicación de información (Ley 1712, 2014).

5.3.15. Resolución 8934 de 2014

Esta resolución establece directrices concernientes a gestión documental y a la organización de archivos que deben cumplir las organizaciones vigiladas por la Superintendencia de Industria y Comercio (2014). En ella se parametriza la producción, recepción, distribución, organización, conservación, recuperación y consulta de la información teniendo en cuenta el medio en que se encuentra.

6. METODOLOGÍA

El modelo de investigación a usar para este proyecto es cualitativo, teniendo en cuenta que la información a estudiar no pretende presentar el conocimiento desde la exactitud numérica sino desde la comprensión y profundización del tema de estudio; el tipo de investigación a utilizar se denomina investigación aplicada la cual tiene por objetivo la resolución de una situación o problema específico, basado en la búsqueda y consolidación de conocimiento para la aplicación práctica en el Ministerio de Educación Nacional de Colombia y el sector de la educación.

Las técnicas a utilizar dentro del desarrollo del presente proyecto son la consulta bibliográfica y documental (Vargas, 2009), la cual garantiza los fundamentos teóricos de la investigación; se tendrá un proceso sistemático y secuencial de recolección de información, luego se implementará una selección, clasificación, evaluación y análisis de contenido del material recolectado (conocimientos empíricos, material impreso, medios gráficos, evidencias físicas y/o virtuales) que sirva de fuente teórica, conceptual y metodológica para la investigación, que permita de esta manera realizar la documentación de la implementación de un CSIRT para el Ministerio de Educación Nacional de Colombia y el sector de la educación. Además de ello, se hará uso de la técnica de indagación e interpretación de datos utilizando la encuesta a administradores IT como herramienta para determinar los incidentes de seguridad de la información que más se presentan en las organizaciones en las que desarrollan sus labores.

Este trabajo investigativo analizará el ámbito de aplicación del CSIRT en el Ministerio de Educación Nacional de Colombia y el sector de la educación, quienes al depender de entes tecnológicos para la prestación de sus servicios se hallan expuestos a ataques y explotación de vulnerabilidades que puedan generar afectaciones en el funcionamiento normal de sus sistemas.

El documento se desarrollará en cuatro fases, las cuales darán cumplimiento a los objetivos específicos planteados, dentro de dichas fases se realizarán tareas investigativas y se documentará todo lo concerniente al CSIRT del Ministerio de Educación Nacional de Colombia y el sector de la educación, por lo que se distribuirán de la siguiente forma:

6.1. Fase I: Simplificación de la Información

Para iniciar, se realiza el proceso de selección, recolección, consulta de información y referencias relacionadas con el tema de estudio objeto de esta investigación, para lo cual se buscó información en internet, bibliotecas virtuales, Google Académico, libros de seguridad de la

información y normas técnicas internacionales. Dentro de esta etapa se establecen como entradas los requerimientos y necesidades que surgen del problema identificado en la institución y como salida dentro de ésta son los documentos, que posiblemente servirán de referencias, experiencias adquiridas que se utilizará para fundamentar el diseño de la estrategia del CSIRT para el MEN y el Sector Educación, todo lo anterior sin descuidar el objetivo de esta etapa que es hacer más eficiente, manejable e interpretable la cantidad de información encontrada en la etapa de exploración y búsqueda de información.

6.2. Fase II: Estructuración de los Servicios del CSIRT

Se diseña un catálogo de servicios, donde se describe detalladamente los servicios reactivos, proactivos y de valor agregado que prestará el CSIRT del Ministerio de Educación Nacional de Colombia y el sector de la educación, logrando así que estos se adapten a la necesidad y exigencias de éste.

6.3. Fase III: Estructura Orgánica del CSIRT

Se detalla la estructura organizacional con la definición de los roles y perfiles del personal que integrará el CSIRT del Ministerio de Educación Nacional de Colombia y el Sector de la Educación, lo que permitirá la caracterización y asignación de las actividades de cada profesional o colaborador.

6.4. Fase IV: Políticas y procedimientos operacionales del CSIRT

Con la documentación de políticas y procedimientos operacionales que apoyarán las tareas y operaciones, se garantiza el manejo de un paso a paso en cada actividad a desarrollar en la implantación y puesta en operación del CSIRT.

7. CRONOGRAMA

Para la definición del cronograma se desarrolló un diagrama de Gantt, el cual se presenta en la Figura 6.

Figura 6

Cronograma

ID	Task Name	Resource Names	Duration	Start	Finish
1	FASE I: SIMPLIFICACIÓN DE LA INFORMACIÓN		268 days	Mon 17/04/23	Mon 13/05/24
2	Revisión de alcance de Proyecto	Luz Jenny González Peña; Cesar Aug	8 hrs	Mon 18/03/24	Mon 18/03/24
3	Levantamiento de información técnica	Luz Jenny González Peña; Cesar Aug	9 days	Tue 19/03/24	Sun 31/03/24
4	Identificación de Requerimientos	Luz Jenny González Peña; Cesar Aug	3 days	Wed 27/03/24	Sun 31/03/24
5	Identificación de las Necesidades para Implementar CSIRT en Ministerio de Educación y Sector	Luz Jenny González Peña; Cesar Augusto Monroy Rojas	3 days	Fri 26/04/24	Tue 30/04/24
6	Análisis del Nivel Inicial de Madurez del CSIRT	Luz Jenny González Peña; Cesar Aug	10 days	Mon 17/04/23	Sun 30/04/23
7	Generación de documento con resultados de estado actual del Ministerio de Educación frente a Ciberseguridad - CSIRT	Luz Jenny González Peña; Cesar Augusto Monroy Rojas	7 days	Fri 3/05/24	Mon 13/05/24
8	FASE II: ESTRUCTURACIÓN DE LOS SERVICIOS DEL CSIRT	Luz Jenny González Peña; Cesar Aug	262 days	Thu 27/04/23	Wed 15/05/24
9	Identificación de Servicios para un CSIRT	Cesar Augusto Monroy Rojas[80%]; Luz Jenny González Peña; Cesar Aug	10 days	Thu 27/04/23	Thu 11/05/23
10	Identificación de Servicios Básicos para el CSIRT	Luz Jenny González Peña; Cesar Aug	10 days	Thu 27/04/23	Thu 11/05/23
11	Identificación de Servicios Proactivos para un CSIRT	Luz Jenny González Peña; Cesar Aug	8 days	Mon 29/04/24	Wed 8/05/24
12	Identificación de Servicios Reactivos para un CSIRT	Luz Jenny González Peña; Cesar Aug	8 days	Mon 29/04/24	Wed 8/05/24
13	Identificación de Herramientas tecnológicas	Luz Jenny González Peña; Cesar Aug	6 days	Thu 2/05/24	Thu 9/05/24
14	Definición de Servicios y Herramientas a Implementar en CSIRT - Ministerio de Educación y Sector	Luz Jenny González Peña; Cesar Augusto Monroy Rojas	4 days	Fri 10/05/24	Wed 15/05/24
15	Generación de Documentos con catálogo de servicios y herramientas	Cesar Augusto Monroy Rojas; Luz Jenny González Peña; Cesar Aug	4 days	Fri 10/05/24	Wed 15/05/24
16	FASE III: ESTRUCTURA ORGANICA DEL CSIRT	Luz Jenny González Peña; Cesar Aug	33 days	Wed 10/04/24	Thu 23/05/24
17	Identificación de la Estructura Organizacional del Ministerio de Educación	Cesar Augusto Monroy Rojas; Luz Jenny González Peña; Cesar Aug	5 days	Thu 18/04/24	Tue 23/04/24
18	Identificación de la Estructura Organizacional del Sector Educación	Luz Jenny González Peña; Cesar Aug	8 days	Fri 19/04/24	Mon 29/04/24
19	Definición de la Estructura Organizacional del CSIRT Para Ministerio de Educación Nacional y el Sector	Luz Jenny González Peña; Cesar Augusto Monroy Rojas	7 days	Tue 30/04/24	Wed 8/05/24
20	Definición y Estructura de Funciones del CSIRT	Luz Jenny González Peña; Cesar Aug	9 days	Wed 10/04/24	Sun 21/04/24
21	Definición de los Roles y Perfiles del Recurso Humano para el CSIRT	Cesar Augusto Monroy Rojas; Luz Jenny González Peña; Cesar Aug	5 days	Tue 7/05/24	Mon 13/05/24
22	Elaboración del Diseño del Diagrama Organizacional del CSIRT	Luz Jenny González Peña; Cesar Aug	9 days	Tue 7/05/24	Fri 17/05/24
23	Generación de Documentos con Estructura Organizacional y Roles y Perfiles del CSIRT	Luz Jenny González Peña; Cesar Aug	5 days	Fri 17/05/24	Thu 23/05/24
24	FASE IV: POLITICAS Y PROCEDIMIENTOS OPERACIONALES DEL CSIRT		28 days	Thu 25/04/24	Thu 30/05/24
25	Identificación de Políticas y Procedimientos para un CSIRT	Luz Jenny González Peña; Cesar Aug	8 days	Mon 3/06/24	Wed 12/06/24
Page 1					
ID	Task Name	Resource Names	Duration	Start	Finish
26	Documentar Políticas para el CSIRT para el Ministerio de Educación Nacional y Sector	Luz Jenny González Peña; Cesar Augusto Monroy Rojas	13 days	Thu 13/06/24	Mon 1/07/24
27	Documentar Procedimientos para el CSIRT del Ministerio de Educación Nacional y Sector	Luz Jenny González Peña; Cesar Augusto Monroy Rojas	13 days	Thu 13/06/24	Mon 1/07/24
28	Cierre de Proyecto	Luz Jenny González Peña; Cesar Aug	2 days	Mon 1/07/24	Tue 2/07/24
Page 2					

Fuente: elaboración propia.

8. DESARROLLO DE LA INVESTIGACIÓN

8.1. Fase I: Simplificación de la Información

Para el análisis del nivel de madurez del CSIRT del sector Educación se empleará el modelo de madurez de administración de incidentes de seguridad SIM3 (*Security Incident Management Maturity Model*) del Open CSIRT Foundation, que permite verificar los niveles de madurez de una manera estándar, hacer comparaciones con diferentes CSIRT a nivel global con base en el GCMF (*Global CSIRT Maturity Framework*), comparar el estado actual con el perfil mínimo requerido para ser miembro del FIRST, así como con los diferentes niveles de madurez global de CSIRTs definidos por ENISA (*European Network and Information Security Agency*) para sus miembros acreditados.

Para la operación inicial del CSIRT Educación se deben cumplir con los niveles mínimos de madurez de todos los parámetros del modelo SIM3 requeridos por el FIRST para ser miembro de este órgano internacional, los cuales están definidos por el *Forum of Incident Response and Security Teams* (FIRST, 2014) y se pueden evaluar en SIM3 (s.f.), con enfoque en avanzar hacia el cubrimiento de los solicitado en el nivel de madurez básico solicitado por ENISA, del cual se contemplan muchos aspectos en la actualidad.

Con base en lo anteriormente planteado, y de acuerdo con la visión del estado del CSIRT del Sector Educación, efectuado a través de un ejercicio de validación con el equipo del MEN, se estableció que el instrumento a emplearse para validar el estado actual y el estado futuro del CSIRT para el Ministerio el sector Educación es el modelo de madurez SIM3 (s.f.), el cual se basa en cuatro dimensiones (Organización, Recursos Humanos, Herramientas y Procesos), de las que se analizarán criterios como la pertinencia y se señalarán los niveles a alcanzar (0 a 4).

A continuación, se describe de forma detallada el instrumento a desarrollar en el Ministerio de Educación para la definición del estado los niveles de madurez del Ministerio.

8.1.1. Descripción del Modelo SIM3

El SIM3 (Security Incident Management Maturity Model) es un modelo de consenso que sirve para medir la madurez de un CSIRT y es el criterio utilizado por diferentes organizaciones para determinar si un CSIRT cumple con las condiciones necesarias para ser miembro o no. Según Stikvoort (2019), se fundamenta en cuatro pilares: prevención, detección, resolución y control de

calidad y realimentación; su alcance está limitado a la respuesta a incidentes relacionados con la seguridad de las tecnologías de la información y la información misma.

El modelo está construido a partir de tres elementos básicos: parámetros de madurez, cuadrantes de madurez y niveles de madurez. Los parámetros son cantidades que son medidas en relación con la madurez. Cada parámetro pertenece a uno de los cuatro cuadrantes de madurez, que a su vez sirven como criterio de categorización para los parámetros. Los cuadrantes son: Organización, Recursos humanos, Herramientas y Procesos. La Tabla 3 expone los parámetros de cada uno de los cuadrantes.

Tabla 4

Parámetros de los cuadrantes

Organización	Recursos Humanos	Herramientas	Procesos
O-1: Mandato	H-1: Código de conducta/práctica/ética	T-1: Lista de recursos informáticos	P-1: Escalada al nivel de gobierno
O-2: Grupo de interés	H-2: Resistencia del personal	T-2: Lista de fuentes de información	P-2: Escalada a la función de prensa
O-3: Autoridad	H-3: Descripción del conjunto de habilidades	T-3: Sistema de correo electrónico consolidado	P-3: Escalada a la función legal
O-4: Responsabilidad	H-4: Formación interna	T-4: Sistema de seguimiento de incidentes	P-4: Proceso de prevención de incidentes
O-5: Descripción de los servicios	H-5: Formación técnica (externa)	T-5: Teléfono resistente	P-5: Proceso de detección de incidentes
O-6: No se define en el estándar	H-6: Formación en comunicación (externa)	T-6: Correo electrónico resistente	P-6: Proceso de resolución de incidentes
O-7: Descripción del nivel de servicio	H-7: Redes externas	T-7: Acceso a Internet resistente	P-7: Procesos específicos de incidentes
O-8: Clasificación de incidentes		T-8: Conjunto de herramientas de prevención de incidentes	P-8: Proceso de auditoría/retroalimentación

O-9: Integración en los sistemas CSIRT existentes		T-9: Conjunto de herramientas de detección de incidentes	P-9: Proceso de accesibilidad en caso de emergencia
O-10: Marco organizativo		T-10: Conjunto de herramientas para la resolución de incidentes	P-10: Presencia en Internet de las mejores prácticas
O-11: Política de seguridad			P-11: Proceso de manejo seguro de la información
			P-12: Proceso de las fuentes de información
			P-13: Proceso de divulgación
			P-14: Proceso de notificación
			P-15: Proceso estadístico
			P-16: Proceso de reuniones
			P-17: Proceso entre pares

Fuente: SIM3 (s.f.).

Los niveles de madurez, que son los que realmente se miden, se dividen en cinco categorías que se aplican a todos los parámetros:

- 0. = no disponible / indefinido / desconocido.
- 1. = implícito (conocido/considerado, pero no escrito, "entre los oídos").
- 2. = explícito, interno (escrito, pero no formalizado de ninguna manera).
- 3. = explícito, formalizado bajo la autoridad del jefe del CSIRT (sellado o publicado).
- 4. = explícito, auditado por la autoridad de los niveles de gobierno superiores al jefe del CSIRT (sujeto a un proceso de control/auditoría/aplicación).

Estos niveles no sólo se ajustan a las mejores prácticas en la definición de modelos de madurez, sino que permiten definir cuáles son las acciones que hay que llevar a cabo para pasar de un nivel a otro:

Tabla 5*Niveles de acción*

Nivel Original	Nivel Nuevo	Acción
0	1	Adicionar consideración - "escucha, somos conscientes de ello"
1	2	Adicionar descripción escrita - "lee, así es como lo hacemos"
2	3	Adicionar responsabilidad - "mira, esto es lo que estamos obligados a hacer"
3	4	Adicionar un mecanismo de control - "y así es como nos aseguramos de que se haga"

*Fuente: SIM3 (s.f.).***8.1.2. Premisas Básicas**

- La operación del CSIRT se ejecuta con autonomía administrativa, operativa y jurídica independiente al Ministerio de Educación Nacional.
- La financiación de la operación es responsabilidad de dicho Ministerio.
- La operación del CSIRT debe incluir acuerdos de niveles de servicio con su electorado.
- La operación del CSIRT debe basarse sobre los marcos de referencia del SIM y NIST / CSIRT.

8.1.3. Equipo Evaluador

Para la evaluación del modelo de madurez intervinieron las siguientes personas con sus respectivos equipos (ver Tabla 6).

Tabla 6*Equipo evaluador*

EQUIPO EVALUADOR		
SESIÓN	ROL	CORREO
ORGANIZACION	- Ligia Galvis - Jefe de la OTSI	<u>Ligia Del Carmen Galvis Amaya</u> <u>ligalvis@mineducacion.gov.co</u>
	- Ana Yised Castro Ortiz - Coordinador de Infraestructura	<u>Ana Yised Castro Ortiz</u> <u>acastroo@mineducacion.gov.co</u>
	- John Nepher Téllez - Coordinador de Aplicaciones	<u>John Nepher Tellez Montaña</u> <u>jtellez@mineducacion.gov.co</u>
	- Clara Eugenia Robayo - Líder Administrativo	<u>Clara Eugenia Robayo Vanegas</u> <u>crobayo@mineducacion.gov.co</u>
	- Luz Jenny González - Líder de Apoyo a Supervisión	<u>Luz Jenny Gonzalez Peña</u> <u>lugonzalez@mineducacion.gov.co</u>
	- Cesar Augusto Monroy - Gestor de Infraestructura	<u>Cesar Augusto Monroy Rojas</u> <u>cmonroy@mineducacion.gov.co</u>
HERRAMIENTAS	- Walter Alfonso Garzón - Gestor de Licenciamiento	<u>Walter Alfonso Garzon Hurtado</u> <u>wgarzon@mineducacion.gov.co</u>
	- Cesar Augusto Monroy - Gestor de Infraestructura	<u>Cesar Augusto Monroy Rojas</u> <u>cmonroy@mineducacion.gov.co</u>
	- Edgar Bautista Gamba – Líder Técnico	<u>Edgar Bautista Gamba</u> <u>ebautista@mineducacion.gov.co</u>
PROCESOS	- Mariela Saavedra Cruz - Gestor de Procesos	<u>Mariela Saavedra Cruz</u> <u>msaavedra@mineducacion.gov.co</u>
	- Clara Eugenia Robayo - Líder Administrativo	<u>Clara Eugenia Robayo Vanegas</u> <u>crobayo@mineducacion.gov.co</u>
	- Mónica Yulieth Álvarez - Gestión Contractual	<u>Monica Yulieth Alvarez Mora</u> <u>moalvarez@mineducacion.gov.co</u>
	- Luz Jenny González - Líder de Apoyo a Supervisión	<u>Luz Jenny Gonzalez Peña</u> <u>lugonzalez@mineducacion.gov.co</u>

Fuente: elaboración propia.

8.1.4. Organización

Con Organización nos referimos al conjunto de seres humanos, recursos, herramientas e infraestructuras que trabajan juntos de forma planificada. Los objetivos o fines de una organización que están dirigidos por un conjunto de metas estratégicas específicas. Como la SIM3 se centra en la madurez de la gestión de los incidentes de seguridad, tenemos que distinguir entre los objetivos estratégicos de toda la organización, por un lado, y los objetivos estratégicos específicos (del servicio) relacionados con la parte de la organización que gestiona los incidentes de seguridad, comúnmente denominada "CSIRT". Los siguientes parámetros "O" se refieren al mandato, la configuración y los servicios de ese CSIRT y al marco que conecta todos los aspectos organizativos.

Los resultados de las entrevistas realizadas se disponen en el Anexo 1.

8.1.5. Recursos Humanos

Por Recursos Humanos se entiende a las personas que trabajan juntas para proporcionar los servicios descritos en el área de Organización y satisfacer el mandato. Todas las personas que contribuyen a los objetivos de la organización (CSIRT) que gestiona los incidentes de seguridad, requieren una educación técnica y/o orientada a la gestión con una considerable formación en el puesto de trabajo, además de formación adicional para conocimientos más detallados como el análisis de *malware* o el análisis forense. Los parámetros "H" en esta área se refieren a los factores de importancia respecto al factor más importante en cualquier CSIRT: el "capital" humano de las personas que trabajan en él.

Los resultados de las entrevistas realizadas se disponen en el Anexo 2.

8.1.6. Herramientas

Por Herramientas se entiende al conjunto de programas, aplicaciones, servicios, instrumentos e incluso simples equipos, que son utilizados por el personal del que se habló en el área Humana, para alcanzar los objetivos y ofrecer los servicios definidos en el área de Organización. En concreto, son aquellas herramientas que permiten o mejoran la gestión de los incidentes de seguridad, mejorándola en tiempo, calidad y/o con mayor granularidad, es decir, "viendo" incidentes que antes podían pasar desapercibidos.

Los resultados de las entrevistas realizadas se disponen en el Anexo 3.

8.1.7. Procesos

Por Procesos se entienden los conjuntos de acciones secuenciadas lógicamente que son llevadas a cabo por humanos (área Humana) o herramientas automatizadas (área Herramientas) con el fin de lograr un resultado específico (definido en el área Organización). Todos los procesos pueden caracterizarse por una serie de atributos. Aplicando estos atributos también se determina el éxito de un proceso concreto (en la realización del trabajo) o el éxito de una organización concreta en la prestación de un servicio (por ejemplo, conseguir que este proceso sea correcto en todo momento). En las organizaciones maduras, los procesos están documentados y son medibles y repetibles. Para poder crecer y mejorar la eficacia de una organización también es importante crear procesos que sean adaptables.

Se trata específicamente de los procesos que apoyan la gestión de incidentes y cualquier otro servicio que el CSIRT ofrezca, por lo que se adopta el término "procesos" en el sentido más amplio de la palabra, de modo que en esta área de Procesos también se encontrarán procesos que a veces podrían etiquetarse como "política" o de otro tipo.

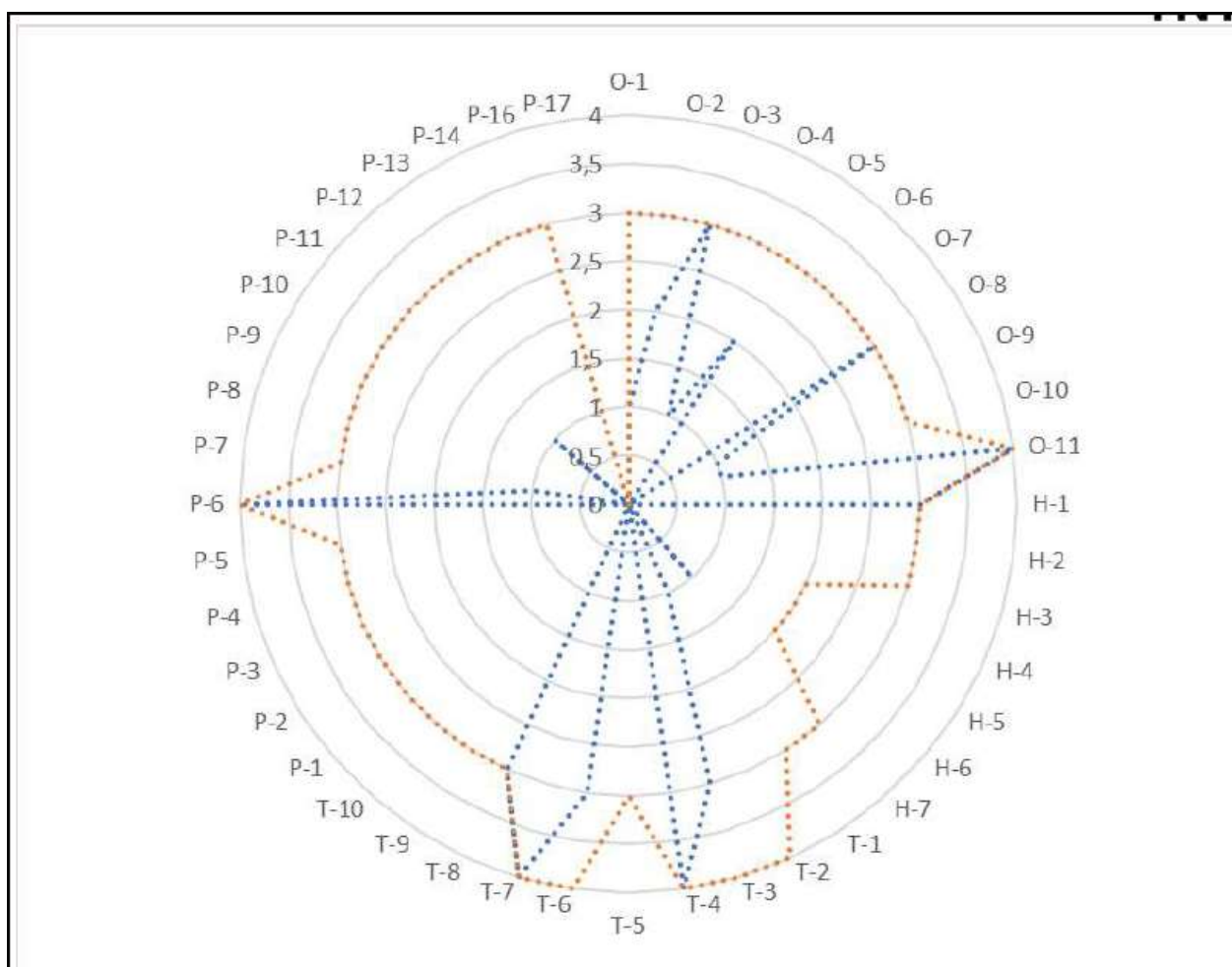
Los resultados de las entrevistas realizadas se disponen en el Anexo 4.

8.1.8. Resultados

El balance final de la evaluación se presenta a continuación (ver Figura 7).

Figura 7

Nivel de madurez del MEN para implementación de CSIRT. Comparación del Nivel de Madurez del CSIRT Sector Educación con lo exigido por el nivel básico de ENISA



Fuente: elaboración propia.

Las líneas azules resaltan el estado actual de madurez, en la que se encuentra la iniciativa CSIRT Educación, mientras que las líneas rojas denotan el estado futuro (*To be*) al cual se desea llegar, y del cual se basa la presente arquitectura y sus lineamientos. El modelo de referencia está conformado por un conjunto de capas horizontales (Dimensiones) y un conjunto de capas verticales/transversales o de soporte. Las capas horizontales se ocupan de habilitar las capacidades funcionales requeridas para el funcionamiento del CSIRT. Las cuatro capas verticales de soporte admiten la funcionalidad que proporcionan las capas horizontales. Cada aspecto del tiempo de ejecución de los diferentes componentes de la arquitectura se abstrae en una capa cuya responsabilidad es significativamente distinta de la de las otras capas.

8.2. Fase II: Definir el Catálogo de Servicios del CSIRT para el Ministerio de Educación Nacional y el Sector Educación

El CSIRT del sector de Educación estará constituido por el Ministerio de Educación Nacional y las Entidades Adscritas y Vinculadas (EAV). A su vez, prestará servicios básicos a todo el sector de educación en el país y servicios avanzados a las entidades del sector que se afilien a él. Con base en el estudio realizado en el nivel de madurez, se identificó que los servicios requeridos para la conformación del CSIRT del Ministerio y Sector Educación están divididos en dos grandes grupos: servicios proactivos y servicios reactivos, los cuales se analizan a continuación.

8.2.1. *Servicios Proactivos:*

Según la Universidad de Carnegie Mellon (Software Engineering Institute, 2023), los servicios proactivos son aquellos diseñados para anticipar, prevenir y mitigar posibles incidentes de seguridad antes de que ocurran. Para el CSIRT del MEN y Sector Educación se definen los siguientes:

- **Alertas de ciberseguridad:** El CSIRT debe enviar alertas que puedan ser relevantes para las Secretarías de Educación y las demás instituciones del sector, con el fin de prevenir a sus funcionarios sobre las amenazas que se pueden presentar en el sector o en otros sectores que pueden impactarlos.
- **Boletines de sensibilización y capacitación:** El CSIRT Educación compartirá temas de interés segmentados para la comunidad objetivo mediante boletines, alertas y campañas que permitan sensibilizar sobre aspectos clave de seguridad de la información y ciberseguridad que deben tenerse en cuenta. Además, fomentará la capacitación en los temas de interés para su comunidad, con ofertas de capacitación disponibles en el mercado que también podrán difundirse a través de boletines.
- **Compartir experiencias:** El CSIRT Educación servirá de espacio para el intercambio de información y casos de éxito sobre la protección del ciberespacio, como apoyo a la gestión de la seguridad y ciberseguridad de las Secretarías de Educación y otras instituciones del sector.
- **Monitoreo de seguridad (*security monitoring*):** El CSIRT de Educación implementará sistemas de detección de intrusos (IDS) y sistemas de prevención

de intrusos (IPS), con el fin de recolectar y analizar continuamente *logs* para identificar actividades sospechosas sobre las aplicaciones o sistemas de información del Ministerio y reportados por las Secretarías de Educación.

- **Evaluaciones de vulnerabilidad (*vulnerability assessment*):** De acuerdo con lo indicado por ENISA (2006) en su documento *Cómo crear un CSIRT paso a paso*, el CSIRT Educación debe realizar escaneos de vulnerabilidades o de virus para averiguar qué sistemas y redes son vulnerables. Dichas actividades se realizarán de forma periódica con el fin de identificar y corregir vulnerabilidades en los sistemas de información y aplicaciones.
- **Gestión de parches/actualizaciones de seguridad (*patch management*):** El CSIRT Educación debe asegurar que todos los sistemas de información y aplicaciones, iniciando desde su sistema operativo, estén al día con las más recientes actualizaciones de seguridad.
- **Análisis de inteligencia de amenazas:** Con base en el estándar establecido en ISO/IEC 27035:2016, titulado *Information technology — Security techniques — Information security incident management* (ISO, 2016), el CSIRT Educación recopilará información de diversas fuentes sobre nuevas amenazas y vulnerabilidades. y analizara patrones y tendencias en los datos de amenazas y con esta técnica anticiparse para posibles ataques.
- **Concienciación y capacitación en seguridad (*security awareness and training*):** El CSIRT de Educación ofrecerá entrenamiento continuo en seguridad a los contratistas y servidores públicos con el fin de que estos adopten una conciencia de seguridad para la realización de las actividades diarias. El Ministerio de Educación Nacional, como integrante del Comité de Seguridad Nacional Digital (Artículo 2.2.21.1.3.5., Decreto 338 de 2022), gestionará con las entidades que conforman el Comité de Seguridad Nacional la realización de ejercicios y simulacros para preparar al personal en la respuesta a incidentes.
- **Gestión de riesgos (*risk management*):** El CSIRT del sector Educación promoverá la adopción de una cultura que permita identificar y evaluar los riesgos de seguridad en las Secretarías de Educación con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad y la respuesta

proactiva y reactiva a posibles amenazas que puedan afectar confidencialidad, integridad o disponibilidad de los sistemas de información, infraestructura tecnológica y aplicaciones. Asimismo, el Ministerio de Educación Nacional realizará la identificación y evaluación de riesgos con el objetivo de desarrollar e implementar planes de mitigación.

8.2.2. Servicios Reactivos

Según el FIRST (2022), los servicios reactivos son aquellos que se activan en respuesta a un incidente de seguridad ya ocurrido. Dichos servicios sirven para gestionar y mitigar los efectos de los incidentes. Teniendo en cuenta el *Framework* de FIRST (2022), los servicios reactivos que se deben implementar en el CSIRT del Sector Educación son los siguientes:

- **Servicios de gestión de incidentes:** El CSIRT Educación contará con un servicio para gestión de incidentes y eventos de ciberseguridad que, desde su fase inicial (notificación y/o recepción), buscará su clasificación, triaje y análisis, para dar una respuesta oportuna que permita la definición de recomendaciones adecuadas en cuanto a la gestión mitigación, escalamiento o remediación de éstos y las actividades de contención, erradicación y recuperación que deben llevarse a cabo desde las instituciones que los estén sufriendo.
- **Compartir Indicadores de Compromiso (IOC):** El CSIRT Educación compartirá indicadores técnicos de compromiso, técnicas y procedimientos que están siendo utilizados por los atacantes, para ayudar a identificar, prevenir y mitigar un incidente de seguridad en las entidades del sector de educación. Los IOC son datos específicos que permitirán la identificación de una red o sistemas que pudieron haber sido comprometidos.

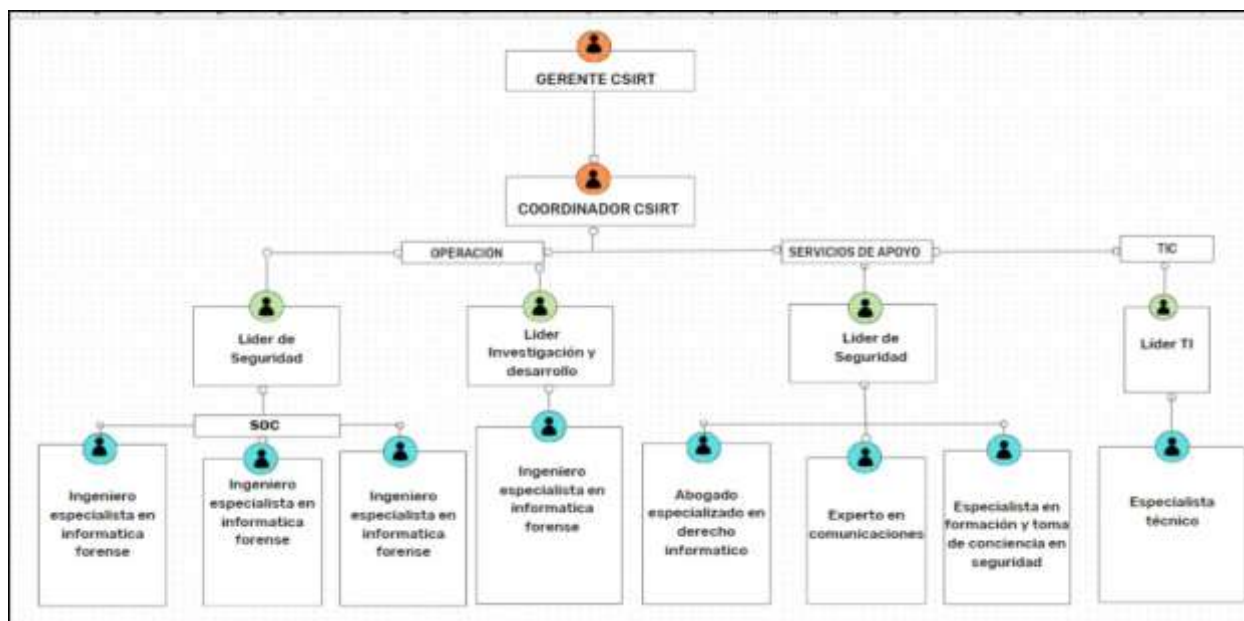
8.3. Fase III: Establecer la Estructura Organizacional y Perfiles que Integran el CSIRT para el Ministerio de Educación Nacional y el Sector Educación

Una vez revisada la documentación de definición de estructura organizacional/organizativa para un CSIRT consignada en *Cómo crear un CSIRT paso a paso* (ENISA, 2006) y *Guía práctica para CSIRTs* (Organización de Estados Americanos, 2023), se identifica que para el Ministerio de Educación Nacional es necesario definir una estructura organizacional/organizativa para la puesta en operación del CSIRT sectorial de Educación, la cual permitirá ordenar las actividades, los procesos y el funcionamiento de dicho CSIRT.

El Equipo de Respuesta a Incidentes de Seguridad Cibernética, CSIRT Sector de Educación, sujetará sus actuaciones a las disposiciones especiales que regulen su actividad o servicio, por lo cual la organización que se propone para comenzar con la creación de un CSIRT Sector Educación en el Ministerio de Educación es la siguiente:

Tabla 7

Organización CSIRT MEN y Sector Educación



Fuente: elaboración propia.

Tabla 8*Perfiles y competencias recurso humano*

PERFILES Y COMPETENCIAS RECURSO HUMANO			
PERFIL	AREA	FUNCIONES ESPECIFICAS	COMPETENCIAS
Gerente CSIRT	Dirección	<ul style="list-style-type: none"> * Liderazgo y gestión del CSIRT. * Definición de la estrategia del CSIRT. * Planificación, implementación y gestión de la respuesta a incidentes. * Gestión del presupuesto del CSIRT. * Garantía de la disponibilidad y el funcionamiento del CSIRT. * Comunicación con las partes interesadas. * Seguimiento de las tendencias en materia de seguridad informática. 	<ul style="list-style-type: none"> * Titulación en Ingeniería en telecomunicaciones, sistemas o carreras afines * Postgrado en Gerencia (MBA, MMoT o similar). * Certificaciones en Seguridad Informática (CISSP, CISM, CISA o similar).
Líder/Coordinador CSIRT	Dirección	<ul style="list-style-type: none"> * Gestión del equipo CSIRT * Habilidad para la planificación estratégica y la gestión de proyectos. * Capacidad para liderar y motivar a un equipo. * Conocimiento de las herramientas y tecnologías de seguridad informática. * Excelentes habilidades de comunicación oral y escrita. * Capacidad para tomar decisiones bajo presión. * Habilidad para la planificación estratégica y la gestión de proyectos. * Capacidad para liderar y motivar a un equipo. * Conocimiento de las herramientas y tecnologías de seguridad informática. 	<ul style="list-style-type: none"> * Titulación en Ingeniería en telecomunicaciones, sistemas o carreras afines * Postgrado en Gerencia (MBA, MMoT o similar). * Certificaciones en Seguridad Informática (CISSP, CISM, CISA o similar).

		* Excelentes habilidades de comunicación oral y escrita.	
Líder de seguridad CISO	Operaciones	<ul style="list-style-type: none"> * Experiencia en gestión de incidentes de seguridad. * Habilidades de liderazgo y toma de decisiones. * Conocimientos técnicos en seguridad informática. * Capacidad para gestionar equipos multidisciplinares. * Habilidades de comunicación y negociación. 	<ul style="list-style-type: none"> * Titulación en Ingeniería en telecomunicaciones, sistemas o carreras afines * Maestría o especialización en seguridad informática * Certificaciones en Seguridad Informática (CISSP, CISM, CISA o similar).
Analista de seguridad	Operaciones	<ul style="list-style-type: none"> * Experiencia en análisis de malware, redes y sistemas. * Conocimientos de técnicas de investigación y análisis de incidentes. * Habilidades para la identificación y clasificación de vulnerabilidades. * Capacidad para trabajar de forma autónoma y en equipo. 	<ul style="list-style-type: none"> * Titulación en Ingeniería en telecomunicaciones, sistemas o carreras afines * Maestría en seguridad informática * Certificaciones en Seguridad Informática (CISSP, CISM, CISA o similar).
Experto en inteligencia de amenazas	Operaciones	<ul style="list-style-type: none"> * Comprensión profunda del panorama de las amenazas, incluyendo actores, vectores y técnicas. * Habilidad para recopilar, analizar y procesar grandes volúmenes de datos de diferentes fuentes. Capacidad para identificar y evaluar las amenazas emergentes. * Habilidad para desarrollar e implementar estrategias de mitigación de riesgos. * Capacidad para comunicar de manera efectiva los riesgos de seguridad a las 	<ul style="list-style-type: none"> * Titulación en Ingeniería Informática, Seguridad Informática o similar. * Máster en Inteligencia de Amenazas o Ciberseguridad. * Certificaciones en Seguridad Informática (CISSP, CISM, CISA, BCM, ISO 27001 o similar).

		<p>partes interesadas.</p> <ul style="list-style-type: none"> * Conocimiento de las herramientas y tecnologías de inteligencia de amenazas. * Habilidad para trabajar de forma independiente y como parte de un equipo. 	
Ingeniero especialista en Informática Forense	Operaciones	<ul style="list-style-type: none"> * Conocimientos profundos en sistemas operativos, redes y seguridad informática. * Experiencia en la investigación y análisis de delitos informáticos. * Habilidad para la recuperación de datos y la preservación de la evidencia digital. * Conocimiento de las herramientas y técnicas de análisis forense. * Capacidad para redactar informes técnicos y periciales. * Habilidad para comunicar de manera efectiva los resultados de las investigaciones. * Capacidad para trabajar de forma independiente y como parte de un equipo. 	<ul style="list-style-type: none"> * Titulación en Ingeniería de Sistemas, software, telecomunicaciones o carreras afines * Maestría o especialización en informática forense * Cursos de especialización en informática forense u otra área de seguridad informática y aseguramiento de información.
Ingeniero especialista de respuesta a incidentes	Operaciones	<ul style="list-style-type: none"> * Experiencia en la implementación de medidas de respuesta a incidentes. * Conocimientos de sistemas operativos, redes y aplicaciones. * Habilidades para la resolución de problemas y la gestión de crisis. * Capacidad para trabajar bajo presión. 	<ul style="list-style-type: none"> * Titulación en Ingeniería en telecomunicaciones, sistemas o carreras afines * Maestría o especialización en seguridad informática * Cursos de especialización en seguridad informática y respuesta a incidentes de

			seguridad de la información.
Especialista en formación y toma de conciencia en seguridad	Operaciones	<ul style="list-style-type: none"> * Sólida formación en seguridad informática. * Habilidades pedagógicas y de comunicación. * Capacidad para desarrollar e impartir cursos de formación. * Conocimiento de las diferentes técnicas de aprendizaje. * Habilidad para evaluar el impacto de la formación. * Conocimiento de las últimas tendencias en seguridad informática. 	<ul style="list-style-type: none"> * Titulación en Ingeniería en telecomunicaciones, sistemas o carreras afines * Maestría o especialización en seguridad informática * Itil v4, Auditor Líder ISO 27001 * Formación en pedagogía y didáctica.
Líder de TI	Tecnología de información	<ul style="list-style-type: none"> * Sólida formación en tecnologías de la información y la comunicación (TIC). * Experiencia en la gestión de equipos de TI. * Habilidades de liderazgo y toma de decisiones. * Capacidad para la planificación estratégica y la gestión de proyectos. * Conocimiento del negocio y las necesidades de los usuarios. * Habilidades de comunicación y negociación. * Capacidad para adaptarse a los cambios y las nuevas tecnologías. * Visión estratégica y capacidad para anticipar las tendencias del mercado. 	<ul style="list-style-type: none"> * Titulación en Ingeniería de Sistemas, software, telecomunicaciones o carreras afines * Maestría o especialización en seguridad informática * Certificaciones en seguridad cibernética (CISSP, CISM, CISA o similar).
Especialista técnico	Tecnología de información	<ul style="list-style-type: none"> * Conocimientos de sistemas operativos, redes y aplicaciones. * Habilidades para la resolución de problemas y la 	<ul style="list-style-type: none"> * Titulación en Ingeniería de Sistemas, software, telecomunicacion

		gestión de crisis. * Capacidad para trabajar bajo presión.	es o carreras afines * Conocimiento de desarrollo de sistemas, familiaridad con al menos tres lenguajes de programación (Python, BashShell, PHP, C++, Java, etcétera).
Abogado especializado en derecho informático	Servicios de Apoyo	* Sólida formación en derecho civil, mercantil y administrativo. * Comprensión profunda del derecho informático y las nuevas tecnologías. * Capacidad de análisis y resolución de problemas complejos. * Habilidad para la negociación y la redacción de contratos. * Dominio de las herramientas informáticas y de la investigación jurídica online. * Capacidad para adaptarse a un entorno legal en constante cambio.	* Título de Abogado. * Máster en Derecho Informático o especialidad en derecho digital. * Cursos y formación específica en las áreas de especialización.
Experto en comunicaciones	Servicios de Apoyo	* Experiencia en redacción de informes técnicos y comunicados de prensa. * Habilidades para la comunicación oral y escrita. * Conocimientos en seguridad informática y gestión de incidentes.	* Titulación en Periodismo, Comunicación Social, Publicidad o Relaciones Públicas. * Máster en Comunicación Corporativa, Marketing Digital o Comunicación Política.

Fuente: elaboración propia.

8.3.1. Horarios Iniciales de Atención

El CSIRT Educación trabajará inicialmente lunes a domingo de 00:00 a.m. a 23:59 p.m. Sus canales de comunicación virtual estarán disponibles continuamente para recibir solicitudes y comunicaciones.

8.3.2. Autoridad

El CSIRT coordina los incidentes de seguridad relacionados con sus miembros y con el Sector Educación. En su función de coordinar y apoyar a sus miembros en la preparación y respuesta ante eventos e incidentes de ciberseguridad que se puedan presentar, este CSIRT realizará recomendaciones a los miembros, pero no asume la responsabilidad de la gestión, la cual permanece en cabeza de los afectados.

8.3.3. Responsabilidad

El ámbito de responsabilidad de este CSIRT es el definido en su misión, visión y servicios para el sector de educación de Colombia.

8.3.4. Dimensionamiento del CSIRT

Tabla 9

Dimensionamiento del CSIRT

DIMENSIONAMIENTO DEL CSIRT			
MÓDULO	ÁREA	AREA DE OPERACIÓN	DESCRIPCIÓN
ALCANCE	Ámbito de aplicación		Comunidad objetivo (Secretarías de Educación) Identificación de necesidades y objetivos Alcance y responsabilidades del CSIRT Procesos y procedimientos
RIESGOS	Evaluación y tratamiento de riesgos	Gerente Coordinador Líder CISO	Riesgos y capacidad de respuesta CSIRT Métricas Mapa de riesgos Registro de incidentes
SERVICIOS	Reactivos	Analista nivel 1 de incidentes Analista nivel 2 de incidentes	Gestión de vulnerabilidades Identificación de vulnerabilidades Pruebas de calidad y software Reportes y recomendaciones Gestión de códigos maliciosos Análisis de código malicioso Soporte a usuarios Gestión y tratamiento de

			<p>incidentes de seguridad de la información</p> <p>Identificación de incidentes</p> <p>Tratamiento de incidentes</p> <p>Soporte a la respuesta a incidentes</p> <p>Reporte de incidentes</p> <p>Levantamiento de estadísticas</p> <p>Alertas de acción</p>
SERVICIOS	Proactivos	Comunicaciones Analista nivel 3 de incidentes	<p>Sistema de alertas tempranas</p> <p>Monitoreo de portales web</p> <p>Boletines de seguridad informática</p> <p>Desarrollo de herramientas</p> <p>Prospectiva tecnológica</p> <p>Formación</p> <p>Concientización</p> <p>Asesoría Legal</p> <p>Gestión de Riesgos</p> <p>Consultoría</p> <p>Coordinación de recuperación de desastres</p>
RECURSO HUMANO	Número de personas en el equipo Habilidades y experiencia	<p>Coordinador CSIRT</p> <p>Analista nivel 1 de incidentes</p> <p>Analista nivel 2 de incidentes</p> <p>Analista nivel 3 de incidentes</p>	<p>Costos de personal:</p> <p>Salarios, beneficios y formación del equipo CSIRT</p> <p>Dirección General</p> <p>Auditoría</p> <p>Dependencia</p>

			Jurídica Secretaría General Finanzas Recursos Humanos Dirección de operaciones Gestión de incidentes Apoyo Dirección estratégica
INFRAESTRUCTUR A	Instalaciones, equipamiento, diseño de red	Salas de reuniones Laboratorio Forense Salas de formación (capacitación) Sala de crisis Laboratorio técnico Sala de custodia de evidencia	Sistema de detección de intrusiones (IDS) Sistema de prevención de intrusiones (IPS) Herramientas de análisis de vulnerabilidades Herramientas de respuesta a incidentes y análisis forense Herramientas de gestión de tickets y comunicación Espacio físico adecuado para el equipo CSIRT Acceso a la información y sistemas críticos Conectividad a internet de alta velocidad Entorno seguro para la gestión de incidentes Costos de herramientas Licencias, mantenimiento y actualizaciones de las

			herramientas de seguridad. Costos de infraestructura: Alquiler de espacio, equipamiento y conectividad.
MARCO LEGAL	Normatividad vigente	Abogado especializado en derecho informático Derivado de la operación diaria y cuando el CSIRT lo requiera	CONPES 3701 de 2011 CONPES 3854 de 2016 Ley 1273 de 2009 Ley 1581 de 2012 Ley 1341 de 2009 Ley 527 de 1999 Ley 679 del 2000 Ley 1712 de 2014 Actos administrativos y decretos
MARCO LEGAL	Normatividad vigente	Ley 1341 de 2009 Ley 1273 de 2009 Ley 527 de 1999 Ley 679 del 2000 CONPES 3701 de 2011 Ley 1581 de 2012 Ley 1712 de 2014 CONPES 3854 de 2016 Decreto 1078 de 2018 CONPES 3995 de 2020 Decreto 338 de 2022	

Fuente: elaboración propia.

8.4. Fase IV: Documentar las Políticas y Procedimientos Operacionales para la Puesta en Funcionamiento del CSIRT del Ministerio de Educación Nacional y el Sector Educación

Como parte del análisis realizado para la implementación del CSIRT Sector Educación, y con el fin de definir la puesta en operación de éste, se hace necesario el establecimiento de políticas y procedimientos que permitan el manejo seguro de la información del Ministerio de Educación Nacional, como también de las entidades del Sector Educación. El no cumplimiento de éstos puede ocasionar pérdidas totales, parciales, fugas, eliminación y hasta alteración de los datos críticos de una de las entidades, pudiendo incurrir en delitos y sanciones judiciales. En aras de establecer las políticas y procedimientos, se tomó como referencia lo planteado por la Organización de Estados Americanos (2023), cuyas recomendaciones se desarrollan a continuación.

Como uno de los primeros pasos para la definición de las políticas y procedimientos se debe establecer la Visión y Misión del CSIRT del sector de Educación, por lo que a continuación se definen estos conceptos.

8.4.1. Misión

Coordinar y apoyar a los miembros del CSIRT Educación en la preparación y respuesta ante eventos e incidentes de ciberseguridad que se puedan presentar, adicionalmente, aportar a una gestión activa de las ciberamenazas que puedan afectar a las instituciones que lo conformen.

8.4.2. Visión

En el 2026, el CSIRT Educación debe ser reconocido como un referente nacional e internacional en la gestión y coordinación de acciones efectivas para disminuir el riesgo e impacto de los incidentes de ciberseguridad en el Sector Educación, al coordinar soluciones técnicas, compartir experiencias y casos de éxito, e intercambiar la información necesaria para la protección del ciberespacio.

8.4.3. Comunidad Objetivo

El CSIRT del Sector Educación estará constituido por el Ministerio de Educación Nacional y las Secretarías de Educación en su fase inicial. Posteriormente, se integrarán las Entidades Adscritas y Vinculadas (EAV). A su vez, prestará sus servicios básicos a todo el sector de educación en el país y servicios avanzados a las entidades del sector que se afilien a él.

8.4.4. Políticas y Procedimientos

8.4.4.1. Política de Clasificación de Información.

Plantea las directrices que permitan a los miembros, operadores y analistas del grupo del CSIRT del Sector Educación asegurar que la información destinada al manejo de incidentes se canalice a través de un único punto de contacto independiente del medio en el que llegue (correo electrónico, teléfono, entre otros) y definir el alcance que puede tener la información según su clasificación TLP (*Traffic Light Protocol*).

8.4.4.2. Política de Divulgación de Información.

Plantea las directrices que permitan definir qué información puede ser revelada, ¿a quién?, ¿cómo? y ¿en qué circunstancias?, incluyendo las partes interesadas, miembros del CSIRT Educación, otros órganos del Gobierno, o incluso otros miembros de este CSIRT. La manera en que se comparta la información se hará de acuerdo con su nivel de clasificación.

8.4.4.3. Política de Gestión de Incidentes.

Plantea las directrices que permitan definir quién tiene la responsabilidad para manejar qué tipo de incidente de ciberseguridad, quién puede ser llamado para apoyar en la implementación de la respuesta en las otras áreas de este CSIRT y cómo deben ser clasificados los incidentes de acuerdo con la taxonomía definida por el ColCERT.

8.4.4.4. Procedimiento de Gestión de Incidentes.

Define cómo se gestionan los incidentes de ciberseguridad que sean reportados por los miembros del CSIRT Educación y demás entidades interesadas, a través de los medios de contacto establecidos con el fin de analizar los incidentes, identificar las causas e impactos, apoyar la gestión, el escalamiento y retroalimentar a la entidad con recomendaciones para que realice las acciones que le permitan prevenir y/o mitigar el riesgo.

8.4.4.5. Política de Seguridad de Datos y Protección de Datos.

Este CSIRT define cómo se gestiona la protección de los datos que se manejan dentro del CSIRT, teniendo en cuenta la protección de datos según la Ley 1781 (2012) y los lineamientos de seguridad digital que brinda el Decreto 1008 (2018). El fin primordial de esta política es la identificación y caracterización de los datos por su nivel de importancia (público, privado,

semiprivado, sensible) para proteger los datos que se manejan dentro del CSIRT y definiendo medidas de seguridad que deben ser incorporadas en las bases de datos. Con la adopción de esta política se garantizará la confidencialidad e integridad de los datos.

8.4.4.6. Procedimientos de *Back Ups* y Respaldos de la Información.

Define los pasos para asegurar que los datos del CSIRT estén protegidos contra pérdidas accidentales, corrupción o desastres; el procedimiento definirá los tipos de *backup*, retención y restauración de la información, con el objetivo de evitar pérdidas de información y garantizando la capacidad de recuperación ante incidentes adversos.

9. REFERENCIAS

- Almanza, J. (2023). XXIII Encuesta Nacional de Seguridad Informática. Valor y beneficio de la ciberseguridad. *Sistemas*, 169, 18-93.
<https://sistemas.acis.org.co/index.php/sistemas/article/view/Investigaci%C3%B3n%20169>
- Axelos. (s.f.). *What is ITIL?* Axelos. <https://www.axelos.com/certifications/itil-service-management>
- Banco Interamericano de Desarrollo. (2020). *Strengthening Cybersecurity in the Digital Era: The Role of National CSIRTs*. IADB. <https://www.iadb.org/en/publications/strengthening-cybersecurity-national-csirts>
- Cardona, L. y Uribe, Andrés. (2015). *Sistema de gestión de incidentes de seguridad informática para corbeta* [tesis de posgrado, Universidad de San Buenaventura]. Repositorio Institucional USB.
<https://bibliotecadigital.usb.edu.co/server/api/core/bitstreams/46c07f61-6dfc-4491-8eb0-c8edecc3cd19/content>
- Congreso de Colombia. (1999, 18 de agosto). *Ley 527 de 1999. Uso de mensajes de datos, del comercio electrónico y firmas digitales*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276>
- Congreso de Colombia. (2000, 14 de julio). *Ley 594 de 2000. Ley General de Archivos*.
<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4275>
- Congreso de Colombia. (2001, 3 de agosto). *Ley 679 de 2001. Estatuto para prevenir la explotación sexual con menores*.
http://www.oas.org/juridico/spanish/cyb_col_ley_679_2001.pdf
- Congreso de Colombia. (2005, 8 de julio). *Ley 962 de 2005. Racionalización de procedimientos administrativos*.
<http://www.aguasdebuga.net/intranet/sites/default/files/Ley%20962%20de%202005>
- Congreso de Colombia. (2007, 16 de julio). *Ley 1150 de 2007. Medidas para la eficiencia y transparencia en la contratación pública*.
<https://www.mintransporte.gov.co/descargar.php?idFile=711>
- Congreso de Colombia. (2009, 5 de enero). *Ley 1273 de 2009. Protección de la Información y Datos*. <http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf>

- Congreso de Colombia. (2009, 6 de marzo). *Ley 1712 de 2014. Ley de transparencia y del derecho a acceso a la información pública nacional*.
<http://www.anticorrupcion.gov.co/SiteAssets/Paginas/Publicaciones/ley-1712.pdf>.
- Congreso de Colombia. (2009, 30 de julio). *Ley 1341 de 2009. Organización de las TIC*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913>
- Congreso de Colombia. (2011, 18 de enero). *Ley 1437 de 2011. Código de Procedimiento Administrativo*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=41249>
- Congreso de Colombia. (2011, 12 de octubre). *Ley 1480 de 2011. Estatuto del Consumidor*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44306>
- Congreso de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012. Protección de datos personales*.
<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Congreso de Colombia. (2018, 24 de julio). *Ley 1928 de 2018. Se adopta el Convenio sobre la Ciberdelincuencia*. <https://www.suin-juriscal.gov.co/viewDocument.asp?id=30035501>
- CONPES. (2011). *Documento CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa*. Min-TIC. https://www.mintic.gov.co/portal/604/articulos-3510_documento.pdf.
- CONPES. (2016). *Documento CONPES 3854. Política nacional de seguridad digital*. DNP.
<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>
- CONPES. (2020). *Documento CONPES 3995. Política nacional de confianza y seguridad digital*. DNP. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf>
- CyberTalk. (s.f.). *What's next for the education sector: cyber-security*. CyberTalk.
<https://www.cybertalk.org/education-sector-cyber-security>
- Departamento Administrativo Nacional de Estadística. (2022). *Encuesta de Tecnologías de la Información y las Comunicaciones en Empresas (ENTIC Empresas) 2020*. DANE.
https://www.dane.gov.co/files/investigaciones/boletines/entic/bol_entic_empresas_2020.pdf
- ENISA. (2006). *Cómo crear un CSIRT paso a paso*. ENISA.
https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

- Escuela Europea de la Excelencia. (2019). *El Anexo A y los controles de seguridad en ISO 27001*. Escuela Europea de la Excelencia. <https://www.escuelaeuropeaexcelencia.com/2019/05/el-anexo-a-y-los-contr>.
- FIRST. (2014). *Requirements and assessment (version 2.5)*. FIRST. <https://www.first.org/membership/site-visit-v2.5.pdf>
- FIRST. (2015). *Historia*. FIRST. <https://www.first.org/about/history>
- FIRST. (2019). *CSIRT Teams*. FIRST. <https://www.first.org/members/teams/?#>
- Gorgona, L. (2018). *Primera respuesta: antes de que llegue la policía*. https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf
- IT Governance Institute-COBIT. (2017). *Marco Referencial*. ULADECH. http://files.uladech.edu.pe/docente/02659781/CAT/S07/02_03MarcoReferencial.pdf.
- Kali Linux. (2019). *Kali Linux By Offensive Security*. Kali. <https://www.kali.org/>
- Lumu Technologies. (2021). *The needed breakthrough in cybersecurity*. Lumu. <https://lumu.io/wp-content/uploads/2021/01/lumu-cybersecurity-ebook.pdf>
- MINTIC. (2014). *Guía para la Gestión y Clasificación de incidentes de seguridad de la información*. Min-TIC. https://www.mintic.gov.co/gestionti/615/articulos-5482_G21_Gestion_Incidentes.pdf
- Montoya, C. y Boyero, M. (2012). El CRM como herramienta para el servicio al cliente en la organización. *Revista Científica Visión de Futuro*, 17(1), 130-151. <https://www.redalyc.org/pdf/3579/357935480005.pdf>
- NIST. (2008). *Computer security incident handling guide (NIST 800-61)*. NIST Department of Commerce-USA. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r1.pdf>
- Organización de los Estados Americanos. (2016). *Buenas Prácticas para establecer un CSIRT nacional*. OAS. <https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf>
- Policía Nacional. (2012). *Balance del cibercrimen en Colombia*. CAI Virtual. https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

Presidencia de la República de Colombia. (2012, 10 de enero). *Decreto Ley 019 de 2012. Normas anti-trámite.*

http://www.secretariassenado.gov.co/senado/basedoc/decreto_0019_2012.html

Presidencia de la República de Colombia. (2017, 11 de septiembre). *Decreto 1499 de 2017. Sistemas de gestión.*

https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=83433

Presidencia de la República de Colombia. (2018, 14 de junio). *Decreto 1008 de 2018. Gobierno digital.* <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902>

Presidencia de la República de Colombia. (2022, 8 de marzo). *Decreto 338 de 2022. Gobernanza de la seguridad digital.*

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>

RTIR. (s.f.). *Best Practical*. Best Practical. <https://bestpractical.com/rtir>.

SIM3. (s.f.). *SIM3 Self Assessment Tool*. SIM3. <https://sim3-check.opencsirt.org/#/>

Software Engineering Institute. (2023). *Best practices for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University.

Stikvoort, D. (2019). *SIM3: Security Incident Management Maturity Model*. Open CSIRT Foundation. <http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf>

Superintendencia de Industria y Comercio. (s.f.). *Delegatura de protección de datos personales*. SIC. <https://www.sic.gov.co/que-es-la-delegatura-datos-personales>

Superintendencia de Industria y Comercio. (2014). *Resolución 8934 de 2014*. SUIN. <http://www.suin-juriscal.gov.co/viewDocument.asp?id=4041484>.

United States-Department of Defense. (2015). *Department Of Defense Trusted Computer System Evaluation Criteria*. CSRC. <https://csrc.nist.gov/csrc/media/publications/conference>.

Vargas, Z. (2009). La investigación aplicada: una forma de conocer las realidades con evidencia científica. *Educación*, 33(1), 155-165. <https://www.redalyc.org/pdf/440/440150>.

10. ANEXOS

Anexo 1. Entrevistas cuadrante Organización

O-1: MANDATO

Cuadrante:	Organización	Parámetro:	O-1: Mandato							
Su CSIRT necesita derivar la justificación de su existencia, su asignación de algún nivel superior de gobierno. Esto se llama el mandato del CSIRT. Idealmente, el mandato proviene de los niveles más altos de gobierno en su entorno específico. A veces proviene inicialmente de un nivel inferior, como el jefe de TI de la empresa o la dirección de un ministerio. Pero preferiblemente procede de los niveles más altos, como el consejo de administración o el gobierno estatal, y en este último caso también puede estar anclado en la legislación. ¿Tiene su CSIRT un mandato de este tipo?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos un mandato escrito aprobado por la dirección de nuestro equipo.										
Evidencia: DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos un mandato escrito aprobado por la dirección de nuestro equipo.										
El CSIRT debe ser creado formalmente. Hoy en día se ha definido en actas de Reuniones del MEN y en el documento de creación y evolución del CSIRT. Se debe revisar si se va a emitir directiva ministerial u otro documento que lo formalice de mejor manera.										

O-2: GRUPO DE INTERÉS

Cuadrante:	Organización	Parámetro:	O-2: Grupo de Interés							
La circunscripción de su CSIRT se define como la "base de clientes", el grupo objetivo para el que realiza el trabajo del CSIRT. Este grupo puede ser su propia organización o empresa - entonces se dice que su grupo es interno a su organización. Su equipo también puede tener una base de clientes externa a su propia organización, como por ejemplo las universidades de su país cuando sirve a la comunidad académica, o una base de clientes de pago, o todos los municipios de su país. ¿Tiene su CSIRT un grupo de interés bien definido?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una definición de circunscripción escrita aprobada por la dirección de nuestro equipo.										
Evidencia:										
DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA.										
COMUNIDAD OBJETIVO: El CSIRT del sector de Educación estará constituido por el Ministerio de Educación Nacional y las Entidades Adscritas y Vinculadas – EAV. A su vez, prestará sus servicios básicos a todo el sector de educación en el país, y servicios avanzados a las entidades del sector que se afilien a él.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una definición de circunscripción escrita aprobada por la dirección de nuestro equipo.										

O-3: AUTORIDAD

Cuadrante:	Organización	Parámetro:	O-3: Autoridad							
La autoridad de un CSIRT es lo que su equipo está *permitido* hacer hacia su circunscripción, para que pueda cumplir con su mandato. La autoridad es básicamente los poderes que han sido invertidos en su CSIRT. Algunos equipos, como especialmente los equipos de coordinación con una circunscripción externa, tienen pocos poderes, poca autoridad y tal vez sólo pueden dar consejos a la circunscripción. Mientras que otros CSIRT tienen autoridad para hacer cumplir las medidas. Qué y cómo se puede escalar, también forma parte de esto. ¿Qué autoridad tiene su equipo?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una definición de autoridad por escrito aprobada por la dirección de nuestro equipo.										
Evidencia:										
DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA.										
El CSIRT coordina los incidentes de seguridad relacionados con sus miembros y con el sector educación.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una definición de autoridad por escrito aprobada por la dirección de nuestro equipo.										

O-4: RESPONSABILIDAD

Cuadrante:	Organización	Parámetro:	O-4: Responsabilidad							
La responsabilidad de un CSIRT es lo que se espera que su equipo haga hacia sus integrantes, para que pueda cumplir con su mandato. La responsabilidad es lo que aquellos que le han otorgado el mandato esperan que haga y realice. Por lo general, un CSIRT tiene más responsabilidad que autoridad, pero si la brecha entre la responsabilidad y la autoridad es demasiado grande, puede producirse un desajuste, en el que se espera demasiado con muy poco poder para lograrlo realmente. ¿Qué responsabilidad tiene su equipo?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una definición de responsabilidad por escrito aprobada por la dirección de nuestro equipo.										
Evidencia: DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA. RESPONSABILIDAD: El ámbito de responsabilidad de este CSIRT es el definido en su misión, visión, servicios para la comunidad objetivo.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una definición de responsabilidad por escrito aprobada por la dirección de nuestro equipo.										

O-5: DESCRIPCIÓN DE LOS SERVICIOS

Cuadrante:	Organización	Parámetro:	O-5: Descripción de los Servicios				
<p>Mientras que la "responsabilidad" suele formularse como una forma de alto nivel de las expectativas de su CSIRT, la descripción de los servicios de su equipo es la forma de dar forma a eso en una lista concisa de los servicios que ofrece a su circunscripción, que muy probablemente incluirá la gestión/respuesta a incidentes, pero también posiblemente la gestión de vulnerabilidades, el análisis de malware, la concienciación y potencialmente otros. La lista original más popular de posibles servicios a seleccionar era la del Manual de CSIRT de CERT/CC (también adoptada por ENISA y Trusted Introducer). Desde 2017, el Marco de Servicios CSIRT de FIRST se ha convertido en un estándar de facto, porque ofrece un enfoque bien estructurado y granular, especialmente en la versión 2.1 más reciente. Sea cual sea la fuente que utilices, es importante hacer una selección clara de aquellos servicios que debes o deberías ofrecer en función de tu mandato, autoridad y responsabilidad, y teniendo en cuenta los recursos que tienes disponibles. Todo esto conduce a una lista de servicios, y es importante considerar que al menos su circunscripción necesita tener acceso a esta lista, incluyendo la información de contacto de su equipo y las ventanas de servicio. Se aconseja encarecidamente utilizar rfc2350 como una forma estandarizada de publicar una lista de alto nivel de sus servicios, información de contacto y ventanas de servicio incluso a Internet en general, ya que para cualquier CSIRT es importante que se sepa cómo llegar a ellos, ya que asumen la responsabilidad de (parte de) la seguridad de su circunscripción, que es parte de Internet en general - al adoptar rfc2350 asegúrese de tener una versión en inglés disponible públicamente (junto a una en su idioma nativo). ¿Tiene su equipo una descripción clara del servicio?</p> <p>Requisito mínimo: Contiene la información de contacto del CSIRT, las ventanas de servicio, una descripción concisa de los servicios ofrecidos y la política del CSIRT sobre el manejo y divulgación de la información. Disponible públicamente en inglés.</p>							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
Tenemos una descripción de servicio escrita aprobada por la dirección de nuestro equipo, y se ha puesto a disposición de nuestra circunscripción.							
<p>Evidencia: DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA.</p> <ol style="list-style-type: none"> 1. Servicios definidos: Servicios proactivos (Alertas de seguridad, Boletines de sensibilización y capacitación, Compartir experiencias). Servicios reactivos: (Servicios de gestión de incidentes, Compartir indicadores de compromiso) 2. Horarios de atención 3. Política de divulgación de información 4. Página Web 							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4

Requerimiento ENISA/GCMF Avanzado	0	1	2	3	4
Requerimiento TI Certificado	0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado					
Nivel Actual CSIRT-SE	0	1	2	3	4
Nivel esperado 2025	0	1	2	3	4
Tenemos una descripción de servicio escrita aprobada por la dirección de nuestro equipo, y se ha puesto a disposición de nuestra circunscripción.					

O-6: DESCRIPCIÓN DEL NIVEL DE SERVICIO

Cuadrante:	Organización	Parámetro:	O-6: Descripción del Nivel de Servicio							
<p>Al definir los servicios que ofrece su CSIRT, es útil establecer también los niveles de servicio para esos servicios. ¿Qué pueden esperar de usted sus usuarios en este sentido? ¿Qué pueden esperar de usted otros CSIRT? El nivel de servicio más sencillo es una medida de la cantidad de tiempo en la que se envía una primera reacción (humana) a un informe de incidente entrante - SIM3 ha establecido un nivel mínimo aquí, es obligatorio enviar una reacción humana a los equipos pares en un plazo de dos días laborables (los equipos pares son aquellos CSIRT con los que se tiene una relación bien definida, como ser miembros de la misma cooperación o foro CSIRT). Los niveles de servicio también pueden ser demandas más detalladas del tipo "ANS", y entonces también pueden depender del tipo y la gravedad de los incidentes (como, por ejemplo, se define en el parámetro O-8, clasificación de incidentes). En función del tipo y la gravedad de los incidentes, pueden definirse diferentes tiempos de reacción, pero también, por ejemplo, el porcentaje de incidentes que debe tratarse en un tiempo determinado. ¿Tiene su CSIRT una descripción del nivel de servicio? Requisito mínimo: Especifica la velocidad de reacción a los informes de incidentes entrantes y a los informes de los constituyentes y de los CSIRT homólogos. Para estos últimos, lo mínimo que se espera es una reacción humana en un plazo de dos días laborables.</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una descripción del nivel de servicio por escrito aprobada por la dirección de nuestro equipo.										
<p>Evidencia: Procedimiento de gestión de incidentes ÁRBOL DE CATEGORÍAS CONFIGURADO CON EL SERVICE DESK Y REFERENCIADO EN EL DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA., Servicios reactivos.</p>										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una descripción del nivel de servicio por escrito aprobada por la dirección de nuestro equipo.										

O-7: CLASIFICACIÓN DE INCIDENTES

Cuadrante:	Organización	Parámetro:	O-7: Clasificación de Incidentes				
Un esquema de clasificación de incidentes suele contener al menos una lista de categorías de incidentes técnicos a los que asociar un incidente o amenaza, como por ejemplo si tiene las características de "spam" o "compromiso de raíz" o "DDoS", etc. Sin embargo, se recomienda incluir también en dicha clasificación alguna medida de la gravedad o el impacto potencial de un incidente o amenaza, y potencialmente también su prioridad evaluada (ya que una amenaza de alto impacto, por ejemplo, puede ser de baja prioridad cuando su probabilidad de que ocurra pronto es muy baja). Estas formas más avanzadas de clasificar los incidentes, unidas a los niveles de servicio definidos en O-7, pueden ayudar a tratar de forma estructurada las cargas de incidentes más elevadas. ¿Tiene su equipo algún tipo de clasificación de incidentes?							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
Tenemos una definición de responsabilidad por escrito aprobada por la dirección de nuestro equipo.							
Evidencia:							
DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA.							
Definiciones sobre taxonomías aplicables, Política de clasificación de información, política de gestión de incidentes y Procedimiento de gestión de incidentes							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado			0	1	2	3	4
Requerimiento TI Certificado			0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado							
Nivel Actual CSIRT-SE			0	1	2	3	4
Nivel esperado 2025			0	1	2	3	4
Tenemos una definición de responsabilidad por escrito aprobada por la dirección de nuestro equipo.							

O-8: INTEGRACIÓN EN LOS SISTEMAS CSIRT EXISTENTES

Cuadrante:	Organización	Parámetro:	O-8: Integración en los Sistemas CSIRT Existentes							
<p>Con 'sistemas CSIRT' nos referimos a cooperaciones bien establecidas de CSIRT, como en su país, sector, región geográfica o en todo el mundo. Su CSIRT puede participar en ellas directamente, por ejemplo, como miembro, o puede hacerlo indirectamente cuando puede hacer uso de los servicios de un CSIRT "anterior" que participe en dichas cooperaciones de CSIRT. Para ser eficaz como CSIRT, es necesario comprometerse con este tipo de participación, ya que la comunidad CSIRT en general depende de este tipo de cooperación entre equipos. ¿Participa su equipo en este tipo de cooperaciones directamente, o indirectamente a través de un CSIRT anterior?</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
<p>Tenemos una declaración formal por escrito sobre la(s) cooperación(es) del CSIRT en la que participamos, aprobada por la dirección de nuestro equipo y respaldada por el presupuesto.</p>										
<p>Evidencia: DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA. Relaciones con partes interesadas internas y externas Acuerdos de colaboración conjunta</p>										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
<p>Tenemos una declaración formal por escrito sobre la(s) cooperación(es) del CSIRT en la que participamos, aprobada por la dirección de nuestro equipo y respaldada por el presupuesto.</p>										

O-09: MARCO ORGANIZATIVO

Cuadrante:	Organización	Parámetro:	O-09: Marco Organizativo							
<p>Lo que llamamos "carta del equipo" o "marco organizativo" para su CSIRT, es un documento de control coherente para su equipo, que describe quién/qué es su equipo, para quién trabaja, qué hace y cómo se le encomendó. Esta carta debe incluir al menos los parámetros O-1 a O-9 del SIM3 y potencialmente algunos más. Lo ideal es que esta carta haya sido aprobada por el mismo nivel de gobernanza que ha ordenado su CSIRT. El estatuto de su equipo es normalmente un documento interno - por lo tanto, el RFC2350, que se entiende básicamente como una descripción de servicio público de su equipo no es adecuado como estatuto del equipo (también el RFC2350 es mucho más limitado en su alcance que el estatuto). ¿Tiene su CSIRT una carta de este tipo? Requisito mínimo: Describe la misión del equipo y los parámetros O-1 a O-9, ya sea proporcionando referencias a documentos específicos o combinando los detalles requeridos en un solo documento.</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una carta escrita aprobada por la dirección de nuestro equipo.										
Evidencia:										
DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una carta escrita aprobada por la dirección de nuestro equipo.										

O-10: POLÍTICA DE SEGURIDAD

Cuadrante:	Organización	Parámetro:	O-10: Política de Seguridad							
Su CSIRT suele estar integrado en una organización anfitriona. Esa organización anfitriona tendrá políticas de seguridad informática o de la información, que también se aplicarán a su equipo. Como CSIRT, a menudo tienes requisitos de TI/seguridad que difieren de los normales - como si quisieras ser capaz de ejecutar pruebas sin que un firewall bloquee esas pruebas, o recibir correo electrónico sin filtro de spam/malware, puede que quieras colocar un honeypot en algún lugar, o puede que necesites ser capaz de utilizar software de encriptación como gpg. Estos requisitos especiales del CSIRT a menudo hacen necesario que, además de la política de seguridad de su organización, su CSIRT también tenga su propia política de seguridad. Por supuesto, cuando se trata de un CSIRT independiente sin organizaciones anfitrionas, se aplican los mismos argumentos. ¿Sigue su CSIRT una política de seguridad establecida, o políticas de seguridad, ya sean propias o de su organización anfitriona?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una política de seguridad escrita que se aplica a nosotros, aprobada por la dirección de nuestro equipo.										
Evidencia: Políticas de seguridad de la información del Ministerio de Educación Nacional DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN EVOLUCIÓN Y FUTURO DEL CSIRT SECTOR EDUCACIÓN DE COLOMBIA.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una política de seguridad escrita que se aplica a nosotros, aprobada por la dirección de nuestro equipo.										

Anexo 2. Entrevistas cuadrante Recursos Humanos

H-1: CÓDIGO DE CONDUCTA/PRÁCTICA/ÉTICA

Cuadrante:	RECURSOS HUMANOS	Parámetro:	H-1: Código De Conducta/Práctica/Ética				
<p>¿Su CSIRT proporciona orientación, directrices o conjuntos de reglas para los miembros de su equipo sobre cómo comportarse profesionalmente, de manera ética? A menudo llamado "Código de Conducta (CoC)" o "Código de Práctica (CoP)", puede proporcionar reglas de oro sobre la confidencialidad, la fiabilidad y otras cualidades humanas clave que se esperan de los miembros del equipo del CSIRT. La organización anfitriona del CSIRT suele tener un código de ética, pero estos códigos son de naturaleza genérica y no tienen nada que ver con el trabajo específico que realiza el CSIRT. El CSIRT a menudo trata con datos altamente sensibles, y se comunica no sólo dentro de la organización anfitriona, sino también fuera de ella. Además, el comportamiento responsable de los miembros del equipo del CSIRT no se limita al contexto laboral, sino que también es relevante en los círculos privados cuando se trata de la seguridad. La CCoP del Introdutor de Confianza puede utilizarse como línea de base de la CoP, ya que fue escrita específicamente para los CSIRT. Es necesaria la alineación con la política de seguridad (O-11). ¿Apoya su equipo este código de conducta/práctica/ética?</p>							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
Tenemos un código de conducta escrito aprobado por la dirección de nuestro equipo.							
Evidencia:							
DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN							
Definición de estructura para el CSIRT Educación.							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado			0	1	2	3	4
Requerimiento TI Certificado			0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado							
Nivel Actual CSIRT-SE			0	1	2	3	4
Nivel esperado 2025			0	1	2	3	4
Tenemos una declaración formal sobre el número de personal CSIRT disponible aprobada por la dirección de nuestro equipo.							

H-2: RESISTENCIA DEL PERSONAL

Cuadrante:	RECURSOS HUMANOS	Parámetro:	H-2: Resistencia del Personal							
<p>¿Tiene su CSIRT suficiente personal para hacer frente a la indisponibilidad planificada o inesperada de los miembros del equipo? Estos casos incluyen enfermedad, vacaciones, abandono del trabajo... Dependiendo de los servicios ofrecidos (O-5) y de los niveles de servicio (O-7), el número de miembros del equipo variará, pero hay que prever la disponibilidad en tiempos de crisis. Sobre la base de la lista de los servicios mínimos que hay que prestar en todos los contextos, se suele acordar que tres miembros del equipo (a tiempo parcial) es un mínimo absoluto para cualquier equipo. ¿Qué pasa con la resistencia del personal de su equipo? Requisito mínimo: Tres miembros (a tiempo parcial o completo) del CSIRT.</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una declaración formal sobre el número de personal CSIRT disponible aprobada por la dirección de nuestro equipo.										
Evidencia: CCoP v2.4. Disponible en https://www.trusted-introducer.org/TI-CCoP.pdf .										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos un código de conducta escrito aprobado por la dirección de nuestro equipo.										

H-3: DESCRIPCIÓN DEL CONJUNTO DE HABILIDADES

Cuadrante:	RECURSOS HUMANOS	Parámetro:	H-3: Descripción del conjunto de habilidades							
¿Tiene su CSIRT una descripción de las habilidades necesarias en todos los puestos del equipo CSIRT? Todos los puestos deben estar definidos e incluir una descripción de las habilidades esperadas de los miembros del equipo: esto incluye habilidades técnicas, de conocimiento, de experiencia y blandas - por ejemplo, comunicación, espíritu de equipo, trabajo bajo estrés... Los planes de formación (véanse H-4, H-5 y H-6) pueden ayudar a colmar las lagunas en las competencias de los miembros del equipo. ¿Ha descrito su equipo las competencias necesarias?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Disponemos de una descripción de competencias por escrito aprobada por la dirección de nuestro equipo.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, con definición de Estructura definida para el CSIRT Educación y Estructura organizacional.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Disponemos de una descripción de competencias por escrito aprobada por la dirección de nuestro equipo.										

H-4: FORMACIÓN INTERNA

Cuadrante:	RECURSOS HUMANOS	Parámetro:	H-4: Formación Interna							
¿Proporciona su CSIRT un catálogo de formación interna a los miembros del equipo, o al menos ofrece una descripción de un "camino" de formación interna a seguir? Estas formaciones deben permitir a los miembros del equipo, tanto a los nuevos como a los existentes, mejorar sus habilidades y alcanzar los objetivos definidos en el conjunto de habilidades (H-3) que se aplican a su puesto de trabajo. La formación puede ser en el puesto de trabajo, con mentores o de forma más tradicional. ¿Tiene su equipo un programa de formación interna de este tipo?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos ideas sobre la formación interna y/o formamos a los miembros del equipo de manera informal, pero nunca anotamos nada sobre las demandas de formación, los temas o los materiales.										
Evidencia:										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos ideas sobre la formación interna y/o formamos a los miembros del equipo de manera informal, pero nunca anotamos nada sobre las demandas de formación, los temas o los materiales.										

H-5: FORMACIÓN TÉCNICA (EXTERNA)

Cuadrante:	RECURSOS HUMANOS	Parámetro:	H-5: Formación Técnica (Externa)							
¿Su CSIRT proporciona a los miembros del equipo una lista de formaciones (externas e internas) que pueden realizar para mejorar sus habilidades y cumplir con los objetivos de orientación técnica definidos en el conjunto de habilidades (H-3) que se aplica a su puesto de trabajo? Esto incluye nuevos temas o tecnologías, futuras direcciones de seguridad y profundizaciones tecnológicas. Las formaciones relacionadas con los CSIRT son TRANSITS-I/II, impartidas por ENISA o FIRST, o programas de formación comerciales -por ejemplo, CERT/CC, SANS... ¿Tiene su equipo un programa de formación técnica de este tipo?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Enviamos a personas a este tipo de formación cuando es necesario, pero no tenemos una política escrita al respecto.										
Evidencia:										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Enviamos a personas a este tipo de formación cuando es necesario, pero no tenemos una política escrita al respecto.										

H-6: FORMACIÓN EN COMUNICACIÓN (EXTERNA)

Cuadrante:	RECURSOS HUMANOS	Parámetro:	H-6: Formación en Comunicación (Externa)							
<p>¿Proporciona su CSIRT una lista de formaciones (externas e internas) que pueden realizar los miembros del equipo para mejorar sus habilidades y alcanzar los objetivos orientados a la comunicación definidos en el conjunto de habilidades (H-3) que se aplica a su puesto de trabajo? Para los miembros del equipo CSIRT, la comunicación es una de las habilidades más críticas, y todos los miembros del equipo deben ser entrenados para interactuar mejor con los clientes, colegas, gerentes, compañeros, autoridades locales o extranjeras, y a veces también con la prensa. Esto se aplica a todo tipo de medios de comunicación -por ejemplo, teléfono, chat, correo electrónico, redes sociales... - y a todo tipo de comunicaciones, como conversaciones directas, reuniones, presentaciones, redacción de informes o asesorías, publicaciones en blogs, tweets y mensajes de texto. Se aplica a las comunicaciones formales e informales, y no sólo a las actividades laborales, sino a veces también fuera del trabajo (en cumplimiento del código ético H-1). También hay que prestar atención al hecho de que, aunque la comunicación "normal" puede cubrir el 90% o más de todas las situaciones, la comunicación de crisis es diferente, pero al menos igual de importante. Por último, aquellos que puedan hablar con la prensa, necesitan una formación adicional para ello. ¿Tiene su equipo un programa de formación en comunicación de este tipo?</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Enviamos a personas a este tipo de formación cuando es necesario, pero no tenemos una política escrita al respecto.										
Evidencia:										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Enviamos a personas a este tipo de formación cuando es necesario, pero no tenemos una política escrita al respecto.										

H-7: REDES EXTERNAS

Cuadrante:	RECURSOS HUMANOS	Parámetro:	H-7: Redes Externas							
¿Tiene su CSIRT una política para enviar a los miembros del equipo a reuniones relacionadas con el CSIRT o con la ciberseguridad? Esto contribuye a la colaboración nacional, sectorial, regional y/o mundial del CSIRT - y esas colaboraciones son esenciales para el éxito y la eficacia de la comunidad CSIRT en su conjunto. Además, reunirse en persona crea la base para las relaciones de confianza con los compañeros, y la "confianza" es el cemento de las colaboraciones CSIRT. ¿Tiene su equipo una política de este tipo para la creación de redes externas?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
No tenemos una declaración formal por escrito sobre nuestro trabajo en red externo, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, se incluye relaciones Internas y Externas.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una declaración formal por escrito sobre nuestro trabajo en red externo, aprobada por la dirección de nuestro equipo.										

Anexo 3. Entrevistas cuadrante Herramientas

T-1: LISTA DE RECURSOS INFORMÁTICOS

Cuadrante:	HERRAMIENTAS	Parámetro:	T-1: Lista de Recursos Informáticos							
<p>La disponibilidad de una lista actualizada y suficientemente detallada de los recursos informáticos/de red que utiliza la circunscripción es muy importante para una gestión eficaz de los incidentes de seguridad. Dicha lista debe incluir información sobre el hardware/software que utilizan los miembros de la circunscripción. Es necesario disponer de información más detallada que incluya las versiones de software en uso para poder hacer frente a las amenazas con mayor eficacia. Algunas organizaciones utilizan la gestión de activos de TI (ITAM) para este fin y mantienen una base de datos de gestión de la configuración (CMDB). El CSIRT no suele gestionar estos recursos, pero necesita tener acceso a ellos. Mantener información actualizada y detallada sobre todo el panorama de hardware y software de TI es un reto, y a veces incluso imposible, como en el caso de la coordinación de los CSIRT con grupos que "manejan cualquier cosa que se les ocurra". La solución alternativa es centrarse sólo en los activos más críticos, y en este caso podría ser el propio CSIRT el que recopilara y mantuviera esa información, en comunicación directa con sus integrantes. ¿Tiene su CSIRT acceso a una lista de recursos informáticos?</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
<p>No tenemos una lista formal de recursos informáticos, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.</p>										
Evidencia:										
<p>DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, se incluye definición de Recursos.</p>										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
<p>No tenemos una lista formal de recursos informáticos, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.</p>										

T-2: LISTA DE FUENTES DE INFORMACIÓN

Cuadrante:	HERRAMIENTAS	Parámetro:	T-2: Lista de Fuentes de Información							
Una parte muy importante de las operaciones del CSIRT es la monitorización diaria de todas las fuentes de información relevantes. Estas fuentes deberían incluir, por ejemplo, cuentas de medios sociales relevantes, que publican o distribuyen información valiosa, o blogs o servicios de sitios web relacionados con la seguridad informática. Tanto la información limitada en el tiempo como las observaciones a más largo plazo son importantes, no sólo para ajustar continuamente las operaciones del CSIRT, sino también -y lo que es más importante- para reaccionar a tiempo y eficazmente a los acontecimientos actuales. Por supuesto, esta lista debe mantenerse. ¿Tiene su equipo una lista de fuentes de información de este tipo?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos una lista formal de fuentes de información aprobada por la dirección de nuestro equipo.										
Evidencia:										
N/A.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos una lista formal de fuentes de información aprobada por la dirección de nuestro equipo.										

T-3: SISTEMA DE CORREO ELECTRÓNICO CONSOLIDADO

Cuadrante:	HERRAMIENTAS	Parámetro:	T-3: Sistema de Correo Electrónico Consolidado							
Un CSIRT debe organizar su trabajo de manera que garantice la gestión eficaz de los incidentes. Esto incluye el intercambio continuo de información entre los miembros del equipo, en muchos casos también cuando no están de servicio. Además, los informes de incidentes llegarán, y también hay que gestionar la comunicación con otros equipos. El correo electrónico sigue siendo el mecanismo de comunicación dominante en la mayoría de estos casos. Por lo tanto, el equipo debe tener un sistema de correo electrónico resistente y de alta calidad que esté consolidado (normalmente en la oficina del equipo, con buenas instalaciones de respaldo) y al que todos los miembros del equipo deban tener acceso. Por supuesto, es posible utilizar el sistema de correo electrónico de la organización anfitriona, o incluso un servicio en la nube; sin embargo, hay que tener en cuenta la seguridad de estas soluciones: puede ser necesario cifrar los datos confidenciales. ¿Su CSIRT utiliza un sistema de correo electrónico consolidado?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Mantenemos el correo electrónico del CSIRT en un repositorio y esto fue aprobado por la dirección de nuestro equipo.										
Evidencia: Definir un dominio como csirt.mineducacion.edu.co DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de correo seguro.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Mantenemos el correo electrónico del CSIRT en un repositorio y esto fue aprobado por la dirección de nuestro equipo.										

T-4: SISTEMA DE SEGUIMIENTO DE INCIDENTES

Cuadrante:	HERRAMIENTAS	Parámetro:	T-4: Sistema de Seguimiento de Incidentes							
<p>Un sistema de tickets bien diseñado y adaptado es importante para cualquier CSIRT. En la práctica, cuando un equipo tiene que gestionar muchos incidentes, es casi imposible gestionar correctamente toda la información y la comunicación entre el equipo y las partes implicadas, sin un sistema de seguimiento de este tipo. Sólo los equipos realmente pequeños con un número reducido de incidentes son capaces de gestionar el proceso de gestión de incidentes utilizando una solución muy básica como una hoja de cálculo compartida. En la mayoría de los casos, se necesita una solución dedicada. A veces, el equipo vuelve a utilizar el sistema de tickets de incidencias de la organización anfitriona; esto es ciertamente posible, pero, al igual que en el caso del correo electrónico, la confidencialidad puede volver a ser un reto, ya que la mayoría de los sistemas genéricos de tickets de incidencias no parecen haber sido diseñados teniendo en cuenta la seguridad. Muchos CSIRTS llevan mucho tiempo utilizando sus propios sistemas específicos de seguimiento de incidentes, concretamente soluciones de código abierto como RTIR (Request Tracker for Incident Response), OTRS (Open Source Ticketing Request System) o (de fecha más reciente) TheHive. Todas estas soluciones son escalables y fáciles de usar. ¿Su equipo utiliza un sistema de seguimiento de incidentes de este tipo?</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Se debe definir un sistema de seguimiento de incidentes y configurar e integrar una mesa de ayuda para este fin.										
Evidencia:										
Integración con mesa de servicio										
Definición de seguimiento de tickets en DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Disponer de un mes de servicio y configuración para seguimiento a incidentes.										

T-5: TELÉFONO RESISTENTE

Cuadrante:	HERRAMIENTAS	Parámetro:	T-5: Teléfono Resistente							
El "teléfono" sigue siendo una herramienta de comunicación crucial para los CSIRT. Es parte de la forma en que los miembros del equipo CSIRT hacen su trabajo, y gestionan los incidentes y realizan sus otras tareas. Por lo tanto, el tiempo de actividad de las herramientas telefónicas disponibles tiene que apoyar los niveles de servicio del equipo (parámetro O-7). Por lo tanto, si un equipo tiene que ser capaz de reaccionar rápidamente a los incidentes y resolverlos con rapidez, entonces el tiempo de actividad de las herramientas telefónicas tiene que ser muy alto, para que cualquier fallo en esas herramientas no obstaculice el rendimiento del equipo. En el caso de la telefonía, deben tenerse en cuenta todas las herramientas de que dispone el equipo, como la clásica "línea fija", la telefonía IP o los teléfonos móviles; especialmente los teléfonos móviles suelen ofrecer buenos medios de resiliencia, sobre todo cuando se utilizan los servicios de más de un proveedor de telefonía móvil. Un caso especial, aunque poco frecuente, es cuando un equipo tiene acceso a un sistema de comunicación protegido (normalmente) a nivel nacional. ¿Cuáles son las instalaciones telefónicas de su equipo y son lo suficientemente resistentes para sus propósitos Requisito mínimo: ¿Mecanismo de reserva para el caso de interrupciones del sistema telefónico?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Cuando el sistema telefónico se cae, adoptamos un plan de emergencia (por ejemplo, utilizando teléfonos móviles), lo documentamos y fue aprobado por la dirección de nuestro equipo.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de telefonía fija y móvil										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Cuando el sistema telefónico se cae, adoptamos un plan de emergencia (por ejemplo, utilizando teléfonos móviles), lo documentamos y se busca la aprobación por la dirección de nuestro equipo.										

T-6: ACCESO A INTERNET RESISTENTE

Cuadrante:	HERRAMIENTAS	Parámetro:	T-6: Acceso a Internet Resistente							
<p>Es crucial que los CSIRT tengan un acceso a Internet suficientemente rápido y fiable. Sin ello, el CSIRT no puede funcionar normalmente. Por lo tanto, el tiempo de funcionamiento del acceso a Internet tiene que soportar al menos y preferiblemente superar los niveles de servicio del equipo (parámetro O-7). Por lo tanto, si un equipo tiene que ser capaz de reaccionar rápidamente a los incidentes y resolverlos rápidamente, entonces el tiempo de actividad del acceso a Internet tiene que ser muy alto, para que cualquier fallo no obstaculice el rendimiento del equipo. Lo ideal es que el CSIRT o su organización anfitriona disponga de un acceso a Internet totalmente redundante (incluso físicamente), pero soluciones mucho menos costosas como disponer de una opción de acceso a Internet de reserva (que utilice una tecnología diferente a la normal) también pueden ser suficientes para satisfacer las demandas de nivel de servicio de su equipo. Como la mayoría de los equipos dependen de su organización anfitriona para el acceso a Internet, es útil que el equipo esté calificado internamente como una de las unidades de la organización más exigentes en cuanto al acceso a Internet. ¿Cuáles son las instalaciones de acceso a Internet de su equipo y son lo suficientemente resistentes para sus propósitos?</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
<p>El nivel de servicio de nuestro acceso a Internet es lo suficientemente bueno para nuestros propósitos, y disponemos de documentación al respecto aprobada por la dirección de nuestro equipo.</p>										
Evidencia:										
<p>El acuerdo de nivel de servicio (ANS) con el proveedor de internet garantiza una disponibilidad del 99.5%</p> <p>DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de conexión a Internet.</p>										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
<p>El nivel de servicio de nuestro acceso a Internet es lo suficientemente bueno para nuestros propósitos, y disponemos de documentación al respecto aprobada por la dirección de nuestro equipo.</p>										

T-7: CONJUNTO DE HERRAMIENTAS DE PREVENCIÓN DE INCIDENTES

Cuadrante:	HERRAMIENTAS	Parámetro:	T-7: Conjunto de Herramientas de Prevención de Incidentes.				
<p>Se trata de tener un conjunto de herramientas bien definido y aplicado que ayude a la prevención de incidentes. Estas herramientas forman parte de la primera línea de defensa de la circunscripción. Un CSIRT debe definir claramente su papel con respecto a cada una de esas herramientas. Algunas de estas herramientas pueden ser ejecutadas por el propio equipo, en otros casos pueden ser el arquitecto y un usuario - o pueden ser sólo un usuario de la herramienta, o tener acceso a los resultados. Debido al creciente número de herramientas posibles, su "orquestración" desempeña un papel cada vez más importante. Es de interés primordial para cualquier CSIRT estar estrechamente involucrado en esta área, o incluso decidir sobre dichas herramientas. Ejemplos de herramientas de prevención: sistemas de prevención de intrusiones, software antivirus, filtros de spam o escáneres de vulnerabilidad. ¿Tiene su equipo un conjunto de herramientas de prevención de incidentes bien definido?</p>							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
Nunca hemos hablado de esto.							
Evidencia:							
N/A. El CSIRT educación trabaja exclusivamente en la respuesta a incidentes.							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado			0	1	2	3	4
Requerimiento TI Certificado			0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado							
Nivel Actual CSIRT-SE			0	1	2	3	4
Nivel esperado 2025			0	1	2	3	4
Disponemos de estas herramientas, pero no las hemos enumerado ni documentado.							

T-8: CONJUNTO DE HERRAMIENTAS DE DETECCIÓN DE INCIDENTES

Cuadrante:	HERRAMIENTAS	Parámetro:	T-8: Conjunto de Herramientas de Detección de Incidentes.							
<p>Se trata de tener un conjunto bien definido e implementado de herramientas que ayuden a la detección de incidentes. Estas herramientas son como los oídos y los ojos del CSIRT: aportan información sobre amenazas e incidentes, desde los potenciales hasta los explotados. Un CSIRT debe definir claramente su papel en relación con cada una de esas herramientas. Algunas de estas herramientas las puede ejecutar el propio equipo, en otros casos puede ser el arquitecto y un usuario - o puede ser sólo un usuario de la herramienta, o tener acceso a los resultados. Debido al creciente número de herramientas posibles, su "orquestración" desempeña un papel cada vez más importante. Es de interés primordial para cualquier CSIRT estar estrechamente involucrado en esta área, o incluso decidir sobre dichas herramientas. Ejemplos de herramientas de detección: MISP, AbuseHelper, IntelMQ, analizadores de paquetes de red - pero también hay que tener en cuenta que el teléfono y el correo electrónico se utilizan para recibir informes de incidentes y, por tanto, también son herramientas de detección. ¿Tiene su equipo un conjunto de herramientas de detección de incidentes bien definido?</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Disponemos de dichas herramientas, las hemos documentado y la dirección de nuestro equipo lo ha aprobado.										
<p>Evidencia: Encuesta sobre infraestructura básica de TI de las Entidades Adscritas y Vinculadas realizada. DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de herramientas para desarrollo del CSIRT Educación.</p>										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Se dispone de herramientas, y se documentarán y aprobarán por el director de nuestro equipo.										

T-9: CONJUNTO DE HERRAMIENTAS PARA LA RESOLUCIÓN DE INCIDENTES

Cuadrante:	HERRAMIENTAS	Parámetro:	T-9: Conjunto de Herramientas para la Resolución de Incidentes.				
<p>Se trata de tener un conjunto bien definido e implementado de herramientas que ayuden a la resolución de incidentes. Estas herramientas apoyan lo que es realmente la actividad principal de cualquier CSIRT: la resolución de incidentes. Un CSIRT debe definir claramente su papel con respecto a cada una de esas herramientas. Debido a que estas herramientas son tan críticas para la misión, el equipo probablemente ejecutará varias de ellas por sí mismo, o será un arquitecto principal y un usuario importante - pero en algunos casos puede ser sólo un usuario de la herramienta, en cuyo caso debe asegurarse de poder dar su opinión y ser escuchado al hacerlo. Debido al creciente número de herramientas posibles, su "orquestación" desempeña un papel cada vez más importante. Es de interés primordial para cualquier CSIRT participar de forma decisiva en este ámbito. Si un CSIRT se ocupa de algunos tipos específicos de incidentes, es especialmente importante crear un conjunto de herramientas adaptadas a esas necesidades específicas de resolución. Hay que tener en cuenta que este conjunto de herramientas incluye software, pero también puede incluir hardware dedicado, y en algunos casos esto llegará hasta la creación de, por ejemplo, un laboratorio de resolución de incidentes, por ejemplo, para el análisis de malware o la informática forense. Ejemplos de herramientas de resolución: de nuevo MISP e IntelMQ, su sistema de seguimiento de incidentes, kits forenses. ¿Tiene su equipo un conjunto de herramientas de resolución de incidentes bien definido?</p>							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
Disponemos de dichas herramientas, las hemos documentado y la dirección de nuestro equipo lo ha aprobado.							
<p>Evidencia: Encuesta sobre infraestructura básica de TI de las Entidades Adscritas y Vinculadas realizada. DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de herramientas para desarrollo del CSIRT Educación.</p>							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado			0	1	2	3	4
Requerimiento TI Certificado			0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado							
Nivel Actual CSIRT-SE			0	1	2	3	4
Nivel esperado 2025			0	1	2	3	4
Disponemos de dichas herramientas, las hemos documentado y la dirección de nuestro equipo lo ha aprobado.							

Anexo 4. Entrevistas cuadrante Procesos

P-1: ESCALADA AL NIVEL DE GOBIERNO

Cuadrante:	PROCESOS	Parámetro:	P-1: Escalada al nivel de Gobierno							
Cada equipo debe ser capaz de escalar los incidentes críticos a los niveles de gestión adecuados, incluido el nivel más alto de gobernanza (por ejemplo, el consejo de administración, el ministro) en caso de crisis potenciales o incidentes que supongan al menos una amenaza significativa para la reputación de la organización. En caso de que el equipo sea responsable de un grupo externo, también debe ser capaz de escalar al nivel de gestión adecuado de todos los grupos; esto último no sólo es necesario cuando el punto de contacto normal del equipo no reacciona (a tiempo), sino que también puede estar justificada dicha escalada en caso de un incidente significativo o una nueva amenaza. Estos escalamientos provocados por incidentes de seguridad u otros eventos deben definirse de acuerdo con la Clasificación de Incidentes del equipo (véase O-8), que permite basar lógicamente el escalamiento en, por ejemplo, el impacto y la prioridad. Es fundamental que los medios para escalar estén disponibles en todo momento, aunque la respuesta o la reacción no sean siempre tan inmediatas, ya que esto lo definen los niveles superiores de gobernanza en la propia organización, o en las organizaciones de los integrantes. ¿Puede su equipo escalar de la forma que se indica aquí?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.										
Evidencia:										
Mecanismos de escalamiento que tiene definida la OTSI DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.										

P-2: ESCALADA A LA FUNCIÓN DE PRENSA

Cuadrante:	PROCESOS	Parámetro:	P-2: Escalada a la Función de Prensa			
Es necesario tratar con la prensa y los medios de comunicación públicos. En el caso de que la mayoría o todos los miembros del CSIRT hayan sido encargados de no hablar con la prensa, las solicitudes de la prensa en relación con los incidentes de seguridad deben seguir siendo tratadas con eficacia, independientemente de dónde lleguen. Por lo tanto, el equipo debe ser capaz de ponerse en contacto con los portavoces adecuados que normalmente se encargan de las consultas de la prensa. Para evitar errores de comunicación y retrasos que puedan afectar a la reputación de la organización, el equipo debe ser capaz de contactar directamente con esos contactos de prensa, y también fuera del horario laboral, para darles el conocimiento necesario de la situación. Es aconsejable que el propio equipo designe a un número limitado de miembros del equipo para que también puedan hablar con la prensa, por ejemplo, junto con un portavoz oficial, ya que estos miembros del equipo designados podrán dar más información sobre los aspectos técnicos de una situación determinada; cuando se haga esta elección, es aconsejable dar a estos miembros del equipo una formación adecuada. ¿Su equipo puede escalar de la forma que se indica aquí?						
					NIVEL	
Nivel Actual CSIRT-SE (Secretaría de Educación)		0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.						
Evidencia:						
Mecanismos de escalamiento que tiene definida la OTSI DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN						
Requerimiento FIRST		0	1	2	3	4
Requerimiento ENISA/GCMF Básico		0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio		0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado		0	1	2	3	4
Requerimiento TI Certificado		0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado						
Nivel Actual CSIRT-SE		0	1	2	3	4
Nivel esperado 2025		0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.						

P-3: ESCALADA A LA FUNCIÓN LEGAL

Cuadrante:	PROCESOS	Parámetro:	P-3: Escalada a la Función Legal.							
Es necesario gestionar las cuestiones legales, incluidas las solicitudes de las fuerzas de seguridad. Estas peticiones a la organización deben ser tratadas de forma muy eficaz para evitar que las pruebas sean destruidas o dejen de estar disponibles, por ejemplo, como resultado de los procesos automatizados que eliminan los datos de forma rutinaria, pero también porque el tratamiento de estas cuestiones de forma incorrecta podría provocar daños a la reputación y pérdidas financieras. Por lo tanto, el equipo debe ser capaz de ponerse en contacto directamente, y también fuera del horario de trabajo, con los expertos jurídicos de su organización (por ejemplo, los abogados) para informarles de los asuntos pertinentes, incluyendo, entre otros, las solicitudes u órdenes judiciales entrantes. Los expertos jurídicos pueden entonces ocuparse ellos mismos de estas cuestiones directamente, o en consulta con el equipo. ¿Puede su equipo escalar de la forma que se indica aquí?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.										
Evidencia:										
Mecanismos de escalamiento que tiene definida la OTSI DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.										

P-4: PROCESO DE PREVENCIÓN DE INCIDENTES

Cuadrante:	PROCESOS	Parámetro:	P-4: Proceso de Prevención de Incidentes.							
Desde una perspectiva de gestión de riesgos, los incidentes deben ser evitados, por lo que el CSIRT debe apoyar los procesos de prevención apropiados internamente - o en caso de una circunscripción externa - para sus integrantes. Ejemplos de procesos de prevención de incidentes son: la creación y difusión de avisos sobre nuevas vulnerabilidades de seguridad; las actividades de escaneo de puertos; la difusión de información sobre amenazas; el intercambio de lecciones aprendidas del análisis de incidentes. Por lo general, se utilizan herramientas para apoyar estos procesos (véase T-8), y luego la forma de hacerlo será parte del proceso. ¿Tiene su equipo un proceso para la prevención de incidentes?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.										
Evidencia: Página Web DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos un proceso formal de escalado por escrito aprobado por la dirección de nuestro equipo.										

P-5: PROCESO DE DETECCIÓN DE INCIDENTES

Cuadrante:	PROCESOS	Parámetro:	P-5: Proceso de Detección de Incidentes.							
Sin la detección de incidentes ningún CSIRT es capaz de responder a ellos. Dependiendo del tipo de CSIRT que consideremos, algunos operan sus propias capacidades de detección (IDS, registros de cortafuegos, <i>honeypots</i>). Otros dependen de los constituyentes para recibir informes de incidentes, o utilizan un SOC para recibir incidentes potenciales que necesitan ser analizados; también es posible un enfoque mixto. La forma de hacerlo se describe en el proceso de detección. El triaje, el proceso de juzgar los informes de incidentes entrantes y asignarlos para su tratamiento posterior, forma parte de la detección de incidentes. Normalmente, se utilizan herramientas para apoyar estos procesos (ver T-8), y entonces cómo hacerlo será parte del proceso. Obsérvese que, con frecuencia, P-5 y P-6 (P-6 sigue a continuación y trata de la resolución de incidentes) se combinan en un solo proceso, a menudo llamado proceso de gestión (o manejo) de incidentes, que es válido siempre que tanto la detección como la resolución se hagan con justicia. ¿Tiene su equipo un proceso para la detección de incidentes? (Si tiene un proceso combinado para P-5 y P-6, elija el mismo nivel para ambos)										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos un proceso formal por escrito aprobado por la dirección de nuestro equipo.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de Política y procedimiento de Gestión de Incidentes,										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos un proceso formal por escrito aprobado por la dirección de nuestro equipo.										

P-6: PROCESO DE RESOLUCIÓN DE INCIDENTES

Cuadrante:	PROCESOS	Parámetro:	P-6: Proceso de Resolución de Incidentes.							
Cualquier CSIRT que gestione incidentes necesita desarrollar al menos un proceso genérico sobre cómo resolver, manejar y mitigar los incidentes. Al ser genérico, cada entrada es procesada por el mismo proceso más o menos de la misma manera, aunque seguramente los resultados variarán. En lugar de centrarse en los aspectos específicos de un incidente (por ejemplo, un malware APT es muy diferente de un ataque DDoS), este proceso se centra en el enfoque general paso a paso tras el proceso de detección (véase P-5). Los principales pasos del proceso son: análisis, acciones de respuesta que conducen a la mitigación, cierre y lecciones aprendidas. Seguir este proceso genérico garantiza que todos los incidentes se gestionen de acuerdo con la práctica establecida, incluido el uso del conjunto de herramientas relacionadas (véase T-10), lo que podría incluir, por ejemplo, el registro de toda la comunicación con los interesados, o el análisis de registros específicos, etc. ¿Tiene su equipo un proceso para la resolución de incidentes? (Si tiene un proceso combinado para P-5 y P-6, elija el mismo nivel para ambos)										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos un proceso formal por escrito aprobado por la dirección de nuestro equipo.										
Evidencia:										
DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de Política y procedimiento de Gestión de Incidentes,										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Tenemos un proceso formal por escrito aprobado por la dirección de nuestro equipo.										

P-7: PROCESOS ESPECÍFICOS DE INCIDENTES

Cuadrante:	PROCESOS	Parámetro:	P-7: Procesos Específicos de Incidentes.				
<p>Es muy importante tener un proceso común para manejar todos los incidentes que son gestionados por un CSIRT - esto es P-6. Pero este proceso genérico asegura el flujo de trabajo general y no puede adaptarse a tipos específicos de incidentes, por lo que es más que probable que se pierdan algunos aspectos técnicos relevantes. Como ya se ha dicho para P-6, un incidente causado por un nuevo malware APT es muy diferente de un ataque DDoS que bloquea Internet para un cliente importante. No sólo las prioridades son diferentes, sino también la respuesta técnica. Por lo tanto, es recomendable que los CSIRTs maduros identifiquen los tipos de incidentes que causan la mayor parte del trabajo - y luego escribir procesos de incidentes específicos para ellos. Esto permitirá omitir algunos pasos o actividades, mientras se describen otros con más detalle o se añaden otros nuevos (podrían ser subpasos del proceso genérico). Además, los procesos específicos de incidentes pueden escribirse no sólo para tipos de incidentes muy comunes, sino también para incidentes de misión crítica (alto impacto, alta prioridad), o para incidentes que requieran una respuesta que no esté comúnmente presente dentro del propio CSIRT, como la experiencia legal. Tenga en cuenta que P-7 puede ser ya parte de P-6, si el proceso de resolución de incidentes admite subprocesos para tratar algunos tipos de incidentes específicos o admite varios caminos para algunos tipos de incidentes específicos - esto es, por supuesto, perfectamente válido. ¿Ha descrito su equipo procesos específicos de incidentes, más allá del proceso genérico de resolución de incidentes?</p>							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
Tenemos algunas formas estándar de tratar los diferentes tipos de incidentes, pero no lo hemos documentado.							
Evidencia:							
DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de Política y procedimiento de Gestión de Incidentes,							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado			0	1	2	3	4
Requerimiento TI Certificado			0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado							
Nivel Actual CSIRT-SE			0	1	2	3	4
Nivel esperado 2025			0	1	2	3	4
Tenemos algunas formas estándar de tratar los diferentes tipos de incidentes, pero no lo hemos documentado.							

P-8: PROCESO DE AUDITORÍA/RETROALIMENTACIÓN

Cuadrante:	PROCESOS	Parámetro:	P-8: Proceso de auditoría/retroalimentación.				
<p>Todos los CSIRT necesitan una garantía de calidad de todos los aspectos críticos y sensibles de su funcionamiento. Si bien existen varios medios para ayudar a garantizar los niveles de calidad (empezando por la autoevaluación, los recorridos, las revisiones por pares, las auditorías tanto internas como externas), el nivel de escrutinio debe ser definido, delimitado y mantenido. A esto lo llamamos proceso de auditoría/retroalimentación. Este proceso debe garantizar el cumplimiento de los niveles de calidad adecuados y reconocer los problemas lo antes posible. El flujo de información resultante debe beneficiar no sólo al propio equipo, sino también a los niveles de gestión pertinentes por encima del CSIRT. Esto es especialmente importante en el caso de los temas cubiertos por los parámetros de la SIM3 en los que el equipo aspira a alcanzar el nivel 4 - para ellos, se requiere una forma de comprobación regular y activa por parte de la dirección superior (por encima del director del CSIRT) - y debe documentarse que se auditan de esa forma y que se da retroalimentación al equipo. Esta participación de la dirección superior es un mecanismo crucial, ya que algunos aspectos de la calidad no pueden ser garantizados por el propio CSIRT, ni siquiera si son controlados por el director del CSIRT o el jefe del equipo. Es obligatorio un feedback imparcial y neutral para no centrarse en los errores o equivocaciones, sino en la mejora y el progreso, teniendo en cuenta la misión de la organización/constitución. ¿Se ha definido un proceso de auditoría/retroalimentación de este tipo para su CSIRT?</p>							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
No tenemos un proceso formal por escrito, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.							
Evidencia:							
DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición del nivel de madurez.							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado			0	1	2	3	4
Requerimiento TI Certificado			0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado							
Nivel Actual CSIRT-SE			0	1	2	3	4
Nivel esperado 2025			0	1	2	3	4
Tenemos un proceso formal por escrito aprobado por la dirección de nuestro equipo.							

P-9: PROCESO DE ACCESIBILIDAD EN CASO DE EMERGENCIA

Cuadrante:	PROCESOS	Parámetro:	P-9: Proceso de accesibilidad en caso de emergencia.				
Cada CSIRT soporta una serie de mecanismos de comunicación que pueden ser utilizados para enviar información o informes de incidentes. Dependiendo de la necesidad de los constituyentes, o del mandato del CSIRT, estos medios se dan a conocer públicamente, o sólo están disponibles para los constituyentes o los CSIRT pares (ver P-17). En la mayoría de los casos, las ventanas de servicio de los CSIRT coinciden con el horario de trabajo estándar. Algunos CSIRT están de guardia fuera de esos horarios, de acuerdo con sus propios niveles de servicio. Sin embargo, las situaciones de crisis/emergencia pueden ocurrir y ocurrirán, y pueden requerir la accesibilidad del CSIRT incluso fuera de las ventanas de servicio normales. Para permitir que los constituyentes o los equipos pares se pongan en contacto con el CSIRT en estos casos especiales, es necesario que exista un proceso de accesibilidad de emergencia que describa los números de teléfono, las direcciones de correo electrónico y posiblemente también las palabras clave especiales reservadas para estas verdaderas emergencias. El proceso debería sancionar el mal uso, ya que reaccionar fuera de las ventanas de servicio normales suele ser caro. Por otro lado, dada su importancia potencial, el proceso debe ejecutarse de vez en cuando para formar a todas las partes implicadas. ¿Cuenta su CSIRT con un proceso de accesibilidad de emergencia de este tipo?							
			NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)			0	1	2	3	4
No tenemos un proceso formal por escrito, por lo que escribimos algo para nuestros propios fines y lo ponemos a disposición de nuestros principales interesados. Nuestra dirección no lo ha aprobado formalmente.							
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de horarios iniciales de atención.							
Requerimiento FIRST			0	1	2	3	4
Requerimiento ENISA/GCMF Básico			0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio			0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado			0	1	2	3	4
Requerimiento TI Certificado			0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado							
Nivel Actual CSIRT-SE			0	1	2	3	4
Nivel esperado 2025			0	1	2	3	4
Tenemos un proceso formal por escrito disponible para nuestros principales interesados y aprobado por la dirección de nuestro equipo. (Tenga en cuenta que la información publicada, ya sea dentro de la circunscripción o en alguna base de datos externa (por ejemplo, TI) también cuenta como nivel 3).							

P-10: PRESENCIA EN INTERNET DE LAS MEJORES PRÁCTICAS

Cuadrante:	PROCESOS	Parámetro:	P-10: Presencia en Internet de las mejores prácticas.							
<p>La comunicación está en el corazón de cualquier CSIRT y ser capaz de llegar a través de Internet y estar localizable es esencial. Además de disponer de varias herramientas de comunicación (ver T-5, T-6 y T-7), todos los CSIRTs necesitan un proceso para monitorizar las peticiones e información entrantes, con el fin de alcanzar sus niveles de servicio definidos (o informales) y cumplir con su responsabilidad. El RFC2142 define las mejores prácticas con respecto a las direcciones de correo electrónico específicas de los dominios (véase el RFC). Los usuarios de Internet confían con frecuencia en estas direcciones estándar y, en general, no es razonable esperar que sólo conozcan los datos de contacto de los CSIRT (o incluso que sepan cómo encontrarlos), por lo que es necesario que cualquier propietario de un dominio, incluidos los CSIRT o su organización anfitriona, los respalde. E incluso si el dominio es propiedad de la organización anfitriona, el CSIRT tiene que asegurarse de que las direcciones de correo electrónico son supervisadas, y que los que las supervisan (que a menudo no están en el equipo) saben sobre el CSIRT y cómo pasarles la información. Por supuesto, toda la información de contacto publicada debe ser coherente a nivel interno y apoyar los niveles de servicio del equipo. Se recomienda encarecidamente poner a disposición la información del RFC2350 (ver también O-5), y además una página de seguridad (ejemplo: www.org.tld/security) - esta última puede ofrecer una gama más amplia de información relacionada con la seguridad en lo que respecta a su organización (anfitriona), pero la información de su CSIRT también debería estar presente allí. ¿Ha definido su CSIRT su presencia en Internet de acuerdo con las mejores prácticas mencionadas anteriormente? Requisito mínimo: El manejo de los alias de buzón definidos en el RFC2142, y también cert@... están asegurados de forma que los gestores formen parte del CSIRT o conozcan el CSIRT, para qué sirve y cómo llegar a él cuando lo necesiten. También se requiere algún tipo de presencia en la web para el CSIRT, al menos internamente.</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Nos hemos ocupado de varios de ellos, pero no lo hemos documentado.										
Evidencia: N/A										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
<p>Se debe documentar y configurar los siguientes puntos de contacto:</p> <ul style="list-style-type: none"> ➤ info@csirteducacion.edu.co: Punto de contacto ➤ support@csirteducacion.edu.co: soporte técnico. ➤ abuse@csirteducacion.edu.co: denuncias de comportamientos inapropiados ➤ security@csirteducacion.edu.co: Reporte de incidentes ➤ Página web 										

P-11: PROCESO DE MANEJO SEGURO DE LA INFORMACIÓN

Cuadrante:	PROCESOS	Parámetro:	P-11: Proceso de Manejo Seguro de la Información.							
Cada CSIRT recibe y procesa información que fue etiquetada como confidencial por los que la enviaron - por ejemplo, para evitar que la información caiga en manos de atacantes, o que esté disponible en Internet públicamente antes de que se hayan distribuido las advertencias apropiadas. Por lo tanto, los CSIRT, pero también, por ejemplo, los investigadores de vulnerabilidades dudan en compartir información a menos que pueda hacerse de forma segura. Ahora, además de la seguridad de la comunicación que ofrece TLS o aplicaciones de seguridad como gpg/pgp, la información también debe ser protegida por los CSIRT receptores (almacenamiento seguro, copias de seguridad, etc.). Para comunicar las restricciones en la distribución posterior de la información enviada, se ha desarrollado el protocolo TLP (Traffic Light Protocol) - y se recomienda encarecidamente a cualquier CSIRT que utilice y se adhiera a TLP. También existen otros protocolos que podrían aplicarse en el contexto de un CSIRT, pero normalmente tendrán que ser explicados. ¿Tiene su equipo un proceso sobre cómo manejar la información de forma segura, incluyendo el uso de TLP?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Tenemos un proceso formal por escrito aprobado por la dirección de nuestro equipo.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de Política de clasificación de la información y Política de divulgación de información Establecer Clave pública de PGP y Adopción de TLP.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Se debe adoptar el uso de PGP como mecanismo criptográfico para garantizar confidencialidad, autenticidad y no repudio. También se adoptan el estándar TLP para el manejo de información sensible.										

P-12: PROCESO DE LAS FUENTES DE INFORMACIÓN

Cuadrante:	PROCESOS	Parámetro:	P-12: Proceso de las Fuentes de Información.							
Para cada CSIRT es obligatorio supervisar y evaluar las fuentes de información adecuadas. Además de las páginas web públicas, podría tratarse de medios sociales, listas de correo, proveedores de seguridad, bases de datos de vulnerabilidades o sitios de exploits, portales como pastebin o nuevas alertas enviadas por proveedores de seguridad de la información. Independientemente de cuántas y qué tipo de fuentes de información se supervisen, el CSIRT debe desarrollar un proceso para hacerlo de forma coherente con el escrutinio y la garantía de calidad adecuados. Hay que evitar que el CSIRT actúe a partir de información errónea o manipulada, ya que esto pondrá en riesgo la reputación del equipo. El proceso también debe describir el ciclo de vida de las fuentes, desde que se añaden a la lista de fuentes de información del CSIRT -que es la T-2- hasta que se eliminan por razones de disminución de la calidad (o se anulan). ¿Tiene su equipo un proceso de este tipo, vinculado a la lista de fuentes (T-2)?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
No tenemos un proceso formal por escrito, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de Plataforma MISP y Política de gestión de incidentes, Herramientas de información de amenazas y Página Web.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
No tenemos un proceso formal por escrito, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.										

P-13: PROCESO DE DIVULGACIÓN

Cuadrante:	PROCESOS	Parámetro:	P-13: Proceso de Divulgación.							
Dado que el CSIRT ofrece un servicio a sus constituyentes, necesita llegar a todos los constituyentes y partes interesadas. Al hacerlo, no sólo se promueve a sí mismo, sino también las mejores prácticas y procesos que recomienda. Aunque la concienciación podría considerarse como una actividad de divulgación, es habitual etiquetar la concienciación como un servicio del CSIRT, ya que forma parte de la prevención de incidentes y, por tanto, de su actividad principal. Sin embargo, también es esencial asegurarse de que la población conoce activamente el CSIRT y los servicios que ofrece. Dar a conocer el equipo de esta manera forma parte del proceso de divulgación. Este proceso debe incluir todas las formas de actividades que aumenten la visibilidad y la reputación del CSIRT, variando desde páginas web, pasando por boletines, seminarios web, libros blancos, conferencias, etcétera. Para cualquier CSIRT nacional, esto incluiría llegar a los sectores de infraestructuras críticas y a los ISAC. ¿Tiene su equipo un proceso de divulgación?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Sabemos cómo lo hacemos, pero no lo hemos documentado.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de Política de divulgación de la información y Pagina Web.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Sabemos cómo lo hacemos, pero no lo hemos documentado.										

P-14: PROCESO DE NOTIFICACIÓN

Cuadrante:	PROCESOS	Parámetro:	P-14: Proceso de Notificación.						
Al gestionar los incidentes para su circunscripción, el CSIRT adquiere conocimientos críticos que de otro modo no estarían disponibles para las partes interesadas, los responsables políticos e incluso los responsables de la seguridad de la información o la protección de datos. Como parte del conocimiento de la situación (el alcance será diferente según la finalidad y el objetivo del CSIRT en particular) es importante comunicar y escalar las lecciones aprendidas. El proceso de información debe proporcionar informes actualizados y explicaciones de fondo para prevenir y remediar mejor incidentes/ataques/riesgos similares en el futuro. Las estadísticas sobre los tipos (véase O-8) y el número de incidentes, los recursos gastados, los niveles de financiación, etc., forman parte del proceso de información. El suministro de estadísticas a la circunscripción o al público, está cubierto por el P-15. ¿Su CSIRT informa a la dirección (superior) según un proceso establecido?									
					NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)					0	1	2	3	4
Sabemos cómo lo hacemos, pero no lo hemos documentado.									
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN.									
Requerimiento FIRST					0	1	2	3	4
Requerimiento ENISA/GCMF Básico					0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio					0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado					0	1	2	3	4
Requerimiento TI Certificado					0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado									
Nivel Actual CSIRT-SE					0	1	2	3	4
Nivel esperado 2025					0	1	2	3	4
No tenemos un proceso formal por escrito, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.									

P-15: PROCESO ESTADÍSTICO

Cuadrante:	PROCESOS	Parámetro:	P-15: Proceso Estadístico							
Mientras que P-14 incluye diversas estadísticas en beneficio de la dirección (superior), P-15 se refiere únicamente a las estadísticas destinadas a ser publicadas a la circunscripción, o incluso al mundo en general (como hacen, por ejemplo, varios equipos nacionales, en los informes anuales de tendencias). Al igual que en el caso de P-14, es útil basar esta forma de presentación de estadísticas en la tipología utilizada para los incidentes (véase O-8). Obsérvese que puede haber otros sistemas de notificación, por ejemplo, la notificación obligatoria según la legislación nacional basada en términos o definiciones diferentes. Para la notificación privada/pública de los números estadísticos se recomienda una exportación (semi) automática que transfiera la tipología y los números internos al formato o formatos externos requeridos. ¿Ofrece su equipo este tipo de estadísticas a las circunscripciones o al público, y existe un proceso para hacerlo?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Sabemos cómo lo hacemos, pero no lo hemos documentado.										
Evidencia: DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Sabemos cómo lo hacemos, pero no lo hemos documentado.										

P-16: PROCESO DE REUNIONES

Cuadrante:	PROCESOS	Parámetro:	P-16: Proceso de reuniones							
La comunicación interna y la eficacia del CSIRT pueden mejorarse en gran medida con reuniones regulares, normalmente semanales o incluso diarias. Existen diversas necesidades, así como diferentes configuraciones organizativas (incluyendo el hecho de tener personas en más de un lugar), por lo que no se impone un calendario fijo. Pero todos los equipos deben considerar el número adecuado de reuniones y el alcance de las mismas. Como mínimo, el proceso de reunión debe garantizar que las acciones necesarias, así como las lecciones aprendidas, se recojan y se distribuyan a todas las partes interesadas. Como siempre se pueden encontrar motivos para cancelar esas reuniones, el proceso debe garantizar que las reuniones obligatorias se celebren realmente y que asistan a ellas la combinación necesaria de funciones y personas. ¿Tiene su equipo un proceso de reuniones bien definido?										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
Nos reunimos regularmente, pero no lo hemos documentado.										
Evidencia: Actas de las reuniones del CSIRT DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
Nos reunimos regularmente, pero no lo hemos documentado.										

P-17: PROCESO ENTRE PARES

Cuadrante:	PROCESOS	Parámetro:	P-17: Proceso Entre Pares							
<p>Es importante ser miembro o formar parte de las comunidades pertinentes para fomentar las relaciones de confianza con otros equipos, con el fin de obtener mejor información de forma más oportuna, y para mejorar la comunicación, tanto en términos de velocidad como de calidad. Asimismo, varios equipos formarán parte de un contexto más estructurado jerárquicamente; por ejemplo, un CSIRT de una organización comercial puede tener que informar a un CSIRT coordinador a nivel corporativo, o los equipos gubernamentales de nivel inferior pueden tener que informar a un CSIRT nacional. En todos los casos, es necesario definir estas relaciones "entre iguales" y definir los procesos adecuados en ambas partes. Si existe una estructura jerárquica, las consecuencias de la misma deben estar claramente documentadas. Cuando los pares son más bien equipos "compañeros" en un contexto no jerárquico (por ejemplo, los miembros de FIRST, o de las cooperaciones regionales de CSIRT), sigue siendo necesario definir cómo esos "pares" trabajan juntos y qué expectativas y procesos existen. ¿Ha definido su equipo cuáles son sus diferentes "pares", y cuál es el proceso(s) hacia esos pares?</p>										
						NIVEL				
Nivel Actual CSIRT-SE (Secretaría de Educación)						0	1	2	3	4
No tenemos un proceso formal por escrito, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.										
Evidencia:										
DOCUMENTO LINEAMIENTOS PARA POLÍTICA DE SEGURIDAD DE DATOS DEL MEN Y DOCUMENTO DISEÑAR UNA ESTRATEGIA PARA IMPLEMENTAR EL GRUPO DE RESPUESTAS A INCIDENTES SEGURIDAD (CSIRT) EN EL MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA Y EL SECTOR DE EDUCACIÓN, definición de relaciones internas y externas.										
Requerimiento FIRST						0	1	2	3	4
Requerimiento ENISA/GCMF Básico						0	1	2	3	4
Requerimiento ENISA/GCMF Intermedio						0	1	2	3	4
Requerimiento ENISA/GCMF Avanzado						0	1	2	3	4
Requerimiento TI Certificado						0	1	2	3	4
Observaciones y Acciones para llegar al nivel esperado										
Nivel Actual CSIRT-SE						0	1	2	3	4
Nivel esperado 2025						0	1	2	3	4
No tenemos un proceso formal por escrito, por lo que escribimos algo para nuestros propios fines. Nuestra dirección no lo ha aprobado formalmente.										