
# Modelo CSIRT para optimizar la respuesta ante incidentes de ciberseguridad en ONG

**Dagoberto Ramírez**

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2025

# Modelo CSIRT para optimizar la respuesta ante incidentes de ciberseguridad en ONG

**Dagoberto Ramírez**

Tesis de investigación presentada como requisito parcial para optar al título de:

**Magister en Seguridad Informática**

Director:

PhD. Miguel Ángel Roldán Álvarez

Línea de Investigación:

Ciencias Computacionales

Grupo de Investigación:

Automática, Electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2025

*“Daría todo lo que sé por la mitad de lo que ignoro”*

*R. Descartes*

# Resumen

En este trabajo se propuso un modelo de Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) adaptado a las necesidades de las organizaciones no gubernamentales (ONG). Para alcanzar este objetivo, se planteó una metodología estructurada en cuatro fases interrelacionadas. En la primera fase, se realizó una exhaustiva revisión de la literatura especializada para caracterizar las buenas prácticas de ciberseguridad en el ámbito de respuesta a incidentes, identificando patrones y elementos comunes relevantes. Después, en la segunda fase, se estableció un modelo conceptual basado en las buenas prácticas identificadas, adaptado a las particularidades y recursos de las ONG. En la tercera fase, se diseñó un modelo CSIRT basado en protocolos de actuación, especificando los pasos a seguir para la detección, análisis, contención, erradicación y recuperación de incidentes. En la cuarta fase, se evaluó la eficacia del modelo con una prueba piloto, analizando los resultados y adaptando las necesarias para validar y mejorar continuamente.

**Palabras clave:** Ciberseguridad, continuidad de negocio, CSIRT, estándares de ciberseguridad, gestión de incidentes y riesgos.

# Abstract

In this work, a Cyber Security Incident Response Team (CSIRT) model was proposed, adapted to the needs of non-governmental organizations (NGOs). To achieve this objective, a methodology structured in four interrelated phases was proposed. In the first phase, an exhaustive review of the specialized literature was carried out to characterize good cybersecurity practices in the field of incident response, identifying relevant patterns and common elements. Then, in the second phase, a conceptual model was established based on the identified good practices, adapted to the particularities and resources of NGOs. In the third phase, a CSIRT model was designed based on action protocols, specifying the steps to follow for the detection, analysis, containment, eradication and recovery of incidents. In the fourth phase, the effectiveness of the model was evaluated with a pilot test, analyzing the results and making the necessary adaptations to validate and continuously improve.

**Keywords:** Cybersecurity, business continuity, CSIRT, cybersecurity standards, incident and risk management.

# Contenido

**Pág.**

# Índice de figuras

**Pág.**

# Índice de tablas

**Pág.**

# 1. Introducción

Partiendo del conocimiento de la situación de muchas organizaciones sociales con respecto los recursos económicos y personal especializado, para esta tesis se planteó como objetivo general, proponer un modelo de centro de respuesta a incidentes que minimice el impacto generado por eventos de ciberseguridad implementando protocolos de actuación basados en buenas prácticas nacionales e internacionales en ONG que prestan servicios de tecnología. Para alcanzar este objetivo se definieron los siguientes objetivos específicos:

- Caracterizar buenas prácticas nacionales e internacionales de ciberseguridad en respuesta a incidentes.
- Establecer un modelo para el manejo de incidentes de ciberseguridad que pueda ser aplicado en ONG mediante las buenas prácticas caracterizadas.
- Desarrollar un marco de operaciones para un CSIRT que permita reducir el tiempo de respuesta ante los incidentes.
- Evaluar la efectividad del modelo mediante el análisis de resultados obtenidos de un caso de estudio donde se verifique que se reduce hasta en al menos el 30% el tiempo de respuesta a incidentes.

La mayoría de las ONG de Latinoamérica, en especial aquellas prestadoras de servicios y que actúan como intermediarias para proporcionar a otras organizaciones recursos tecnológicos que les permitan alcanzar sus objetivos, no cuentan con un Equipo de Respuesta a Incidentes de Seguridad Informática que ejecute adecuadamente determinados protocolos de actuación cuando se ven impactados por un ataque de ciberseguridad. Dichos protocolos podrían evitar que estas organizaciones enfrenten problemas legales y de reputación derivados de la exposición de datos confidenciales y la vulnerabilidad de la privacidad de sus colaboradores.

De acuerdo con lo anterior, se identificó una carencia en los procesos y procedimientos que facilitan la colaboración entre diferentes CSIRT, lo cual es crucial para detectar y abordar proactivamente cualquier amenaza de ciberseguridad que pueda comprometer, no solo los procesos tecnológicos, sino también resultar en la divulgación no autorizada de información sensible sobre beneficiarios, colaboradores y donantes. Un ataque cibernético

no gestionado adecuadamente puede resultar en la pérdida de fondos, la interrupción de servicios esenciales y, en casos extremos, la incapacidad de continuar operando. La falta de coordinación y comunicación efectiva entre estas entidades limita la capacidad de respuesta ante incidentes, permitiendo que las amenazas se propaguen y causen mayores daños.

Ante esto, se propuso un modelo de CSIRT con estándares reconocidos y mejores prácticas, para minimizar el impacto de los ataques cibernéticos y optimizar la gestión de incidentes. Este modelo se diseñó para fomentar la cooperación y coordinación eficientes entre las entidades CSIRT, permitiendo una respuesta más rápida y efectiva ante las amenazas emergentes en el entorno digital. Además, se establecieron mecanismos claros para la comunicación, el intercambio de información y la colaboración en la aplicación de medidas preventivas y correctivas, contribuyendo así a fortalecer la seguridad cibernética a nivel organizacional y sectorial.

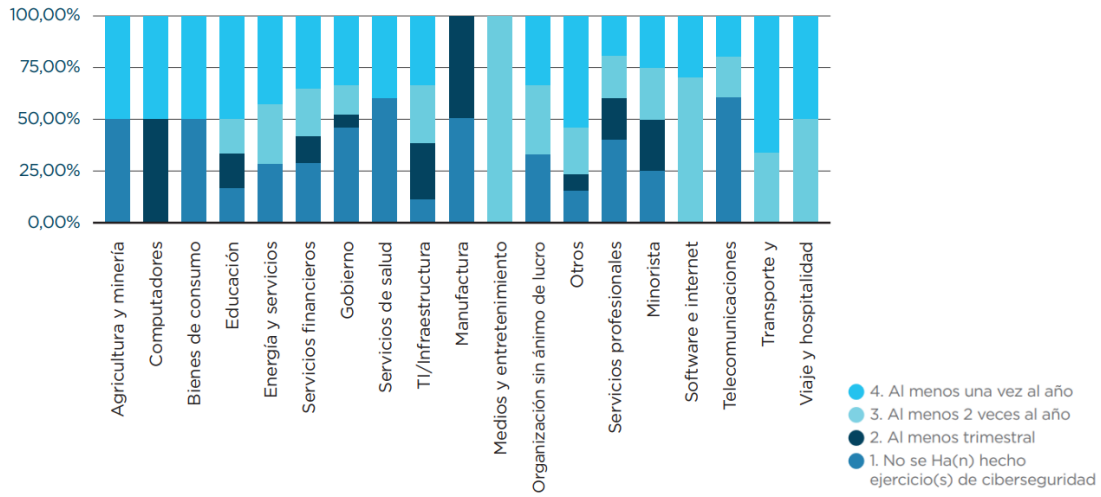
Gracias a la transformación digital, la conectividad y la digitalización de la información se han convertido en un factor fundamental en todos los sectores de la sociedad. Las organizaciones sin ánimo de lucro o no gubernamentales (ONG), se han adaptado gradualmente a estos cambios para aprovechar los beneficios que trae consigo esta transformación. Estos cambios tecnológicos incluyen desafíos que podrían evitar que las organizaciones desarrollen sus actividades, como la gestión de riesgos para minimizar las amenazas de ataques cibernéticos [1].

Muchas ONG comenzaron su proceso de digitalización después que otras entidades, lo que ha aumentado su superficie de ataque. Esto presenta desafíos que resultan en malas prácticas y más incidentes exitosos en su contra. Aunque en el primer semestre del 2019 hubo una reducción en la gravedad y en la frecuencia de las reclamaciones, en el sector social se presentó un incremento del 57%. Los ataques, motivados en su mayoría por intereses financieros, podrían haberse evitado con controles básicos. Aunque los delincuentes cifran datos críticos y exigen rescates, recurrir a aseguradoras cibernéticas no es la primera opción recomendada [2].

La expansión de las operaciones en línea, junto con la creciente recolección de información sensible y la creciente dependencia tecnológica, expone a las ONG a desafíos en cuanto a ciberseguridad. En muchos casos, estas organizaciones carecen de un departamento de

tecnología de la información (TI), lo que agrava aún más su vulnerabilidad. Según [3], el 66.67% de las ONG no realizaron una evaluación de riesgos entre 2022 y 2023, y como puede apreciarse en la Figura 1**,** menos del 35% no han realizado simulacros de ciberseguridad.

**Figura 1.** Frecuencia de ejercicios de simulación cibernética por sector



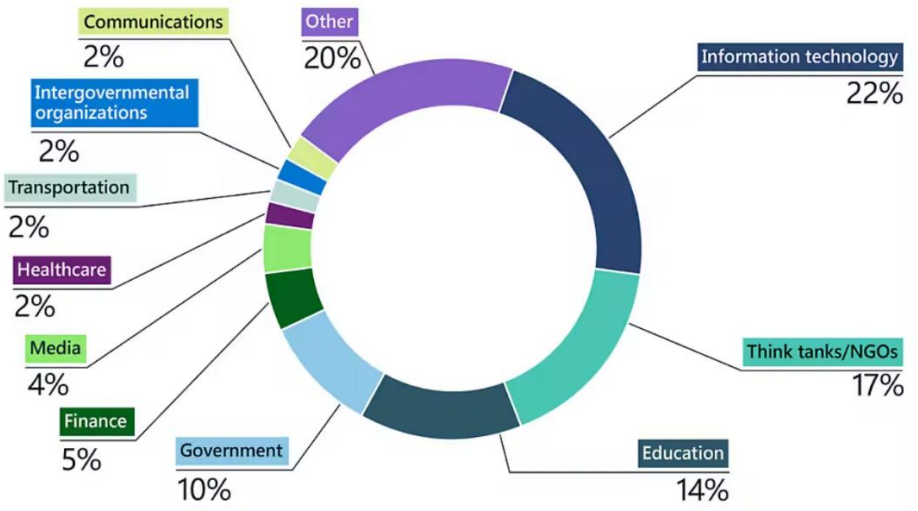

Nota. Frecuencia con la que se han realizado simulaciones en los diferentes sectores comerciales. Fuente: tomado de [3].

La combinación de estas circunstancias ha convertido a las ONG en objetivos atractivos para los ciberdelincuentes. La falta de recursos financieros y tecnológicos no solo dificulta la implementación de medidas de seguridad adecuadas, sino que también crea brechas en la protección de datos, lo que facilita a los ciber-atacantes el lanzamiento de sus ofensivas. Las ONG se enfrentan a una serie de amenazas, entre la cuales están el phishing, el malware y el ransomware, que pueden tener consecuencias devastadoras, comprometiendo la integridad de sus datos, la privacidad de sus colaboradores y la confianza del público en su misión y operaciones. Es imperativo que las organizaciones reconozcan estos desafíos y tomen medidas proactivas para fortalecer su postura de ciberseguridad y mitigar los riesgos asociados con las amenazas cibernéticas [4].

Por otro lado, [5] revela un aspecto crucial sobre la ciberseguridad: los actores estatales, apoyados por gobiernos, dirigen sus ataques a sectores industriales, y como se aprecia en la Figura 2, un notable 17 % de estos ataques se dirigieron en parte a las ONG. Este hallazgo posiciona a las organizaciones no gubernamentales en el tercer lugar de la lista

de objetivos, justo después de los sectores de Tecnologías de la Información y grupos de expertos, académicos y funcionarios públicos. Este fenómeno destaca la vulnerabilidad de las ONG ante las amenazas cibernéticas, lo que subraya la necesidad urgente de que estas organizaciones refuercen sus medidas de seguridad digital para protegerse de potenciales ataques y salvaguardar sus operaciones y datos sensibles.

**Figura 2.** Ataques dirigidos a los sectores industriales




Nota. Porcentajes de ataques dirigidos por los actores de estado nación. Fuente: tomado de [5].

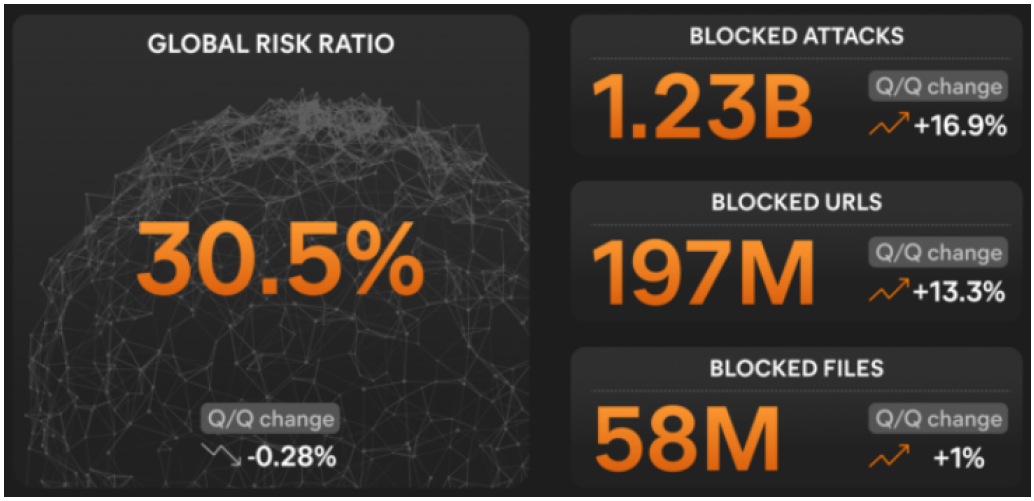
En su informe [6] busca comprender cómo las organizaciones sin ánimo de lucro usan la tecnología y que está basado en las respuestas de encuestas de 1732 profesionales de este sector, indica que el 27% de las ONG han experimentado un ciberataque. Esto sugiere que las ONG pueden enfrentar diversas consecuencias como la pérdida de datos confidenciales, interrupciones en los servicios, daño a la reputación y posiblemente sanciones legales, lo que podría afectar su capacidad para cumplir con su misión y objetivos. Además, podría resultar en costos financieros significativos relacionados con la recuperación de los datos y la reparación de la reputación.

Debido a la pandemia del Covid-19, las organizaciones se tuvieron que adaptar e implementar rápidamente cambios para poder afrontar los retos tecnológicos a los que se enfrentaron. Una de las situaciones más críticas que se presentó fue el aumento de los ciberataques. Según [7], los ciberdelitos denunciados en Colombia durante el 2022 aumentaron un 20.5% respecto al 2021, convirtiendo el 2022 en el segundo año con mayor

incremento en delitos cibernéticos, superado por el 2020, cuando se registraron más de 22.000 incidentes que equivalen a 109% en la variación porcentual.

El reporte del cuarto trimestre de 2023, [8] indica un incremento en el número de ataques bloqueados que supera los 10.000 millones y el índice de riesgo global es de 30.5% (Ver Figura 3). También se destacan los desarrollos de amenazas cibernéticas, incluyendo el regreso de Qakbot y nuevas estrategias de ataque, como el uso de la API de Google OAuth por parte de ladrones de información. Las estafas web, phishing y publicidad maliciosa dominaron el panorama, junto con el resurgimiento de amenazas móviles como el banquero Camaleón. Con el aumento de las estafas en línea, las ONG podrían ser víctimas, lo que ocasionaría una pérdida de confianza por parte de los donantes. Por eso es crucial que estas organizaciones refuercen sus medidas de seguridad cibernética para protegerse y garantizar la continuidad de sus operaciones.

**Figura 3.** Resultados reporte de amenazas




Nota. Principales estadísticas del reporte de amenazas. Fuente: tomado de [8].

En su iniciativa Gestión Tercer Sector, [9] menciona que los ciberataques están en aumento, afectando a grandes corporaciones como el SEPE y el Hospital Clínico de Barcelona, donde el 70% de las intervenciones programadas quedaron paralizadas durante días en marzo de 2023. En la mayoría de los casos, estos ataques buscan interrumpir la actividad y encriptar los datos para exigir rescates a cambio de la clave de desencriptación. Este es un claro ejemplo de que las ONG no pasan desapercibidas para los ciberdelincuentes.

Según [10], muchas ONG asumen que por su propósito social están a salvo de los delincuentes informáticos y no consideran la ciberseguridad como una prioridad debido a sus limitados recursos financieros y de tiempo. Esto las hace vulnerables a los ciberataques, especialmente porque los atacantes pueden aprovecharse de esta falta de preparación. Las organizaciones sin ánimo de lucro pequeñas no deben subestimar el riesgo de sufrir un ciberataque, ya que su tamaño y recursos escasos las hacen un objetivo atractivo para los ciberdelincuentes.

# 2. Marco Teórico y Estado del Arte

Esta sección presenta los fundamentos conceptuales y técnicos que sustentan el desarrollo del modelo CSIRT propuesto, así como un análisis del estado del arte en materia de manejo de incidentes de ciberseguridad. Mientras que el marco teórico aborda definiciones clave para el desarrollo de esta tesis, el estado del arte recopila y analiza experiencias, guías y modelos de referencia reconocidos a nivel nacional e internacional, lo que permite identificar buenas prácticas, tendencias actuales y vacíos que justifican la creación de un modelo adaptado a las necesidades de las ONG.

## 2.1 Marco teórico

En el ámbito de las organizaciones, existen diversos tipos que cumplen funciones específicas en la sociedad, como las empresas que buscan generar lucro a través de actividades comerciales, y las entidades gubernamentales que administran y regulan políticas públicas para el bienestar de la ciudadanía. Adicionalmente, hay otro tipo de compañías que no buscan lucro. Estas son las Organizaciones No Gubernamentales, conocidas comúnmente por sus siglas como ONG, que abordan diversas cuestiones sociales y humanitarias y son independientes del gobierno [11]. Estas entidades operan a nivel local, nacional e internacional; y buscan mejorar la calidad de vida de las personas, promover el desarrollo sostenible, y defender los derechos y libertades fundamentales.

En la era actual, la protección de la información de las organizaciones es imperativo. Por eso, hay que considerar que la ciberseguridad es fundamental en el mundo digital ya que abarca más que la protección de recursos en la nube. Si bien es cierto que la nube representa una parte significativa de los activos digitales que requieren protección, la ciberseguridad se extiende mucho más allá de este ámbito. Para tomar un ejemplo, [12] la define como la práctica de salvaguardar los recursos de las organizaciones contra ataques digitales. Esto implica implementar medidas de seguridad tanto preventivas como reactivas para salvaguardar la integridad, confidencialidad y disponibilidad de los activos digitales frente a una variedad de amenazas cibernéticas. Por otro lado, [13] en uno de sus artículos publicados en su centro de recursos, indica que el término se aplica a diferentes contextos empresariales y se clasifica en varias categorías, entre las que se encuentran la seguridad redes informáticas, la seguridad en aplicaciones, cuyo objetivo es proteger el software y

los equipos de las amenazas y la seguridad de la información, que protege la integridad y privacidad de los datos.

Los actores maliciosos están constantemente buscando aprovechar las debilidades de los sistemas digitales de las organizaciones. Tan pronto encuentran una falencia lanzan un ataque cibernético, es decir, cualquier intento de robo, exposición, modificación, o destrucción de datos, aplicaciones u otros activos mediante el acceso no autorizado a una red, sistema informático o dispositivo digital. Los perpetradores realizan estos ataques por una variedad de motivos, que pueden ir desde robos menores hasta actos de guerra. Utilizan diversas estrategias, como el uso de malware, engaños de ingeniería social y robo de contraseñas, para obtener acceso no autorizado a los sistemas objetivo. Aunque los ataques cibernéticos pueden tener diversas motivaciones, destacan tres categorías principales que son delictivas, personales y políticas [14].

Así mismo, se habla de incidente de seguridad de la información, cuando se hace referencia a cualquier evento o situación que ponga en riesgo la seguridad, confidencialidad o integridad de los sistemas informáticos, redes o datos de una organización. Estos incidentes pueden surgir debido a una variedad de factores, que van desde amenazas maliciosas, como ataques de hackers y malware, hasta errores humanos, como la pérdida o el robo de dispositivos, fallas técnicas, como la interrupción del servicio, o eventos naturales, como desastres naturales que afectan la infraestructura tecnológica. Para los equipos de respuesta a incidentes, es fundamental identificar, gestionar y mitigar estos incidentes de manera eficiente y efectiva. Esto implica una respuesta rápida y coordinada para minimizar el impacto del incidente y restaurar la normalidad operativa lo antes posible [15].

Con el aumento de las amenazas cibernéticas, la conformación de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas del inglés Computer Security Incident Response Team) se convierte en una prioridad. Los CSIRT son entidades que tienen como función principal entregar información oportuna relacionada con el tratamiento de incidentes de seguridad informática para dar respuestas rápidas y reducir el efecto que puedan producir estos eventos. Estos equipos deben informar sobre cómo proceder ante los diferentes tipos de incidentes, determinar la causa

y el impacto, ofrecer recomendaciones y soluciones y apoyar a los involucrados en la implementación de estrategias de respuesta [16].

Además de gestionar los incidentes y apoyar a los afectados, la mayoría de los CSIRT también ofrecen servicios preventivos y educativos a su comunidad. Emiten alertas sobre vulnerabilidades en el software y hardware utilizados, así como información sobre exploits y virus que aprovechan estas debilidades. De esta manera, los miembros pueden aplicar rápidamente parches y actualizaciones en sus sistemas. La creación de estos equipos permite aclarar más rápido y eficientemente la raíz del problema para evitar daños mayores internos o externos a terceros que puedan llegar a ser afectados [17].

Los estándares de ciberseguridad relacionados con los CSIRT son fundamentales para garantizar la eficacia y la consistencia en la respuesta a incidentes cibernéticos. Estos estándares son un conjunto de directrices y mejores prácticas diseñadas para proteger sistemas, redes y datos contra amenazas cibernéticas y proporcionan un marco estructurado y comúnmente aceptado que ayuda a las organizaciones a establecer y mantener un nivel adecuado de seguridad informática. Entre los estándares más conocidos se encuentra el ISO/IEC 27001, que establece requisitos para un sistema de gestión de seguridad de la información [18].

Otro estándar relevante es [19], que ofrece un conjunto de pautas y prácticas recomendadas para gestionar y mejorar la ciberseguridad de una organización sin importar su tamaño o el sector. Es adaptable a diferentes niveles de madurez y conocimientos, y no sigue un enfoque único para todas las organizaciones, lo que constituye su mayor fortaleza, ya que permite que cada entidad lo adapte a sus necesidades, recursos y prioridades, haciendo que su implementación sea realista y alineada con los objetivos estratégicos del negocio. Además, existen entre otras, instituciones como la Agencia de la Unión Europea para la Ciberseguridad (ENISA) [20] dedicadas a la ciberseguridad a nivel regional e internacional; y el estándar RFC-2350 [21] que proporciona directrices para la descripción y el funcionamiento de los CSIRT.

Las organizaciones deben prepararse para atender incidentes informáticos sin importar la razón. La gestión de incidentes de seguridad es un proceso que permite detectar, responder y mitigar eventos no deseados que comprometan la seguridad de sistemas o

datos confidenciales. Esto implica la planificación de procedimientos de respuesta, la coordinación de equipos multidisciplinarios, la recopilación de datos forenses y la implementación de medidas correctivas para minimizar el impacto y prevenir futuros incidentes. Estas actividades son esenciales para proteger la integridad, confidencialidad y disponibilidad de la información crítica de las organizaciones [22]. Una gestión de incidentes de seguridad eficaz ayuda a reducir el impacto que genera en las organizaciones la vulneración de la seguridad por parte de una amenaza. Por esta razón, es importante implementar planes y directivas que ayuden a gestionar este tipo de incidentes. Algunos pasos que se pueden dar durante la gestión de incidentes son preparar herramientas tecnológicas, identificar el incidente para determinar su alcance y contener, para impedir que el incidente afecte otros recursos [23].

La gestión de riesgos en el contexto de la ciberseguridad se entiende como un proceso que abarca la identificación, evaluación y mitigación de riesgos potenciales que puedan afectar los activos, la información o las operaciones de una organización y se centra en la identificación amenazas y vulnerabilidades que podrían comprometer la seguridad de los sistemas de información y la integridad de los datos. Su propósito es comprender el impacto de estos riesgos y priorizar soluciones para reducir las deficiencias en los procesos en los que se han identificado dichas vulnerabilidades [24]. En [25], se hace una diferencia entre el significado de los términos gestión del riesgo y gestionar el riesgo. El primer término es el conjunto de principios y metodologías que se utilizan para manejar el riesgo de manera efectiva en una organización o contexto determinado. Por otro lado, gestionar el riesgo implica aplicar estos principios y metodologías específicamente a riesgos particulares que enfrenta una organización. Es la acción concreta de implementar estrategias para abordar riesgos específicos y proteger los intereses de la organización.

Un tema relacionado con esta tesis es la continuidad de negocio, que se refiere a la capacidad de las organizaciones para mantener la operación, responder a incidentes cibernéticos u otros eventos y recuperarse de ellos rápida y efectivamente, garantizando la continuidad de las actividades frente a amenazas o ataques informáticos. Esto implica implementar planes, definir el alcance y llevar a cabo procesos y estrategias que permitan mitigar y gestionar los impactos negativos de los incidentes de seguridad [26]. En este sentido, la gestión de continuidad de negocio (BCM por sus siglas en inglés), se refiere al proceso de identificación de amenazas que pueden afectar potencialmente a una

organización y la evaluación del impacto que puede tener en la operación del negocio. Ofrece una estructura o plan para ayudar a las organizaciones a ser más fuertes cuando enfrentan problemas. Este plan ayuda a las organizaciones a responder de manera adecuada para proteger lo que es importante, como las personas importantes para la organización, su buena reputación, su nombre o marca y las actividades de valor [27].

## 2.2 Estado del arte

Uno de los principales referentes en Latino América es el Proyecto Amparo, cuyo propósito principal es promover la difusión y la capacitación en las organizaciones del sector privado y social en temas relacionados con la metodología de CSIRT. Uno se los hallazgos de este proyecto fue que la información relacionada a los incidentes de seguridad no se hace pública para no afectar la reputación de las organizaciones vulneradas. Esto hace que se dificulte la mitigación y la reducción del impacto del imprevisto ocurrido. Como hecho positivo se destaca el compromiso de los involucrados en el proyecto, a tal punto que los participantes piden la creación de un foro para compartir experiencias y buenas prácticas. En la etapa de implementación y gestión del proyecto se creó el “Manual Gestión de Incidentes de Seguridad Informática para América Latina y el Caribe” y adicionalmente se crearon 4 talleres con temáticas relacionadas a la gestión de incidentes. Como resultado, tras estos talleres, se evidencia una relación de confianza entre los entes participantes, haciendo que mejore la comunicación y que haya intercambio de información [28].

A nivel nacional se tiene un referente muy importante que es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT. Dentro de su propuesta de misión se incluyen la identificación de infraestructuras críticas, la gestión de riesgos y la entrega de información preventiva, apoyo y asesoría a empresas del sector privado y público para garantizar la continuidad en la prestación de sus servicios. En su portafolio cuenta con tres tipos de servicios. Servicios proactivos, que se enfocan en mejorar los procesos de seguridad para prevenir incidentes; servicios reactivos, que ayudan en la gestión y manejo de incidentes y servicios de gestión de la calidad, que buscan elevar la conciencia en seguridad digital y fortalecer las habilidades de líderes y empleados para fomentar una cultura de reporte y gestión de incidentes cibernéticos [29].

En [30] se consolidan los documentos CONPES en los que se tratan temas que tienen que ver con la seguridad digital. En este apartado se encuentran, entre otros, el CONPES 3701, cuyo propósito es detener el aumento de amenazas informáticas mediante una estrategia basada en políticas de ciberseguridad y ciberdefensa y en el que se estableció una instancia del COLCERT como organismo de defensa cibernética en Colombia y el CONPES 3854, en el que se establece un conjunto de reglas y prácticas estructuradas en torno a la seguridad digital. En este último, el COLCERT jugó un papel importante en cuanto a la gestión de incidentes digitales y la capacitación para funcionarios públicos y privados y concientización del público general.

En los Estados Unidos, la Cybersecurity and Infrastructure Security Agency (CISA) es una institución para la defensa cibernética del país que pertenece a la agencia de ciberdefensa de América. CISA despliega una amplia gama de recursos y herramientas destinadas a gestionar y mitigar el impacto ocasionado por ciberataques. Destacan los programas de capacitación diseñados para reducir los riesgos de seguridad, y los grupos de colaboración que facilitan la interconexión de actores clave, fomentando la construcción de un entorno digital más seguro y resiliente. Además, CISA ofrece un gran repositorio en línea con publicaciones, incluyendo guías, informes y políticas, proporcionando una valiosa recopilación de conocimientos y orientaciones para enfrentar los desafíos del ciberespacio. Esta combinación de iniciativas y recursos posiciona a CISA como un pilar fundamental en la defensa cibernética de los Estados Unidos, fortaleciendo la capacidad del país para hacer frente a las crecientes amenazas y desafíos en el ámbito digital [31].

En el artículo “Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta – CSIRT", el autor plantea el problema de gestión que tienen los administradores de TI de entidades públicas de Bolivia frente a la gran cantidad de incidentes de seguridad reportados y propone un modelo gestión para ayudar a los equipos de respuesta a atender efectivamente estos incidentes. El desarrollo de este modelo se basa en la normativa nacional de Bolivia y en el estándar ISO 27035 que proporciona los procesos y directrices que se deben realizar para garantizar la gestión eficaz de los eventos de seguridad. Como resultado no solo se obtiene el modelo, sino que también se determinan herramientas de gestión útiles y se definen los roles y responsabilidades de las personas que intervienen en el proceso [32].

En la tesis de grado “Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad”, el autor presenta un modelo integral de ciberseguridad diseñado para establecer un eficaz manejo de incidentes de seguridad. En su investigación, la autora desarrolla una metodología compuesta por tres fases fundamentales: la identificación y análisis de riesgos de ciberseguridad, la caracterización de normativas y procedimientos para el manejo y respuesta a incidentes, y la evaluación práctica del modelo mediante un caso de estudio concreto. Los valiosos aportes de esta investigación al presente trabajo se centran en proporcionar una estructura metodológica sólida y aplicable, orientada a fortalecer el manejo de incidentes de ciberseguridad en el contexto de operaciones que ofrecen servicios informáticos. Este enfoque se alinea con el propósito del proyecto, que busca construir un modelo de ciberseguridad basado en el análisis de riesgos, para fortalecer un manejo de incidentes de ciberseguridad para las ONG que prestan servicios tecnológicos [33].

Pese a los esfuerzos de los autores mencionados, y aunque existen organizaciones como FIRST, que reúne equipos de seguridad informática de diversos sectores, facilita una respuesta más efectiva a los incidentes de seguridad mediante una membresía y promueve la cooperación, la coordinación y el intercambio de información entre sus miembros [34], hasta ahora no se ha consolidado un modelo específico para las organizaciones no gubernamentales que incluya mejores prácticas y que consideren la diversidad de estructuras organizativas y la variabilidad en los niveles de madurez cibernética entre estas organizaciones. Por tanto, se necesita investigación adicional y desarrollo de modelos de CSIRT específicos para las ONG, que aborden eficazmente sus requerimientos y desafíos particulares en materia de ciberseguridad.

# 3. Metodología

Este capítulo se estructuró en cuatro fases como se muestra en la Figura 4. Estas fases fueron definidas para cumplir con los objetivos específicos planteados de manera progresiva y sistemática. Cada fase representa un paso estratégico en la construcción e implementación del modelo CSIRT propuesto, facilitando una comprensión integral del proceso. Al finalizar las actividades desarrolladas, se da completitud al objetivo general

planteado. En conjunto, estas fases ofrecen una visión clara y estructurada del proceso requerido para establecer un centro de respuesta a incidentes funcional, sostenible y ajustado al contexto y recursos de las ONG.

**Figura 4.** Fases de la metodología


Nota. Resumen de las fases desarrolladas en la metodología.

## 3.1 Fase 1: Caracterización de buenas prácticas de respuesta a incidentes

A continuación, se detallan las actividades que se realizaron para buscar, seleccionar y caracterizar la información necesaria que fundamentó la creación del modelo de manejo de incidentes de ciberseguridad. Estas actividades hicieron parte de una fase clave del proyecto, ya que permitieron identificar y analizar fuentes confiables que abordan los procesos de respuesta a incidentes de seguridad informática. Esta fase permitió comprender las mejores prácticas en el área y adaptar sus elementos esenciales al contexto de las organizaciones no gubernamentales.

### 3.1.1 Búsqueda de documentación

**Tabla 1.** Matriz de consolidación de documentos encontrados

| Documento/Estándar/ Recurso Consultado | Fuente | Descripción | Aporte a la Tesis |
|---|---|---|---|

Nota. Formato usado para consolidar la información relevante de los documentos encontrados.

Se realizó una búsqueda en la base de datos académica IEEE, en Scholar Google y en los repositorios de los institutos NIST y ENISA. Se buscaron documentos relacionados con buenas prácticas de ciberseguridad y gestión de incidentes de ciberseguridad. Se examinaron estudios, artículos, estándares y documentos relevantes para identificar las mejores prácticas implementadas en diferentes países y organizaciones. Además, se consideraron informes y documentos de organismos gubernamentales y no gubernamentales internacionales como la Organización de los Estados Americanos (OEA) y el Forum of Incident Response and Security Teams (FIRST) para obtener una perspectiva global y variada. Al finalizar este proceso se recolectaron un total de 20 materiales que se consolidaron en la etapa de resultados en una matriz como la que se muestra en la Tabla 1.

### 3.1.2 Selección de documentos para la base de conocimientos

Para seleccionar el material bibliográfico final que sirvió de base para el desarrollo del modelo de manejo de incidentes, se estableció un sistema de puntuación que permitió evaluar de forma objetiva la calidad y pertinencia de cada documento consultado. Este sistema se aplicó a cuatro criterios fundamentales: accesibilidad, nivel de detalle, calidad de la fuente y actualidad y/o vigencia del contenido. Cada criterio fue calificado en una escala del 1 al 5, y la suma total de los puntajes permitió identificar los documentos más relevantes. En la Tabla 2 se describen los niveles de puntuación por cada criterio.

**Tabla 2.** Definición de los niveles de puntuación por criterio

| Criterio | Definición de Puntuación | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Accesibilidad | Solo disponible mediante compra o | De acceso limitado con | Disponible en bases de datos especializadas | Requiere registro o suscripción | Disponible gratuitamente en línea o en |

| | | | | | |
|---|---|---|---|---|---|
| | suscripción sin opciones de acceso gratuito | restricciones de pago parcial | o accesible solo a través de instituciones educativas | gratuita en una plataforma | plataformas abiertas sin restricciones |
| Nivel de detalle | Menciona la gestión de incidentes, pero no aporta información práctica | Presenta solo una visión general del tema sin profundizar en estrategias técnicas o metodológicas | Contiene información relevante, pero sin mucho nivel de detalle | Explica buenas prácticas y estrategias de respuesta a incidentes con cierto nivel de profundidad, pero sin ejemplos específicos o estudios de caso | Proporciona información completa, incluyendo fases del proceso, metodologías, herramientas y casos de estudio |
| Calidad de la fuente | Artículos y blogs generales de internet | Artículos publicados por proveedores de productos o servicios reconocidos en el área de ciberseguridad | Documentos de agencias u organizaciones como la OEA, MinTIC y la SIC que incluyen guías de ciberseguridad | Documentos de bases de datos especializadas o de universidades con programas avanzados en ciberseguridad | Documentos de organismos globalmente reconocidos como NIST, ENISA, CISA, LACNIC, FIRST o RFC |
| Actualidad y/o vigencia | Materiales con contenido obsoleto y desactualizado | Materiales con contenido parcialmente desactualizado | El documento es vigente, sin embargo, puede requerir actualizaciones puntuales | Materiales con contenido vigente y aplicable sin importar la fecha de publicación | Materiales que se encuentran en su última versión y el contenido sigue siendo aplicable |

Nota. Sistema de puntuación definido para evaluar los criterios de selección.

**Tabla 3.** Matriz de asignación de puntuación

| Documento, Estándar, Recurso Consultado | Accesibilidad | Nivel de Detalle | Calidad de la Fuente | Actualidad | Total |
|---|---|---|---|---|---|

Nota. Formato usado para calificar los documentos con base en los criterios definidos.

Con los criterios de selección definidos, se procedió a asignar la correspondiente puntuación a cada uno de los documentos encontrados. Se seleccionaron los materiales con una puntuación igual a 19 y 20 porque representan los mejores recursos para la base de conocimientos. Estos documentos incluyen los aspectos más importantes de otros materiales y, en algunos casos, han sido referenciados en fuentes que obtuvieron menor

puntuación, lo que respalda su relevancia y calidad. La Tabla 3 muestra la matriz usada para la asignación de la puntuación a los documentos encontrados.

### 3.1.3 Caracterización de los documentos seleccionados

Los documentos seleccionados fueron caracterizados considerando tres aspectos clave para su clasificación y análisis:

- **Origen:** se clasificaron según su procedencia nacional o internacional, permitiendo observar el contexto específico de cada fuente.
- **Etapa del Proceso:** para el desarrollo de la tesis se identificaron dos etapas. La primera es la relacionada a la gestión de incidentes de ciberseguridad y la segunda tiene que ver con la creación del modelo CSIRT. Esta característica facilita el uso de cada documento en la etapa correspondiente.
- **Categoría:** cada documento se clasificó según su propósito en esta tesis, identificando si describe procedimientos para la gestión de incidentes, si propone políticas o si sirve como recurso para el modelo una vez establecido.

La Tabla 4 ejemplifica la matriz usada en la sección de resultados para realizar la caracterización de los documentos seleccionados.

**Tabla 4.** Matriz de caracterización de documentos

| Documento. Estándar o Recurso Consultado | Origen | Etapa del Proceso | Categoría |
|---|---|---|---|

Nota. Formato usado para caracterizar los documentos seleccionados.

**Tabla 5.** Matriz de resumen de buenas prácticas encontradas

| Documento/Estándar/ Recurso Consultado | Etapa del Proceso | Buenas Prácticas |
|---|---|---|

Nota. Formato usado para resumir las buenas prácticas caracterizadas.

Después de caracterizar los documentos seleccionados, se procedió a identificar y resumir las buenas prácticas recomendadas en cada uno de ellos, con el objetivo de extraer los

elementos clave que pudieran aplicarse en el contexto de las organizaciones no gubernamentales. Esta información fue organizada y consolidada en una matriz como la presentada en la Tabla 5, lo que permitió visualizar de forma estructurada los aportes de cada fuente y facilitó la identificación de prácticas recurrentes. Estas serán la base para establecer el modelo para el manejo de incidentes.

## 3.2 Fase 2: Establecimiento de un modelo para el manejo de incidentes de ciberseguridad en ONG

En esta fase se detallan las actividades realizadas para establecer un modelo de manejo de incidentes de ciberseguridad adaptado a las particularidades de las ONG. El diseño del modelo se fundamentó en las buenas prácticas identificadas previamente durante la fase de caracterización de documentos, seleccionando aquellas que resultan viables y efectivas en entornos con recursos limitados. Se tuvo en cuenta la realidad operativa de las ONG, donde muchas veces no existe un equipo de TI dedicado, por lo que el modelo debía ser práctico, escalable y de fácil adopción.

### 3.2.1 Deseño de un modelo para manejo de incidentes en una ONG

Para el diseño del modelo propuesto, se seleccionaron como documentos principales el estándar del NIST y el modelo de ENISA, reconocidos internacionalmente por su enfoque estructurado y buenas prácticas en la gestión de incidentes de ciberseguridad. Como complemento, se utilizó el material desarrollado por Carnegie Mellon University (CMU). A partir del análisis de estas fuentes, se definió un modelo de atención de incidentes compuesto por cinco etapas fundamentales que permiten una gestión ordenada frente a eventos de seguridad informática.

### 3.2.2 Creación del flujograma del proceso de manejo de incidentes de ciberseguridad

Con el modelo de manejo de incidentes ya establecido, se creó un flujograma de proceso que permite representar de forma gráfica y clara la secuencia de pasos que debe seguir el personal encargado ante la ocurrencia de un evento de ciberseguridad. Este diagrama facilita la comprensión del proceso, estandariza la respuesta y sirve como guía de

actuación para los diferentes miembros del equipo. El flujograma incluye desde el momento en que se recibe el reporte de un incidente, pasando por las etapas de análisis, clasificación, respuesta y escalamiento, hasta las actividades posteriores al cierre del caso.

## 3.3 Fase 3: Desarrollo de un marco de operaciones para un CSIRT

En esta fase se diseñó un modelo organizacional para el CSIRT que se ajusta a las características típicas de las ONG, como la escasez de recursos humanos especializados, la infraestructura técnica limitada y las restricciones presupuestales. El modelo propuesto busca ser funcional en entornos donde no existe un equipo de TI dedicado, permitiendo que personal con otras responsabilidades pueda asumir roles dentro del CSIRT en caso de incidentes. Además, se estructuró como un modelo escalable, con el objetivo de que pueda adaptarse a organizaciones con distintos niveles de madurez tecnológica y capacidades operativas. Esta flexibilidad permite que el modelo sea implementado tanto en ONG pequeñas como en aquellas con procesos más avanzados.

### 3.3.1 Diseño de un modelo CSIRT para ONG

En esta actividad se propuso la estructura jerárquica del CSIRT y se definieron los roles y responsabilidades de los integrantes del equipo. Esta etapa es clave para su implementación en cualquier ONG, asegurando que el modelo incluya las mejores prácticas documentadas y que están alineadas con las capacidades de la organización. La definición de la estructura organizativa permite que personal no especializado pueda desempeñar funciones clave con el apoyo adecuado. Además, se procuró que esta estructura integrara las mejores prácticas documentadas y que fuera coherente con las condiciones reales de operación de las ONG.

En el modelo propuesto, la función de Gobierno se definió como una responsabilidad explícita del Líder del CSIRT, lo que significa que este rol debe comprender muy bien el contexto de la organización para procurar que la que las políticas y la estrategia del esquipo estén alineadas con la misión y el propósito de la ONG. Adicionalmente, los demás miembros del equipo deben apoyar esta función de manera transversal para asegurar que

el CSIRT no solo actúe de manera reactiva ante incidentes, sino que cuente con un marco de gobernanza que fortalezca su efectividad y sostenibilidad en el tiempo.

### 3.3.2 Definición de los servicios que prestará el CSIRT

Los factores que influyeron para la definición de los servicios fueron el presupuesto y los conocimientos del personal de la organización. Adicional a esto, en la literatura se encontró que existen tres tipos de servicios que un CSIRT puede prestar. Estos son, los servicios reactivos, proactivos y complementarios. Con esto, y teniendo en cuenta la limitación de recursos humanos, tecnológicos y presupuestales de las ONG, hay servicios que no se contemplan dentro del alcance, por ejemplo, la implementación de sistemas de monitoreo y detección de intrusos o la evaluación y gestión de vulnerabilidades. Se realizó un análisis de los servicios encontrados para determinar los que más se adecuan a las características de las ONG.

### 3.3.3 Definición de protocolos de actuación

**Tabla 6.** Formato para documentar el historial de revisiones

| **Historial de revisiones** | | | | |
|---|---|---|---|---|
| **Documento:** | Nombre del protocolo | | **Fecha de creación** | DD/MM/YYYY |
| **Razón de la revisión** | **# de revisión** | **Revisado por** | **Aprobado por** | **Fecha de revisión** |
| Creación del documento | 1.0 | Nombre del revisor | Nombre del aprobador | DD/MM/YYYY |

Nota. Formato sugerido para documentar los cambios en los protocolos de actuación.

Para la redacción de los protocolos de actuación se consideraron las fases del modelo de atención de incidentes y la estructura organizacional del modelo CSIRT propuestos, procurando que los procedimientos establecidos sean congruentes con las actividades y responsabilidades tenidos en cuenta en el planteamiento de dichos modelos. Los protocolos definidos fueron el protocolo de registro y clasificación, protocolo de atención, protocolo de comunicaciones y protocolo de escalamiento. La razón para seleccionar estos 4 protocolos fue que, durante el análisis de los documentos finales seleccionados para la base de conocimientos de esta tesis, estos temas resaltaban entre otros, evidenciando su

importancia para la gestión de incidentes de ciberseguridad. La documentación del historial de versiones de los protocolos de actuación se realiza en un formato como el que se muestra en la Tabla 6.

### 3.3.4 Redacción de un plan de implementación del modelo de CSIRT

El plan de implementación del modelo CSIRT se desarrolló con base en la documentación seleccionada para el desarrollo de esta tesis, identificando etapas clave para su correcta ejecución que abarcan desde la definición del grupo de atención y la redacción de la política y misión, hasta la preparación de los recursos esenciales como formularios, sistemas de gestión de tickets y documentación de referencia. Asimismo, se contempló la selección del personal, la identificación de colaboradores clave y la capacitación del equipo para asegurar que cuenten con las habilidades necesarias para la gestión de incidentes. Además de esto, se tuvo en cuenta la difusión del modelo dentro de la organización y la puesta en marcha del CSIRT.

## 3.4 Fase 4: Evaluación de la efectividad del modelo mediante el análisis de resultados obtenidos de un caso de estudio

La evaluación de la efectividad del modelo CSIRT se realizó en una ONG real que no contaba con un equipo de TI establecido. Para ello, se realizó un estudio de caso que permitió medir el desempeño del equipo en términos del tiempo de reacción ante incidentes de ciberseguridad. Esta fase incluyó cuatro actividades orientadas a implementar y validar la funcionalidad del modelo propuesto, medir los tiempos de respuesta antes y capacitar los miembros del equipo y recopilar la información necesaria para el análisis de los resultados.

### 3.4.1 Iniciar el plan de implementación

Aunque los pasos descritos anteriormente en la redacción del plan de implementación son en resumen los más relevantes según las buenas prácticas caracterizadas, los que eran realmente importantes o indispensables para continuar con el desarrollo de este trabajo

eran la selección del personal y la preparación del material de entrenamiento. Por tal motivo, en esta parte no se incluyeron los demás pasos, ya que se consideraban específicos de cada organización y no eran necesarios para el desarrollo del ejercicio de mesa que se implementó en las actividades posteriores.

### 3.4.2 Realizar una medición inicial del tiempo de respuesta ante incidentes de ciberseguridad

**Tabla 7.** Formato usado en ejercicio de mesa

| Momento | Etapa | Actividad | Descripción de la actividad | Hora de Inicio | Hora de Finalización |
|---|---|---|---|---|---|
| 1, 2, 3 | | | | hh:mm | hh:mm |

Nota. Formato usado para registrar las respuestas a las preguntas realizadas en el ejercicio de mesa.

Para realizar la primera medición del tiempo de respuesta ante incidentes de ciberseguridad, se diseñó un ejercicio de mesa que simulaba un ataque de phishing y se le presentó a los miembros del equipo en tres momentos secuenciales relacionados a las etapas de reporte, clasificación, acciones de respuesta y actividades post-incidente. Cada momento incluía una pregunta formulada para que los participantes, con sus conocimientos actuales, es decir, sin recibir el entrenamiento en gestión de incidentes de seguridad informática, listaran las actividades relacionadas a cada etapa. El ejercicio se creó con base en [35] e incluía objetivos, contexto, alcance y la guía que introducía los tres momentos mencionados. Para obtener los tiempos de respuesta, se les pidió a las personas que diligenciaran un formato en Excel como el que se ve en la Tabla 7, donde además de las actividades, debían dar una descripción de cada una de ellas y registrar el tiempo de inicio y de finalización de cada momento.

### 3.4.3 Capacitar al equipo y realizar una segunda medición del tiempo de respuesta

Como parte del proceso de implementación del modelo CSIRT, se llevó a cabo una sesión de capacitación dirigida a los integrantes del equipo. Esta capacitación incluyó la socialización del modelo de atención de incidentes propuesto, así como la explicación de los protocolos de actuación definidos. Posteriormente, en una tercera sesión, se repitió el

ejercicio de mesa utilizado en la primera medición, siguiendo exactamente el mismo escenario y dinámica. El propósito fue medir nuevamente el tiempo de respuesta, esta vez con el modelo implementado, para comparar los resultados e identificar si hay mejoras.

### 3.4.4 Analizar los resultados obtenidos

En esta actividad se analizaron los resultados obtenidos en las dos mediciones realizadas, con el fin de evaluar la efectividad del modelo CSIRT propuesto. Con los tiempos de inicio y finalización de cada momento registrados por el equipo en las sesiones 1 y 3, se calculó el tiempo invertido, tanto para la primera medición antes del entrenamiento, como para la segunda. Esto dio como resultado, un tiempo total invertido para la medición inicial T1 y un tiempo total invertido para la medición final T2, que fueron usados para calcular la variación porcentual. Este análisis permitió identificar el porcentaje de cambio en los tiempos de respuesta.

# 4. Resultados

En esta sección se presentan los resultados obtenidos a lo largo del desarrollo de la tesis. Cada uno de los apartados corresponde directamente a una de las actividades descritas en la metodología, lo que permite mantener una relación coherente entre lo planificado y lo ejecutado. Esta estructura facilita la comprensión del proceso seguido, así como la evaluación del cumplimiento de los objetivos planteados. Los hallazgos se derivan tanto del análisis de la documentación consultada como de la implementación y evaluación del modelo propuesto.

## 4.1 Caracterización de buenas prácticas para la creación de CSIRT y de ciberseguridad para el manejo de incidentes

A continuación, se presentan los resultados obtenidos del proceso de búsqueda, análisis y caracterización de buenas prácticas orientadas a la adecuada gestión de incidentes de ciberseguridad y a la creación e implementación de un CSIRT en una ONG. Las buenas prácticas recopiladas fueron seleccionadas con base en criterios de relevancia, accesibilidad, nivel de detalle, actualidad y calidad de la fuente, lo que aseguró una base sólida y contextualizada para el desarrollo del modelo propuesto. La información fue organizada para facilitar su comprensión, estableciendo así las bases para estructurar un modelo adaptado a las necesidades y capacidades de las ONG. Estos resultados constituyen un insumo fundamental para las siguientes fases de la tesis.

### 4.1.1 Documentación encontrada

**Tabla 8.** Documentos encontrados

| Documento/Estándar/Recurso Consultado | Fuente | Descripción | Aporte a la Tesis |
|---|---|---|---|
| Prerequisites for Building a Computer Security Incident Response Capability [36] | IEEE | Este documento presenta fuentes bibliográficas relevantes para la creación de un CSIRT e indica requisitos previos necesarios para constituir este tipo de equipos en una organización. | - Estándares y referencias usadas.<br>- Conjunto de requisitos previos para la creación de un CSIRT.<br>- La herramienta para resumir la información recopilada: se |

| | | | |
|---|---|---|---|
| | | | usa una matriz conceptual en la que se discriminan los aportes que hace la literatura encontrada a los requisitos previos caracterizados. |
| A step-by-step approach on how to set up a CSIRT [37] | Enisa | Este documento es una guía en la se detallan los pasos para crear un CSIRT. | - Servicios que ofrece un CSIRT<br>- Definición del modelo financiero<br>- Definición de la estructura organizacional<br>- Tipos de modelos de CSIRT<br>- Ejemplos de procedimientos técnicos y operacionales |
| Expectations for Computer Security Incident Response [22] | RFC | El estándar RFC-2350 describe buenas prácticas para el manejo de los incidentes de ciberseguridad por parte de un CSIRT. | - Describe la forma como debe interactuar el CSIRT con la comunidad para la cual opera y con otros CSIRT<br>- Establece la correcta forma de comunicación que debe implementar el CSIRT<br>- Sugiere una plantilla de políticas y procedimientos |
| Buenas Prácticas para Establecer un CSIRT Nacional [38] | Organización de los Estados Americanos | Este documento analiza varias clases de CSIRT y examina el proceso de creación y puesta en funcionamiento de un CSIRT nacional. Contempla criterios y aspectos necesarios para determinar su estructura, misión, visión, ámbito de acción, servicios, plazos, y aspectos legales e institucionales. | - Marco institucional y legal<br>- Alcance y servicios que ofrece un CSIRT<br>- Estructura organizacional<br>- Actividades para establecer un CSIRT<br>- Requisitos de capacitación para el personal |
| Guía Práctica para CSIRTs [39] | Organización de los Estados Americanos | este documento sirve de guía para la creación, desarrollo o modernización de un CSIRT de carácter público a partir de una mirada estratégica. | - Cómo planear y diseñar un CSIRT con enfoque sostenible y a largo plazo<br>- Concejos sobre temas puntuales para que un CSIRT sea eficiente<br>- Presenta los principales retos que puede enfrentar un CSIRT |
| Computer Security Incident Response Team (CSIRT): How to Build One [40] | Heimdal Security | Este artículo proporciona un panorama general y conciso de lo que es un CSIRT y cómo puede adoptarse en una organización para hacerle frente a las ciber amenazas. Además, resume los modelos operacionales de CSIRT que se pueden crear, señala las principales habilidades que deben tener sus miembros y resalta 3 elementos importantes que se deben tener en cuenta a la hora de implementar este tipo de equipos. | - Explica la forma como funciona un CSIRT<br>- Resume los modelos operacionales de CSIRT<br>- Enlista habilidades que deben tener los miembros del equipo |
| Cybersecurity Best Practices [41] | CISA | CISA es una agencia nacional de Estados Unidos que provee | En su página de recursos se pueden encontrar materiales |

| | | | |
|---|---|---|---|
| | | artículos, guías, servicios y herramientas que permiten mejorar la postura de ciberseguridad, tanto en organizaciones públicas como privadas. Este artículo entrega una serie de recursos disponibles relacionados a buenas prácticas en ciberseguridad. | para consulta de implementación útiles para los CSIRT. |
| Incident Response Recommendations and Considerations for Cybersecurity Risk Management [42] | NIST | Este documento ayuda a las organizaciones a integrar las capacidades para responder a incidentes de seguridad y manejarlos de forma eficiente y efectiva, con la gestión de riesgos de ciberseguridad. | - Explica las fases del modelo para el manejo de incidentes.<br>- Presenta ejemplos de roles y responsabilidades para el manejo de incidentes.<br>- Define elementos clave para las políticas, procesos y procedimientos de la gestión de incidentes. |
| Good Practice Guide for Incident Management [43] | Enisa | Esta guía entrega una descripción de buenas prácticas para el manejo de incidentes de seguridad de la información. | - Propone flujos de trabajo para el manejo de incidentes<br>- Describe el proceso de manejo de incidentes |
| Organizational Models for Computer Security Incident Response Teams (CSIRTs) [44] | Carnegie Mellon University | Este documento es un manual que proporciona información relevante sobre los tipos de modelos organizacionales de CSIRT que se pueden implementar. Dentro de la información que se puede encontrar en este manual no solo está la estructura de cada modelo, sino también sus ventaja y desventajas. | - Define los principales componentes de un CSIRT (constituyentes o grupo atendido, misión y servicios)<br>- Describe los modelos organizacionales de CSIRT, incluyendo elementos importantes como su estructura, servicios y recursos |
| Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0 [45] | FIRST | el objetivo de este framework es simplificar la forma de establecer y mejorar las operaciones de un CSIRT, apoyando a los equipos en el proceso de identificación, selección de los servicios y sus elementos que los componen. | - Define los elementos clave del framework<br>- Detalla cada uno de los elementos definidos<br>- Indica las actividades que se deben llevar a cabo en cada servicio e incluye su propósito, la descripción y el resultado. |
| Curso básico para la creación y gestión de un CSIRT [46] | Lacnic | Desde la plataforma educativa de Lacnic se ofrece este curso que permite entender cómo crear y gestionar un CSIRT. | Dentro de los temas que se ven en este curso y que aportan a la tesis están:<br>- Estructura organizacional de un CSIRT<br>- Políticas y procedimientos característicos de un CSIRT<br>- Tratamiento seguro en el intercambio de información |
| Manual Básico de Gestión de Incidentes de Seguridad Informática [47] | Lacnic | Este manual entrega la información necesaria para el proceso de integración de un CSIRT en las organizaciones, incluyendo el marco normativo, una descripción de la infraestructura y políticas de seguridad informática. | - Recomienda directrices y acciones para la creación de un CSIRT<br>- Explica los modelos organizacionales de CSIRT<br>- Describe las funciones que debe tener internamente un CSIRT |

| | | | |
|---|---|---|---|
| | | | - Detalla las políticas para la gestión de riesgo |
| Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales [48] | SIC | Este documento orienta a los encargados del tratamiento de datos personales sobre cómo enfrentar incidentes relacionados con este tipo de datos. | - Establece el proceso para la conservación de registros internos<br>- Propone un protocolo de respuesta a incidentes<br>- Describe los pasos que se deben seguir para responder a un incidente de seguridad |
| How to create a CSIRT: 10 best practices [49] | TechTarget | Este artículo explica brevemente en 10 pasos las buenas prácticas que se deben tener en cuenta para crear un CSIRT | Presenta de una manera resumida las pautas que se deben seguir para facilitar la creación de un CSIRT |
| Handbook for Computer Security Incident Response Teams (CSIRTs) [50] | Carnegie Mellon University | Esta guía para la creación y manejo de CSIRT busca entregar los recursos necesarios tanto para los equipos en proceso de formación como para los existentes. | Este documento sirve como referencia para:<br>- Definir la estructura organizacional, políticas, servicios y necesidades<br>- Establecer el servicio de manejo de incidentes<br>- Describir las operaciones del CSIRT |
| Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información [51] | MinTIC | Este documento aplica a todas las organizaciones que quieran implementar un modelo para la gestión de incidentes de seguridad de la información. | - Esta guía propone una serie de pasos que abarcan todo el ciclo de vida de la gestión de incidentes de seguridad (preparación; detección, evaluación y análisis; contención, erradicación y recuperación; y actividades post-incidente).<br>- Describe los roles y perfiles requeridos para la atención de incidentes.<br>- Hace recomendaciones sobre actividades adicionales que se deben tener en cuenta para mitigar el impacto de los incidentes. |
| Guía 21 - Gestión de Incidentes [52] | MinTIC | La página del gobierno digital de MinTIC provee una serie de guías, que, aunque están enfocadas para las entidades públicas y sus proveedores, también puede ser usada como referencia para cualquier organización que desee implementar un modelo de seguridad de la información. | Conjunto de guías para la implementación de metodologías, políticas y procesos relacionados a la gestión de la seguridad de la información en todas sus fases. |
| ISO/IEC 27035-1:2023 Information technology - Information security incident management [53] | ISO | Este estándar establece los fundamentos para la gestión de incidentes de seguridad de la información de manera genérica para que pueda adaptarse a cualquier organización, sin importar su tamaño o sector. | Esta norma sirve como guía para establecer los procesos que cualquier organización debe seguir para la gestión de incidentes de seguridad de la información. |

| | | | |
|---|---|---|---|
| ColCERT [54] | ColCERT | El Grupo de Respuesta a Emergencias de Ciberseguridad de Colombia se creó para acoplar de una manera coordinada a organizaciones tanto públicas como privadas en torno a temas relacionados con ciberseguridad. | Un CSIRT pude usar la página de ColCERT para:<br>- Reportar correos de Phishing<br>- Denunciar ciberdelitos<br>- Reportar Incidentes<br>- Acceder a boletines |

Nota. Formato con la consolidación de la información relevante de los documentos encontrados.

En la Tabla 8 se presentan los documentos recopilados durante el proceso de búsqueda, organizados en el orden en que fueron encontrados. A cada documento se le realizó un análisis previo a partir de su introducción y tabla de contenido, lo que permitió identificar rápidamente su enfoque, alcance y relevancia para el desarrollo de esta tesis. Este análisis inicial facilitó la descripción de cada fuente y su posible aporte a la construcción del modelo de manejo de incidentes de ciberseguridad. Esta etapa fue clave para filtrar de manera eficiente el material que serviría como base para las fases siguientes del trabajo.

### 4.1.2 Documentos relevantes seleccionados

**Tabla 9.** Puntuación de los documentos encontrados

| Documento, Estándar, Recurso Consultado | Accesibilidad | Nivel de Detalle | Calidad de la Fuente | Actualidad | Total |
|---|---|---|---|---|---|
| Prerequisites for Building a Computer Security Incident Response Capability [36] | 3 | 3 | 4 | 3 | 13 |
| A step-by-step approach on how to set up a CSIRT [37] | 5 | 5 | 5 | 4 | 19 |
| Expectations for Computer Security Incident Response [22] | 5 | 3 | 5 | 3 | 16 |
| Buenas Prácticas para Establecer un CSIRT Nacional [38] | 5 | 5 | 3 | 5 | 18 |
| Guía Práctica para CSIRTs [39] | 5 | 4 | 3 | 5 | 17 |

| | | | | | |
|---|---|---|---|---|---|
| Computer Security Incident Response Team (CSIRT): How to Build One [40] | 5 | 2 | 2 | 5 | 14 |
| Cybersecurity Best Practices [41] | 3 | 3 | 5 | 5 | 16 |
| Incident Response Recommendations and Considerations for Cybersecurity Risk Management [42] | 5 | 5 | 5 | 5 | 20 |
| Good Practice Guide for Incident Management [43] | 5 | 5 | 5 | 5 | 20 |
| Organizational Models for Computer Security Incident Response Teams (CSIRTs) [44] | 5 | 5 | 5 | 5 | 20 |
| Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0 [45] | 5 | 3 | 5 | 5 | 18 |
| Curso básico para la creación y gestión de un CSIRT [46] | 2 | 1 | 5 | 5 | 13 |
| Manual Básico de Gestión de Incidentes de Seguridad Informática [47] | 5 | 5 | 5 | 5 | 20 |
| Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales [48] | 5 | 4 | 3 | 5 | 17 |
| How to create a CSIRT: 10 best practices [49] | 5 | 2 | 2 | 5 | 14 |
| Handbook for Computer Security Incident Response Teams (CSIRTs) [50] | 5 | 5 | 5 | 4 | 19 |

| | | | | | |
|---|---|---|---|---|---|
| Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información [51] | 5 | 4 | 3 | 5 | 17 |
| Guía 21 - Gestión de Incidentes [52] | 5 | 5 | 3 | 5 | 18 |
| ISO/IEC 27035-1:2023 Information technology - Information security incident management [53] | 1 | 4 | 5 | 5 | 15 |
| ColCERT [54] | 5 | 2 | 3 | 5 | 15 |

Nota. Matriz de puntuación de los documentos encontrados basada en los criterios definidos.

En la Tabla 9 se presenta la puntuación asignada a cada uno de los materiales analizados, con base en los criterios definidos previamente. A cada documento se le asignó una calificación del 1 al 5 por cada criterio. La suma final de estos puntajes se registró en la columna Total, sirviendo como indicador principal para determinar la relevancia del material dentro del marco de la tesis. Esta puntuación permitió establecer un umbral mínimo para la selección de los documentos más completos y útiles, que fueron utilizados como referencia en las fases posteriores del proyecto.

### 4.1.3 Caracterización de los documentos seleccionados

Después de completar el proceso de clasificación y selección de materiales, se identificaron seis documentos que fueron considerados los más relevantes y útiles para el desarrollo de esta tesis, no solo porque obtuvieron las puntuaciones más altas en la actividad previa, sino también porque ofrecen aportes significativos, ya sea en la estructuración de un CSIRT o en la gestión de incidentes de ciberseguridad. En la Tabla 10 se presentan los documentos seleccionados junto con sus características respectivas de origen, etapa del proceso y categoría.

**Tabla 10.** Caracterización de documentos seleccionados

| Documento. Estándar o Recurso Consultado | Origen | Etapa del Proceso | Categoría |
|---|---|---|---|

| | | | |
|---|---|---|---|
| A step-by-step approach on how to set up a CSIRT [37] | Internacional | Creación del CSIRT | Procedimientos |
| Incident Response Recommendations and Considerations for Cybersecurity Risk Management [42] | Internacional | Gestión de Incidentes | Políticas, procedimientos, recursos |
| Good Practice Guide for Incident Management [43] | Internacional | Gestión de Incidentes | Políticas, procedimientos |
| Organizational Models for Computer Security Incident Response Teams (CSIRTs) [44] | Internacional | Creación del CSIRT | Procedimientos |
| Manual Básico de Gestión de Incidentes de Seguridad Informática [47] | Internacional | Gestión de incidentes | Políticas, procedimientos |
| Handbook for Computer Security Incident Response Teams (CSIRTs) [50] | Internacional | Creación del CSIRT | Procedimientos |

Nota. Matriz de caracterización de los documentos que conforman la base de conocimientos.

A continuación, se resumen las mejores prácticas recomendadas agrupadas según la etapa del proceso en la que se aplicarán:

**Resumen de buenas prácticas recomendadas para el manejo de incidentes de ciberseguridad:**

**Documento consultado:** A step-by-step approach on how to set up a CSIRT [37].

**Buenas prácticas recomendadas:**

Este documento propone la respuesta a incidentes a través de la conformación de un CSIRT. A continuación, se presentan las ideas principales:

**Servicios que ofrece un CSIRT:** definir los servicios que el equipo debe prestar es importante. Para ello se debe tener en cuenta los recursos económicos y las habilidades y conocimientos del personal de equipo. Un CSIRT debe prestar como mínimo los siguientes servicios:

- Alertas y avisos.
- Gestión de incidentes.
- Anuncios.

**Definición del modelo financiero:** aunque los fondos que se invertirán en el CSIRT deberían estar definidos por las necesidades del grupo de atención, lo cierto es que el presupuesto se debe adaptar a los servicios que se prestarán. Por otro lado, los costos del

modelo están determinados por las horas de servicio que se prestarán (determinadas principalmente por los horarios de operaciones de la organización) y la cantidad y calidad de personas que se emplearán.

**Definición de la estructura organizacional:** la estructura organizacional de CSIRT depende de 2 factores. El primero es la estructura de la organización anfitriona y su grupo de atención. El segundo factor es el personal experto con el que se cuente.

**Tipos de modelos de CSIRT:**

- Modelo de negocio independiente: el equipo funciona como una organización independiente, con su propia administración y empleados.
- Modelo integrado: el equipo usa recursos (personal y técnico) de la organización anfitriona. El líder del equipo puede solicitar apoyo de los especialistas internos.
- Modelo de campo: suelen ser CSIRT académicos ubicados en varias sedes, pero bajo la coordinación de un CSIRT principal.
- Modelo voluntario: es el creado por un grupo de especialistas que se reúnen voluntariamente para apoyarse entre sí.

**Documento consultado:** Organizational Models for Computer Security Incident Response Teams (CSIRTs) [44].

**Buenas prácticas recomendadas:**

**Definición del grupo de atención o público objetivo:** identificar el grupo de atención es decisivo para determinar el modelo organizacional del centro de respuesta. El grupo de atención puede ser interno o externo, lo que significa que el CSIRT está en la misma organización o fuera de ella, respectivamente. Puede ser centralizado, es decir, que está ubicado geográficamente en un área cercana o en el mismo edificio; o distribuido, lo cual quiere decir que el grupo de atención está ubicado en diferentes lugares, ciudades o países.

**Definición de la misión:** este es un factor que también influye en el modelo organizacional que se debe seleccionar.

**Definición de los servicios:** este documento clasifica los servicios en tres categorías:

- Servicios reactivos: son aquellos que se desencadenas cuando se genera un evento. Estos hacen parte de las actividades principales del CSIRT.

- Servicios proactivos: son aquellos que dan asistencia e informan al grupo de atención para protegerlo antes de que un ataque suceda.
- Servicios de gestión de calidad de seguridad: son servicios adicionales y diferentes a los de gestión de incidentes que buscan mejorar la postura de seguridad de la organización reduciendo el número de incidentes.

**Modelos organizacionales:** los modelos organizacionales comunes son:

- **Equipo de seguridad:** no es un CSIRT propiamente dicho. Está compuesto por personal de TI que gestiona los incidentes de seguridad. Los servicios que proporciona este equipo son limitados.
- **CSIRT distribuido interno:** constituido por personal que está distribuido en otras áreas de la organización y que además de realizar sus labores diarias, también deben realizar las tareas de gestión de incidentes. Estas personas son seleccionadas por sus conocimientos en tecnología.
- **CSIRT centralizado interno:** compuesto por personal dedicado completamente a prestar los servicios de gestión de incidentes. El gerente del CSIRT le reporta a la alta gerencia.
- **CSIRT interno combinado centralizado y distribuido:** este modelo optimiza el uso del personal ubicado en diferentes partes de la organización, centralizando la coordinación del equipo para ofrecer una visión más completa de las amenazas y riesgos de seguridad.
- **Coordinación de CSIRT:** el CSIRT coordina y gestiona los incidentes en varias organizaciones internas o externas o en otros CSIRT. Su grupo de atención es más amplio y tiene un mayor alcance.

**Documento consultado:** Manual Básico de Gestión de Incidentes de Seguridad Informática [47].

**Buenas prácticas recomendadas:**

Directrices y acciones para la creación de un CSIRT

- Presupuesto: se debe ajustar a las necesidades del grupo de atención. Comúnmente se calcula para un año y se deben tener en cuenta los costos de inversión inicial relacionados a la infraestructura tecnológica y física y los costos de funcionamiento que incluyen la contratación, salarios y capacitación del personal.

- Servicios: dentro de los tipos de servicios que se pueden ofrecer están los reactivos, proactivos o de investigación. Cada CSIRT define los servicios en base a su alcance y a sus recursos tecnológicos y humanos. Algunos servicios se pueden ofrecer de manera compartida con otras áreas de la organización o tercerizada a través de proveedores. Una buena práctica es que cuando el CSIRT está recién formado se enfoque en principalmente en la respuesta a incidentes y aquellos servicios que sean necesarios.
- Recomendaciones para la inserción de CSIRT a la organización: la estructura organizacional del CSIRT debe ser acorde a los servicios que presta y a la estructura de la organización anfitriona. Los puntos clave para establecer un CSIRT son:
    - Crear la misión y visión.
    - Definir el segmento que se atenderá (comunidad objetivo).
    - Establecer los canales de comunicación.
    - Seleccionar un modelo organizacional y los servicios.
    - Estructura dentro de la Organización: políticas, procesos y procedimientos.
- Modelos organizacionales: para definir el modelo organizacional se deben tener en cuenta los siguientes factores:
    - Misión del centro de respuesta.
    - Servicios que prestará.
    - Posición del CSIRT en la estructura organizacional.
    - Financiamiento de las operaciones.
    - Alcance.
- Categorías de modelos:
    - Equipo de seguridad: el equipo no se dedica exclusivamente a las labores de respuesta a incidentes y por eso se dificulta la realización de algunas actividades.
    - Equipo centralizado: las actividades las realiza un único equipo. Es el modelo recomendado para pequeñas organizaciones o empresas con una única sede.

    - Equipo distribuido: son varios equipos que se crean para atender incidentes específicos, por ubicación o de acuerdo con la estructura organizacional y juntos conforman el centro de respuesta.
    - Equipo coordinador: es aquel que da soporte y coordina a equipos de otras organizaciones.
- Personal: no es obligatorio que los miembros del equipo sean expertos, pero sí se recomienda que tengas habilidades para dar apoyo durante un incidente. Se debe tener un plan de entrenamiento y recursos de consulta para mejorar estas habilidades.
- Funciones internas del centro de respuesta: sin importar el modelo organizacional que se establezca, existen funciones que se deben cumplir por los miembros del equipo, como, por ejemplo, director, gestión de incidentes, legal, entre otras.
- Políticas para la gestión de riesgos: las políticas hacen parte del marco normativo y define los lineamientos que se debe seguir para la gestión de riesgos en la organización.

**Resumen de buenas prácticas para la gestión de incidentes:**

**Documento consultado:** Incident Response Recommendations and Considerations for Cybersecurity Risk Management [42].

**Buenas prácticas recomendadas:**

Este documento propone un modelo de atención de incidentes de ciberseguridad como parte fundamental de la gestión de riesgos, que se compone de seis funciones que permiten tratar de manera efectiva dichos incidentes. En él, las funciones de Gobernar, Identificar y Proteger están más relacionadas con la gestión de riesgos, y se complementan con las funciones de Detectar, Responder y Recuperar, que tienen más que ver con la gestión de incidentes como tal.

El documento también sugiere una lista de roles y responsabilidades que se deberían incluir en el modelo de atención de incidentes que adopte la organización y los elementos más relevantes que se deben contemplar en la política de gestión de incidentes. Adicionalmente, recomienda procesos y procedimientos e indica que se deben basar en la política y el plan de respuesta a incidentes.

**Documento consultado:** Good Practice Guide for Incident Management [43].

**Buenas prácticas recomendadas:**

El modelo de gestión de incidentes de ENISA propone 6 fases principales que son reporte, registro, triaje, solución, cierre y post-análisis. También indica que estas fases se pueden expandir y detallar según los requerimientos de la organización. A continuación, se describen cada una de ellas:

- Reporte del incidente: en esta etapa se pueden usar diversos medios para recibir la notificación del incidente.
- Registro: se refiere al sistema de gestión de tickets donde se deben registrar los incidentes notificados. Debe tener una nomenclatura definida para su fácil identificación.
- Triaje: en esta etapa se debe priorizar las acciones en base a la gravedad del incidente. Esta etapa se compone de tres sub-etapas que son:
    - verificación, donde se hace una revisión de los reportes para identificar si en realidad es un incidente o no, o si es un reporte proveniente del grupo de atención bajo su responsabilidad.
    - Clasificación inicial, basado en un esquema de clasificación definido previamente. Para realizar esta primera clasificación se debe recolectar la mayor cantidad de información posible.
    - Asignación del incidente, que consiste en delegar la responsabilidad de la gestión del incidente a una persona en específico.
- Solución del incidente: esta es la etapa más dispendiosa del proceso de gestión de incidentes. Como se aprecia en la Figura 5, está definida por un ciclo básico compuesto por análisis de datos, investigación de resolución, acción propuesta, acción realizada, y erradicación y recuperación.

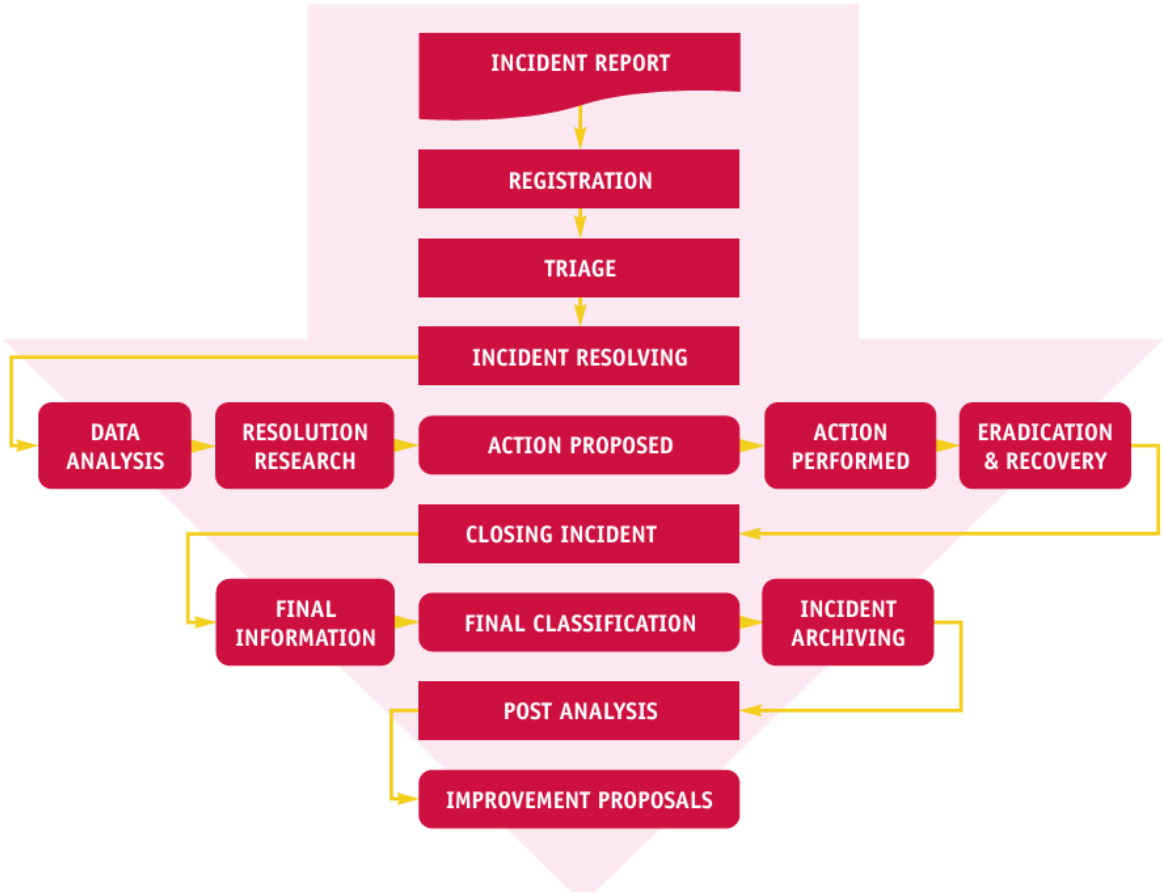
**Figura 5.** Proceso de gestión de incidentes


Nota. Actividades recomendadas para la etapa de gestión de incidentes. Fuente: tomado de [41].

- Cierre del incidente: después de remediar el incidente se debe realizar el cierre del caso informando a las partes interesadas lo ocurrido. Este informe debe ser ajustado a quien vaya dirigido. Además, se procede a archivar el caso teniendo en cuenta que la información relacionada al incidente es sensible y por tal motivo se debe asegurar correctamente.
- Post-Análisis: esta etapa se refiere la sesión que se debe tener después del cierre del incidente para recoger las lecciones aprendidas.

En la Figura 6 se presenta el diagrama de flujo del modelo propuesto por ENISA para la atención de incidentes:

**Figura 6.** Flujograma de proceso de gestión de incidentes




Nota. Flujo de trabajo de gestión de incidentes ENISA. Fuente: tomado de [41].

**Documento consultado:** Handbook for Computer Security Incident Response Teams (CSIRTs) [50].

**Buenas prácticas recomendadas:**

Los objetivos establecidos para el servicio y la disponibilidad de recursos del CSIRT son factores que limitan el servicio ofrecido. Con un entendimiento de estas limitaciones se puede definir el nivel de gestión de incidentes que se puede entregar.

Este documento describe 4 actividades esenciales que debe realizar un CSIRT durante la gestión de incidentes de seguridad:

- Triaje: esta actividad actúa como un punto central para gestionar la información entrante y saliente del servicio. Permite aceptar, clasificar y transmitir datos, adaptándose a las necesidades del equipo. Cada nuevo evento recibe una prioridad inicial y, a veces, un número de seguimiento. Además, se pueden realizar acciones

adicionales, como archivado o traducción, para facilitar la gestión de incidentes posteriores.

- Manejo del incidente: proporciona apoyo y orientación en cuanto a los incidentes sospechosos o confirmados. Incluye diversas actividades, como la revisión de informes para determinar lo sucedido. Esto puede implicar analizar evidencia, como archivos de registro, para identificar a las personas implicadas y la asistencia requerida. El equipo debe definir las respuestas adecuadas y notificar o hacer seguimiento al caso.
- Anuncios: crean información adaptada a la situación en varios formatos, revelando detalles sobre amenazas actuales y medidas de protección. También proporciona información sobre la naturaleza y el alcance de ataques recientes. En un CSIRT que ofrece más servicios, la publicación de anuncios puede considerarse un servicio independiente que brinda información adicional de análisis de vulnerabilidades y otros aspectos.
- Retroalimentación: ofrece soporte para proporcionar comentarios sobre temas no directamente relacionados con incidentes específicos. Estos comentarios pueden ser solicitados por los medios de comunicación y pueden presentarse de manera periódica, como en informes anuales, o de forma proactiva. Esta función también incluye un conjunto básico de respuestas a preguntas frecuentes y actúa como una interfaz para solicitudes de medios o aportes al equipo.

**Tabla 11.** Resumen de buenas prácticas caracterizadas

| Documento/Estándar/ Recurso Consultado | Etapa del Proceso | Buenas Prácticas |
|---|---|---|
| A step-by-step approach on how to set up a CSIRT [37] | Conformación de CSIRT | Actividades recomendadas para la creación de un CSIRT:<br>- Definir los servicios que se prestarán: reactivos, proactivos, adicionales.<br>- Definir el presupuesto y los costos del modelo.<br>- Definir la estructura organizacional, incluyendo los roles y responsabilidades.<br>- Definir el modelo que se adoptará. |
| Organizational Models for Computer Security Incident Response Teams (CSIRTs) [44] | Conformación de CSIRT | Pasos para la creación de un CSIRT:<br>- Identificar si el grupo de atención es interno o externo, centralizado o distribuido.<br>- Establecer la misión del CSIRT.<br>- Definir los servicios: reactivos, proactivos y de gestión de la calidad de |

| | | |
|---|---|---|
| | | seguridad.<br>- Seleccionar el modelo organizacional: distribuido interno, centralizado interno, interno combinado o de coordinación. |
| Manual Básico de Gestión de Incidentes de Seguridad Informática [47] | Conformación de CSIRT | Directrices para la creación de un CSIRT:<br>- Ajustar el presupuesto a las necesidades del grupo de atención.<br>- Definir los servicios con base al alcance, los recursos tecnológicos y humanos.<br>- Establecer la estructura organizacional acorde a los servicios y a la estructura de la organización anfitriona.<br>- Definir el modelo teniendo en cuenta la misión, los servicios, la estructura, el financiamiento y el alcance.<br>- Seleccionar el personal de acuerdo con sus habilidades, el presupuesto y la disponibilidad del equipo.<br>- Establecer las funciones que desempeñarán los miembros del equipo.<br>- Las políticas deben ser ajustadas al marco normativo del país al que pertenece el CSIRT y a los propósitos de la organización. |
| Incident Response Recommendations and Considerations for Cybersecurity Risk Management [42] | Gestión de Incidentes | Funciones para la gestión de riesgos y atención de incidentes de seguridad informática:<br>- Gobierno: función estratégica y transversal a las demás funciones. Establece lo que se debe hacer para lograr los resultados esperados.<br>- Identificar: permite conocer los activos de la organización y sus riesgos para priorizar recursos.<br>- Proteger: gestiona los riesgos identificados en los activos.<br>- Detectar: identifica actividades anómalas o incidentes en curso.<br>- Responder: se ejecutan las acciones necesarias para contener los incidentes detectados.<br>- Recuperar: se restauran los servicios y activos afectados por un incidente. |
| Good Practice Guide for Incident Management [43] | Gestión de Incidentes | Fases para la gestión de incidentes:<br>- Reporte del incidente a través de diferentes medios de notificación.<br>- Registro de los incidentes en un sistema de gestión de tickets.<br>- Triaje para priorizar las acciones con base en la gravedad del incidente.<br>- Solución del incidente según la |

| | | |
|---|---|---|
| | | definición del ciclo básico: análisis, investigación, acción propuesta, acción realizada, erradicación y recuperación.<br>- Cierre del incidente informando a las partes interesadas lo ocurrido y archivando el caso.<br>- Post-análisis para recoger las lecciones aprendidas. |
| Handbook for Computer Security Incident Response Teams (CSIRTs) [50] | Gestión de Incidentes | Actividades esenciales que un CSIRT debe realizar durante un incidente:<br>- Triaje: permite aceptar, clasificar y transmitir datos adaptándose a las necesidades del equipo.<br>- Manejo del incidente: proporciona apoyo y orientación relacionada a los incidentes sospechosos o confirmados.<br>- Anuncios: crean información adaptada a la situación sobre amenazas actuales y medidas de protección.<br>- Retroalimentación: proporciona comentarios sobre temas no directamente relacionados con incidentes de seguridad. |

Nota. En este formato se consolidan las buenas prácticas encontradas.

En la Tabla 11 se consolidó el resumen de las buenas prácticas caracterizadas de los documentos seleccionados en la fase previa. En ella se presentan en forma organizada por etapa del proceso, las características más relevantes de cada uno de los materiales para el desarrollo de este trabajo.

## 4.2 Establecimiento del modelo para el manejo de incidentes de ciberseguridad para ONG

A continuación, se presentan los resultados correspondientes a la actividad de establecimiento del modelo para el manejo de incidentes de ciberseguridad en una ONG. En esta actividad se buscó desarrollar un esquema que permitiera guiar de manera estructurada y eficiente la gestión de incidentes, abarcando todas las etapas del proceso, desde la planeación hasta las acciones posteriores al cierre del caso. El modelo propuesto integra buenas prácticas internacionales permite fortalecer la capacidad de respuesta de las ONG frente a amenazas de seguridad informática.

### 4.2.1 Diseño de modelo para manejo de incidentes en una ONG.

El modelo de atención de incidentes de ciberseguridad propuesto se compone de cinco etapas que sirven como guía para que los responsables del proceso actúen de manera organizada y metódica ante los eventos de seguridad informática. Estas etapas están enmarcadas de manera general por la función de Gobierno que define las tareas estratégicas que se deben realizar para que se cumplan los resultados esperados en cada etapa. La Figura 7 representa gráficamente las etapas del modelo.

**Figura 7.** Modelo para el manejo de incidentes de ciberseguridad


Nota. Etapas del modelo de manejo de incidentes de ciberseguridad propuesto.

A continuación, se describen cada una de las etapas:

1. **Preparación y prevención:** en esta etapa se establecen previamente los recursos necesarios para la gestión de incidentes:
   - Protocolos de atención: se deben establecer guías estructuradas de los procedimientos que se deben realizar durante un incidente de ciberseguridad.
   - Recursos de comunicación: listado de números telefónicos y correos electrónicos, no solo de los integrantes del equipo de respuesta a incidentes de la organización, sino también, de otros equipos de respuesta externos, proveedores de servicios, la policía, organismos de control y otros contactos que puedan ser útiles durante un suceso de ciberseguridad.
   - Portátiles: exclusivos para las actividades de gestión de incidentes.

- Documentación: adicional a la definición de políticas, roles y responsabilidades, se debe contar con documentación técnica que pueda ser usada cuando ocurra un evento (manuales de dispositivos, documentación de proveedores de servicios) y con playbooks que establezcan los procesos que se deben realizar cuando se presentan incidentes.
- Simulaciones y entrenamiento: programar simulaciones de ataques periódicas y entrenamientos, tango para el personal técnico como para los usuarios finales.
- Antivirus: los equipos de todos los usuarios deben contar con un antivirus debidamente licenciado.

2. **Reporte y registro:** los eventos son informados a través de sistemas para reportar incidentes (números de teléfono, correos, formularios). Una vez recibido el reporte, se registran en un sistema de tickets que permita llevar una trazabilidad de cada caso. El registro se hace usando una nomenclatura que facilita la búsqueda y gestión de los casos.
3. **Análisis y clasificación:** en esta etapa se determina si un evento reportado es un incidente o un falso positivo. Esto permitirá responder de manera rápida y, por consiguiente, disminuirá el impacto generado. En caso de ser un incidente, se priorizan las acciones que se llevarán a cabo dependiendo de su gravedad, usando la matriz de clasificación que se muestra en la Tabla 12.

**Tabla 12.** Matriz de clasificación de incidentes de seguridad

| Gravedad | Descripción | Acción Requerida |
|---|---|---|
| **Crítico** | Incidentes que afectan significativamente la operación de la ONG y comprometen datos sensibles o confidenciales. | Respuesta inmediata y prioritaria. |
| **Alto** | Incidentes que afectan la operación, pero no son críticos. | Respuesta rápida y oportuna. |
| **Medio** | Incidentes que tienen un impacto moderado en la operación y pueden haber comprometido datos, pero no sensibles ni confidenciales. | Respuesta en un plazo razonable. |
| **Bajo** | Incidentes menores que no afectan la operación ni comprometen datos. | Monitoreo y respuesta según disponibilidad. |

Nota. Matriz sugerida para la clasificación de incidentes según su gravedad.

4. **Respuesta:** en esta etapa se realizan los procesos previamente definidos durante la fase de preparación para detener el incidente y poner de nuevo en marcha los sistemas afectados. Además de las tareas definidas con anterioridad, se tiene como recurso adicional la siguiente matriz de incidentes de ciberseguridad que se muestra en la Tabla 13. Esta matriz proporciona una estrategia de contención para casos particulares de ataques.

**Tabla 13.** Matriz de incidentes de seguridad informática

| Tipo de Incidente | Ejemplos | Estrategias de contención |
|---|---|---|
| Malware | Virus, ransomware, spyware. | • Aislamiento del sistema<br>• Escaneo y eliminación<br>• Restauración de copias de seguridad<br>• Actualización de software |
| Phishing | Correos electrónicos fraudulentos, sitios web falsos. | • Cambio de contraseñas de cuentas comprometidas<br>• Activación de MFA<br>• Educación del personal<br>• Monitoreo de cuentas afectadas |
| Ataques de Red | DDoS, sniffing, spoofing. | • Cierre de puertos vulnerables<br>• Bloqueo de IPs sospechosas<br>• Habilitar firewalls e IPS<br>• Aislar segmentos de red<br>• Análisis de tráfico |
| Acceso No Autorizado | Intrusiones, uso indebido de credenciales. | • Revocar credenciales comprometidas<br>• Aislar sistemas comprometidos<br>• Auditoría de registros |
| Pérdida de Datos | Fugas de datos, robo de dispositivos. | • Restauración de datos<br>• Mejora de políticas de acceso a los datos<br>• Notificación de incidentes |
| Vulnerabilidades | Explotación de vulnerabilidades conocidas. | • Aplicación de parches<br>• Realizar pruebas de seguridad<br>• Configurar reglas de seguridad |
| Amenazas que involucran IA | Modelos de IA corruptos | • Ver estrategias de mitigación en [55] |

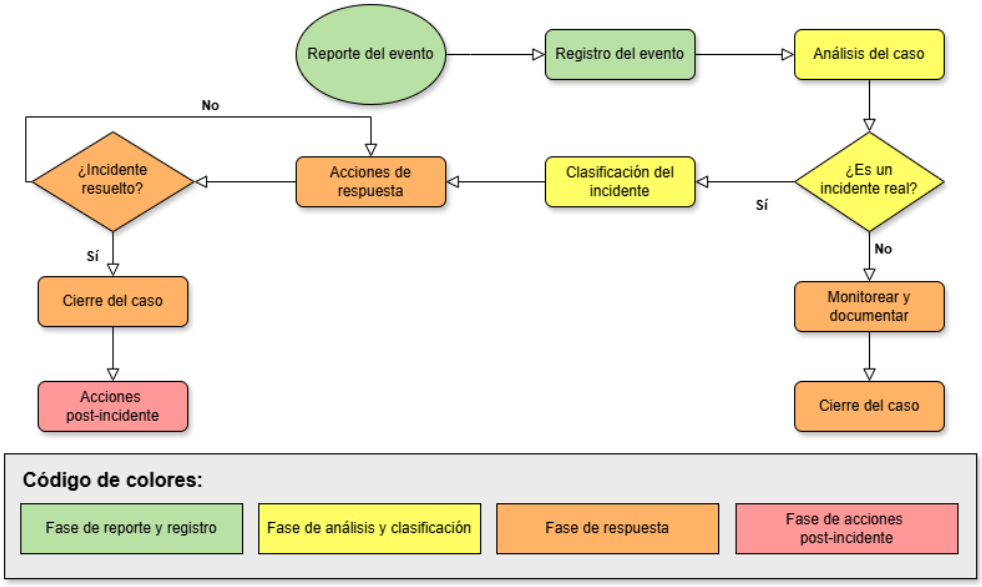
Nota. Estrategias recomendadas para la mitigación de incidentes particulares.

5. **Acciones Post-Incidente:** en esta fase final, después del cierre del caso, se debe programar una reunión con todos los involucrados en el proceso para analizar los hechos ocurridos y los procesos que se llevaron a cabo para determinar los aprendizajes y las posibles acciones de mejora.

### 4.2.2 Creación del flujograma del proceso de manejo de incidentes de ciberseguridad.

El diagrama que se presenta en la Figura 8 es una adaptación para una ONG basada en los modelos estudiados durante la caracterización de buenas prácticas. En este flujograma se representan de manera gráfica las acciones que se deben realizar durante el proceso de gestión de incidentes de seguridad informática.

**Figura 8.** Flujograma modelo de manejo de incidentes




Nota. Acciones que se deben realizar durante el proceso de gestión de incidentes de seguridad informática.

A continuación, se describen los roles y responsabilidades relacionados a casa una de las actividades del proceso de gestión de incidentes:

1. **Actividad:** reporte de eventos

- **Rol:** responsables de la gestión de incidentes o cualquier persona de la organización, clientes, usuarios externos u personal de otras entidades u organizaciones.
- **Responsabilidad:** reportar cualquier actividad sospechosa e incluir evidencia.

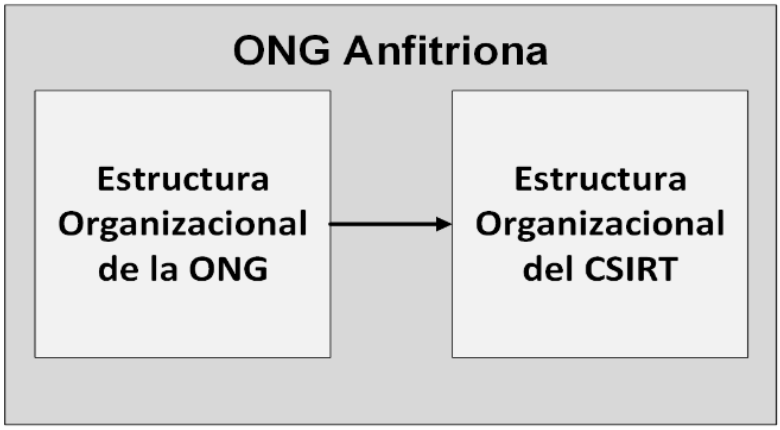
2. **Actividades:** registro del evento, análisis del caso, monitorear y registrar el caso, clasificar el incidente, realizar las acciones de respuesta, cierre del caso y acciones post-incidente

- **Rol:** integrantes del equipo encargado de la gestión de incidentes.
- **Responsabilidades:**
    - Recibir y registrar las alertas reportadas.
    - Evaluar la alerta para determinar su validez y gravedad.
    - Decidir si la alerta representa una amenaza real.
    - Documentar y archivar el caso si es un falso positivo.
    - Iniciar el proceso de atención si es un incidente de ciberseguridad.
    - Restaurar los sistemas afectados.
    - Concluir el proceso de atención del incidente.
    - Revisar el incidente y las acciones tomadas para identificar mejoras.

## 4.3 Desarrollo de un marco de operaciones para un CSIRT.

Con base en la caracterización de la documentación consultada, se determinó que el de modelo que mejor se ajusta a las necesidades propias de las ONG para la atención de incidentes de seguridad informática, es un modelo de CSIRT, cuyos recursos tecnológicos y humanos hacen parte de la organización anfitriona. El equipo propuesto está conformado por personal que comúnmente desempeña labores relacionadas a sus respectivos cargos en la compañía, pero que durante un incidente de ciberseguridad se enfoca en las tareas respectivas al CSIRT. La Figura 9 representa gráficamente la postura del CSIRT dentro de la ONG anfitriona.

**Figura 9.** Postura del CSIRT dentro de la ONG




Nota. Representación gráfica de la posición del CSIRT dentro de la organización anfitriona.

### 4.3.1 Diseño del modelo CSIRT para ONG.

En la Figura 10 se presenta de manera gráfica la estructura jerárquica del modelo CSIRT propuesto. Esta representación permite visualizar cómo se organizan los roles dentro del equipo, destacando los niveles de responsabilidad y la división de funciones entre los diferentes miembros.

**Figura 10.** Estructura organizacional del CSIRT


Nota. Representación gráfica de la estructura jerárquica del modelo CSIRT propuesto.

Esta estructura se organiza de la siguiente manera:

- **Líder del CSIRT:** es la persona responsable de la función de Gobierno, la gestión y coordinación general del equipo de respuesta a incidentes de ciberseguridad y de actuar como punto de contacto principal entre la ONG y los consultores externos.
- **Líder Técnico:** está subordinado al líder del CSIRT y es el encargado de dirigir al Equipo Técnico, el cual se encarga de las tareas técnicas operativas de respuesta a incidentes.
- **Consultor de Comunicaciones:** responsable de manejar la comunicación tanto interna como externa durante la gestión de incidentes. Esto incluye coordinar los mensajes que se envían a las partes interesadas y al público, en caso de ser necesario.
- **Consultor Legal:** proporciona asesoría en aspectos legales y de cumplimiento durante la respuesta a incidentes, asegurándose de que todas las acciones del CSIRT cumplan con las leyes y regulaciones aplicables.
- **Consultores Externos:** son recursos adicionales como proveedores de servicios u otros CSIRT que ayudan al equipo en situaciones donde se requiere experiencia específica o en incidentes de gran magnitud que requieren apoyo externo.

A continuación, se describen los perfiles y las competencias necesarias para cada cargo:

- **Líder del CSIRT**:

    a. **Perfil**: el líder del CSIRT es responsable de velar por la definición de políticas claras, la asignación de responsabilidades, la priorización de recursos, coordinar la respuesta a incidentes y supervisar el trabajo del equipo. Este rol puede ser desempeñado por una persona que ya ocupe un puesto de liderazgo en la organización, preferiblemente en áreas relacionadas con TI o gestión de proyectos.
    b. **Conocimientos y habilidades**:
        i. Conocimientos en gestión de proyectos.
        ii. Habilidad para la toma de decisiones bajo presión.
        iii. Conocimientos básicos en gestión de incidentes de seguridad informática.
        iv. Capacidades organizativas y de liderazgo.

v. Buenas habilidades de comunicación para coordinar esfuerzos entre diferentes áreas y asegurar que las actividades del CSIRT se alineen con los objetivos de la organización.

- **Líder Técnico**:

a. **Perfil**: encargado de la dirección técnica del equipo, la supervisión de las tareas de respuesta a incidentes y de promover el uso de estándares de ciberseguridad adecuados. Este rol puede ser asumido por un técnico de TI o un analista de sistemas con conocimientos en ciberseguridad o una persona amante de la tecnología y con habilidades de liderazgo y toma de decisiones.
b. **Conocimientos y habilidades**:
   i. Uso de herramientas digitales.
   ii. Conocimientos en sistemas operativos.
   iii. Capacidad para diagnosticar y resolver problemas técnicos.
   iv. Habilidad para orientar y proporcionar directrices en situaciones de crisis.

- **Equipo Técnico**:

a. **Perfil**: este equipo realiza las tareas operativas y técnicas necesarias para la contención y resolución de incidentes. Los miembros del Equipo Técnico pueden ser personal de TI que habitualmente desempeña funciones de soporte, administración de sistemas o personas que se les facilite el uso de la tecnología y que tengan conocimientos en seguridad informática.
b. **Conocimientos y habilidades**:
   i. Buenas prácticas en seguridad digital.
   ii. Conocimiento en redes y sistemas operativos.
   iii. Familiaridad con herramientas de análisis de ciberseguridad.
   iv. Capacidad de realizar investigaciones técnicas y análisis de registros.
   v. Habilidad para ejecutar procedimientos de manera rápida y efectiva.

- **Consultor de Comunicaciones**:

    a. **Perfil**: este rol es fundamental para definir la política y los protocolos de comunicación y para coordinar la comunicación interna y externa antes, durante y después de un incidente. Puede ser asumido por una persona del equipo de comunicaciones, relaciones públicas o cualquier miembro con habilidades de comunicación estratégica.
    b. **Conocimientos y habilidades**:
        i. Habilidades en redacción y comunicación, tanto escrita como verbal, para transmitir mensajes claros y coherentes.
        ii. Experiencia en relaciones públicas y manejo de crisis.
        iii. Capacidad para coordinarse con miembros del CSIRT, asegurando que la información compartida sea precisa y apropiada para cada audiencia.
        iv. Sensibilidad para manejar información confidencial y coordinar declaraciones con el Consultor Legal cuando sea necesario.

- **Consultor Legal**:

    a. **Perfil**: responsable de brindar asesoría legal durante el manejo de incidentes, asegurando el cumplimiento con las leyes y regulaciones aplicables. Este rol puede ser desempeñado por un abogado o un especialista en cumplimiento regulatorio de la organización.
    b. **Conocimientos y habilidades**:
        i. Conocimiento en leyes de protección de datos y regulaciones de ciberseguridad aplicables al sector.
        ii. Habilidad para evaluar las implicaciones legales de los incidentes de ciberseguridad y asesorar sobre las mejores prácticas para la documentación de incidentes y preservación de pruebas.
        iii. Capacidad para coordinarse con el Líder del CSIRT y el Consultor de Comunicaciones para asegurar que las acciones del equipo cumplan con los requisitos legales.

iv. Habilidades para desarrollar y recomendar políticas de respuesta a incidentes que minimicen riesgos legales y financieros para la organización.

- **Consultores externos:**

a. **Perfil:** es el personal de soporte técnico de los proveedores de productos y servicios como Microsoft o Google, integrantes de otros CSIRT o voluntarios de otras organizaciones. Su función es brindar apoyo durante un incidente dando asesoría técnica y recomendaciones y buscando soluciones para minimizar el impacto. Además, pueden colaborar en la investigación del caso y la recuperación de sistemas afectados.

### 4.3.2 Servicios prestados por el CSIRT

Aunque en la documentación se mencionan una gran cantidad de servicios que un CSIRT puede prestar, se recomienda que, para un equipo que apenas inicia sus actividades, comience con un conjunto pequeño pero lograble. Es por eso que se priorizaron aquellas funciones que generan mayor valor y son realizables con los recursos disponibles. De esta manera, el equipo podrá enfocarse en desarrollar capacidades sólidas en áreas clave. Con el tiempo, y a medida que se consolide su operación, podrá expandir su alcance e incorporar nuevas responsabilidades. La Figura 11 representa gráficamente las tareas iniciales asumidas por el CSIRT.

**Figura 11.** Servicios prestados por el CSIRT


Nota. Servicios que prestará el CSIRT al iniciar la operación.

Inicialmente el CSIRT prestará los siguientes servicios:

- **Servicios Proactivos**:
  Anuncios sobre amenazas: informar regularmente sobre amenazas actuales que puedan afectar a la organización, sus miembros, colaboradores y beneficiarios.
- **Servicios Reactivos:**
  Respuesta a incidentes de ciberseguridad.
- **Servicios complementarios:**
  Eventos o actividades enfocadas a concientizar al grupo de atención sobre temas relacionados a ciberseguridad.

### 4.3.3 Definición de protocolos de actuación.

A continuación, se presentan los protocolos de actuación definidos:

**Protocolo de registro y clasificación:**

- **Introducción:** el reporte de eventos de seguridad permite no solo alertar al equipo de atención sobre un posible ataque, sino también recolectar la mayor cantidad información que ayude determinar su origen y las acciones necesarias para contenerlo. En este apartado se describen los procedimientos mínimos requeridos para reportar y clasificar este tipo de eventos.

- **Objetivo:** asegurar que los eventos de seguridad informática sean registrados y clasificados correctamente para una atención rápida y efectiva.

- **Procedimiento:**
    - **Recepción del caso:** recibir el reporte de los eventos realizados a través de los medios establecidos para el envío de información: formulario, correo electrónico, celular.
    - **Registro del caso:** registrar el evento en el sistema de tickets usando una nomenclatura que facilite la búsqueda y gestión, por ejemplo, esquema de numeración y etiquetas fáciles de identificar para las personas. Información requerida: hora, nombre de quien reporta, descripción del suceso, recurso comprometido, soportes (capturas de pantalla, mensajes de error), información que permita clasificar de manera rápida y precisa el evento.
    - **Pre-Análisis del evento:** hacer un estudio rápido para establecer si la información recolectada es suficiente para determinar si el evento es un incidente o no.
    - **Búsqueda de información adicional:** validar si hay otros usuarios o sistemas afectados, buscar registros asociados al evento y si es necesario, contactar a la persona que realizó el reporte para obtener más información.
    - **Clasificación del evento:** realizar la clasificación basada en la matriz de clasificación y en el análisis de la información recolectada.
    - **Activación el protocolo de atención:** iniciar el proceso de atención de incidente.

**Tabla 14.** Historial de revisiones del protocolo de registro y clasificación

| **Historial de revisiones** | | | | |
|---|---|---|---|---|
| **Documento:** | Protocolo de registro y clasificación | | **Fecha de creación** | 25/03/2025 |
| **Razón de la revisión** | **# de revisión** | **Revisado por** | **Aprobado por** | **Fecha de revisión** |
| Creación del documento | 1.0 | Dago Ramírez | | 25/03/2025 |

**Protocolo de atención:**

- **Introducción:** en este protocolo se define el proceso de atención de manera que la respuesta a los incidentes de seguridad se realice de manera estructurada y coordinada desde su identificación hasta su resolución.

- **Objetivo:** establecer un marco de operación que permita responder de manera rápida y efectiva a los incidentes de ciberseguridad.

- **Procedimiento:**
    - **Identificación de los recursos afectados:** hacer un listado de los usuarios, cuentas, aplicaciones, dispositivos y demás recursos comprometidos**.**
    - **Coordinación de la respuesta:** convocar al equipo de atención de incidentes, movilizar los recursos necesarios y contactar a los proveedores de servicios, autoridades u otros CSIRT si es necesario su apoyo**.**
    - **Medidas de contención:** usar los playbooks predefinidos para cada tipo de incidente y llevar a cabo las actividades requeridas para detenerlo. En caso de no existir un playbook para el caso, se debe recurrir a la documentación del fabricante o solicitar apoyo del proveedor del servicio o de consultores externos**.**
    - **Documentación del caso:** recolectar debidamente la información y evidencias requeridas para llevar un registro de la gestión del incidente, para la creación de informes o para usarlas en instancias legales.
    - **Revisión/ejecución de procedimientos legales o normativos:** analizar las repercusiones legales y tomar las medidas necesarias.
    - **Comunicación:** mantener una comunicación clara y efectiva basada en el protocolo de comunicación y durante todo el proceso de gestión del incidente.
    - **Escalamiento:** seguir el protocolo de escalamiento para elevar el incidente al nivel que la situación lo requiera.
    - **Cierre del caso:** verificar que el incidente ha sido resuelto, restaurar los servicios y notificar al grupo de atención.
    - **Seguimiento:** llevar a cabo las acciones post-incidentes y realizar las acciones de mejora necesarias**.**

**Tabla 15.** Historial de revisiones del protocolo de atención

| Historial de revisiones | | | | |
|---|---|---|---|---|
| **Documento:** | Protocolo de atención | | **Fecha de creación** | 25/03/2025 |
| **Razón de la revisión** | **# de revisión** | **Revisado por** | **Aprobado por** | **Fecha de revisión** |
| Creación del documento | 1.0 | Dago Ramírez | | 25/03/2025 |

**Protocolo de comunicación:**

- **Introducción:** la comunicación durante todas las etapas de gestión de un incidente es fundamental para facilitar la toma de decisiones y para mantener informadas a todas las partes interesadas.

- **Objetivo:** definir los procedimientos y canales que permitan tener una comunicación interna y externa efectiva durante un incidente de seguridad informática.

- **Principios:**
    - **Claridad:** usar un leguaje preciso, acorde al público y evitando tecnicismos innecesarios.
    - **Confidencialidad:** compartir la información estrictamente necesaria dependiendo de a quién se dirija el comunicado.
    - **Oportuna:** informar en el momento adecuado.
    - **Veracidad:** compartir información real y validada.

- **Canales de comunicación:**
    - **Internos:**
        - Correo electrónico
        - Formularios
        - Teléfono
        - Chats corporativos (Microsoft Teams, Slack, Google Meets)
        - Reuniones virtuales o presenciales
        - Intranet
    - **Externos:**

- Página web
- Correo electrónico
- Redes sociales o blogs
- Prensa, radio o televisión
- Reportes en plataformas oficiales de las autoridades competentes o los entes regulatorios.

- **Procedimiento según la fase del incidente:**
  - **Reporte y registro:** el usuario del grupo de atención o tercero notifica la detección de actividad sospechosa usando el canal oficial establecido.
  - **Análisis y clasificación:** alertar al equipo de respuesta con detalles iniciales del evento.
  - **Respuesta y contención:** informar sobre las acciones y medidas de control tomadas, emitir comunicados oficiales a los usuarios internos y público en general, si es el caso, sobre el estado y la afectación del incidente. Reportar a las autoridades y entes regulatorios en caso de ser necesario. Informar a los socios y proveedores sobre el impacto en los servicios y las operaciones. Reportar a la alta dirección sobre la evolución, estado y decisiones tomadas.
  - **Cierre y actividades post-incidente:** informar a la comunidad objetivo y si aplica, al público en general, sobre la resolución del incidente y las medidas implementadas, presentar un reporte final, notificar a los socios y proveedores sobre el restablecimiento de los servicios. Documentar las lecciones aprendidas y las acciones de mejora.

**Tabla 16.** Historial de revisiones del protocolo de comunicación

| **Historial de revisiones** | | | | |
|---|---|---|---|---|
| **Documento:** | Protocolo de comunicación | | **Fecha de creación** | 26/03/2025 |
| **Razón de la revisión** | **# de revisión** | **Revisado por** | **Aprobado por** | **Fecha de revisión** |
| Creación del documento | 1.0 | Dago Ramírez | | 26/03/2025 |

**Protocolo de escalamiento**

- **Introducción:** el protocolo de escalamiento permite que los incidentes se atiendan de manera adecuada, estableciendo niveles de elevación basados en su criticidad.

- **Objetivo:** definir los criterios de escalonamiento que permitan una gestión ordenada de los incidentes de ciberseguridad.

- **Niveles de escalamiento:**
    - **Nivel 1:** incidentes de gravedad baja y que pueden resolverse tan pronto se hace el reporte o según disponibilidad de personal. En este caso el incidente se resuelve con la experiencia y los conocimientos del equipo técnico, sin tener que consultar fuentes de información. Una vez resuelto el evento, se registra y se le hace seguimiento para verificar que todo quede funcionando con normalidad.
    - **Nivel 2:** incidentes de gravedad media y que requieren un tratamiento más específico, pero, sin necesidad solicitar apoyo de entes externos. Para resolver la situación, el líder técnico debe coordinar las acciones recomendadas en las guías y documentación que se encuentran en la base de conocimiento.
    - **Nivel 3:** incidentes de gravedad alta que afectan considerablemente la operación de la organización. El líder del CSIRT debe coordinar el apoyo de los proveedores de servicios o consultores externos para controlar la situación, con el consultor de comunicaciones para emitir las notificaciones y avisos respectivos y con el consultor legal para analizar posibles repercusiones y tomar medidas al respecto.
    - **Nivel 4:** incidentes críticos. En este nivel se debe recurrir a las autoridades policiales para denunciar el caso y reportar el incidente ante los entes regulatorios como la SIC.

**Tabla 17.** Historial de revisiones del protocolo de escalamiento

| **Historial de revisiones** | | | |
|---|---|---|---|
| **Documento:** | Protocolo de escalamiento | **Fecha de creación** | 30/03/2025 |

| Razón de la revisión | # de revisión | Revisado por | Aprobado por | Fecha de revisión |
|---|---|---|---|---|
| Creación del documento | 1.0 | Dago Ramírez | | 30/03/2025 |

### 4.3.4 Redacción de un plan de implementación del modelo CSIRT.

La redacción del plan de implementación del modelo propuesto se estructuró en etapas secuenciales que permitieron organizar de manera simple el proceso de puesta en marcha del CSIRT. Cada etapa incluyó actividades clave que abarcaron desde la definición del grupo de atención hasta la puesta en funcionamiento del equipo. En la Figura 12 se muestra de forma gráfica la secuencia del plan de implementación propuesto. Este esquema sirve como guía para comprender el proceso completo de forma visual.

**Figura 12.** Plan de implementación del CSIRT


Nota. Actividades que se realizarán en el desarrollo del plan de implementación.

A continuación, se presenta la descripción de los pasos establecidos para implementar el modelo CSIRT en la ONG:

- Definir el grupo de atención estableciendo la comunidad que el CSIRT atenderá, incluyendo el tipo de usuarios (internos y externos) y sus necesidades, la ubicación geográfica y el alcance de la cobertura.
- Redactar, comunicar y velar por el cumplimiento de la política de seguridad de la información teniendo en cuenta la legislación local, la misión, el propósito y los objetivos estratégicos de la organización.
- Preparar los recursos que usará el CSIRT para la ejecución de sus actividades: crear formularios para el reporte de incidentes, solicitar las cuentas de correos electrónicos, dispositivos celulares y de cómputo, si es el caso, requerir el presupuesto necesario para suplir gastos, implementar un sistema de gestión de tickets que permita llevar la trazabilidad de los casos, crear la base de conocimientos con la documentación necesaria para la resolución de incidentes (playbooks, instructivos de proveedores, etc.).
- Seleccionar el personal que conformará el CSIRT basado en la descripción de los perfiles mencionados en la fase de diseño del modelo.
- Establecer alianzas y crear un directorio con la información de contacto de voluntarios expertos, miembros de otros CSIRT, autoridades policiales especializadas en ciberseguridad, proveedores de servicios tecnológicos de la organización y demás entidades o personal que pueda ser útil durante un incidente.
- Preparar el material de entrenamiento y talleres prácticos que permitan a los miembros del equipo adquirir las habilidades necesarias para desarrollar las actividades requeridas. Definir lineamientos para que la capacitación sea un proceso continuo, evaluado y documentado. Dentro de las actividades de capacitación se deben socializar el modelo de atención de incidentes y los protocolos de atención.
- Crear un plan de comunicación que permita que todos los usuarios conozcan el rol y funcionamiento del CSIRT. El plan debe contemplar una estrategia de socialización sobre cómo reportar incidentes y cómo actuar ante posibles amenazas. Se deben dar a conocer los canales de comunicación con el CSIRT.
- Poner en marcha el CSIRT empezando a prestar los servicios ofrecidos y gestionando los incidentes según los protocolos definidos. Adicionalmente, se debe establecer un mecanismo de monitoreo que permita evaluar la efectividad del CSIRT y ajustar los recursos, servicios, procesos y protocolos según se requiera.

## 4.4 Evaluación de la efectividad del modelo.

Para la evaluación de la efectividad del modelo se inició con el plan de implementación propuesto y se programaron 3 sesiones de una hora a través de Microsoft Teams con las 6 personas seleccionadas para integrar el equipo según sus habilidades. En la primera sesión se hizo una socialización de la estructura organizacional del modelo CSIRT propuesto para que los participantes entendieran este concepto y se tomó la primera medición del tiempo de respuesta ante incidentes. En la segunda sesión se entrenó a los participantes el tema de gestión de incidentes de seguridad informática y en la tercera sesión se realizó la segunda medición del tiempo de respuesta. A continuación, se detallan los resultados de estas actividades.

### 4.4.1 Inicio del plan de implementación.

Como parte del plan de implementación, se seleccionaron 6 personas de la organización en la que se realizó el estudio de caso. Estas personas se convocaron porque cumplían con los perfiles descritos en la actividad de diseño del modelo CSIRT. Los roles que desempeñaron fueron el de líder del CSIRT, líder técnico, consultor legal, consultor de comunicaciones y dos integrantes del equipo técnico. Adicional a este paso, se seleccionó como material para la sesión de entrenamiento del CSIRT, el modelo de atención de incidentes y los protocolos de atención propuestos. Con la realización de estas dos tareas se logró tener un nivel de implementación mínimo necesario para continuar con el desarrollo de esta tesis.

### 4.4.2 Medición inicial del tiempo de respuesta ante incidentes de ciberseguridad.

El siguiente es el ejercicio de mesa diseñado para medir el tiempo de respuesta del equipo ante un incidente de seguridad informática. Después socializar los objetivos, el contexto y el alcance, se presentó de manera gradual, cada uno de los tres momentos del evento sospechoso preparado.

**Objetivos**

- Evaluar el tiempo de respuesta ante incidentes de ciberseguridad.

- Analizar la capacidad de coordinación entre los miembros del equipo.
- Identificar debilidades en procesos y documentación establecidos.

**Contexto**

Este ejercicio de mesa forma parte del proceso de implementación y validación del modelo CSIRT propuesto para la organización. Su propósito es evaluar la capacidad de respuesta del equipo ante un incidente de ciberseguridad, antes y después de recibir capacitación formal en el modelo y sus protocolos. El ejercicio simula el reporte de un correo electrónico sospechoso, que aparenta provenir de Microsoft, solicitando el cambio de contraseña tras un supuesto bloqueo de cuenta.

**Alcance**

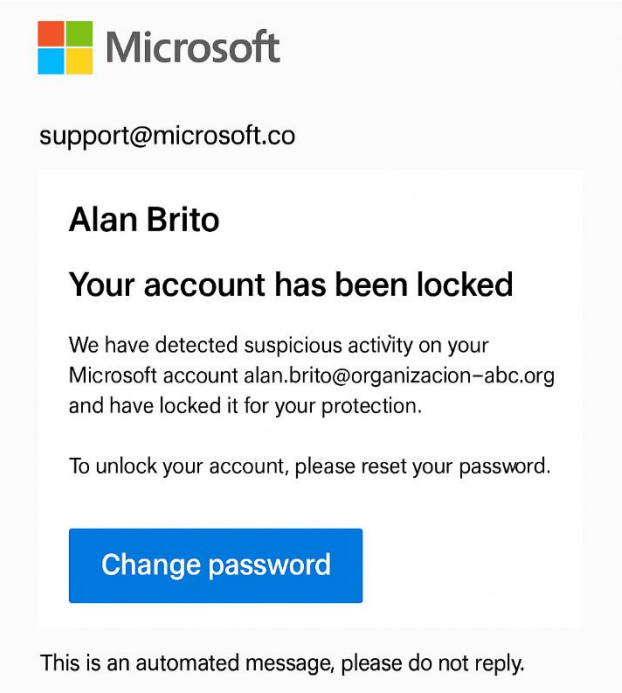
El ejercicio se enfoca en evaluar el proceso de gestión del evento desde el momento 1 en que es reportado hasta el momento 3 en el que se cierra el caso. El alcance incluye únicamente la gestión teórica y estratégica del evento; no se ejecutarán acciones técnicas reales sobre sistemas o cuentas. Además, se registrarán los tiempos que el equipo tarda en completar cada fase a través del diligenciamiento de un formato estructurado, con el fin de comparar el desempeño antes y después de la implementación completa del CSIRT.

**Momentos del evento**

**Momento 1:**

Un usuario envía la imagen que se ve en la Figura 13, que es de un correo que él recibió:

**Figura 13.** Correo electrónico sospechoso




Nota. Representación de correo electrónico malicioso recibido por un usuario. Fuente: imagen generada por ChatGPT.

Antes de ejecutar cualquier acción, ¿Cuáles son los procedimientos o actividades que se deben realizar para determinar si es un incidente o no?

**Momento 2:**

Basados en el análisis de la información recolectada, se determinó que el correo se trata de un ataque de Phishing que les llegó a todos los usuarios de la organización y 5 de ellos hicieron clic en el enlace e ingresaron las credenciales, ¿Cómo se debe proceder para solucionar el incidente?

**Momento 3:**

Después de llevar a cabo las acciones de respuesta, se ha logrado solucionar el incidente, ¿Qué actividades se deben realizar después del cierre del caso?

Cada vez que se introducían los momentos del ejercicio, los participantes analizaban las situaciones planteadas, discutían las posibles acciones que se debían llevar a cabo y diligenciaban el formato de la Tabla 18.

**Tabla 18.** Respuestas ejercicio de mesa medición 1

| Momento | Etapa | Actividad | Descripción de la Actividad | Hora de Inicio | Hora de finalización |
|---|---|---|---|---|---|
| 1 | Verificación / Validación | Análisis del email | Revisar el remitente y el dominio del que llega<br>Revisar el contenido (textos e imágenes)<br>Revisión de los enlaces | 11:39 | 11:53 |
| | | Intento de ingreso | Indicar al usuario que pruebe ingresar directamente desde la plataforma de correos para verificar si efectivamente hay un bloqueo | | |
| | | Verificación desde el administrador | El usuario administrador de las licencias debe revisar el estado de la cuenta en cuestión. | | |
| | | Revisión del equipo técnico | Solicitar asistencia del equipo técnico para la revisión del correo e identificación de posibles causas. | | |
| | | Verificación desde Microsoft o el soporte | Consulta con el soporte o documentación técnica si este tipo de mensajes se envían y cuáles son los pasos a seguir. | | |
| | | Verificación de casos similares | Validar si hay otros casos similares en la organización | | |
| 2 | Equipo Interno | Bloqueo de cuentas | Solicitar al administrador que bloquee las cuentas de los 5 | 11:54 | 12:07 |

| | | |
|---|---|---|
| | | usuarios que hicieron clic. |
| | Cambio de permisos y bloqueo de cuentas | Bloquear o forzar la salida de todos los usuarios de la organización de sus cuentas.<br><br>Identificar información sensible en SharePoint que pudo quedar en riesgo y asegurarla. |
| | Anuncio interno | Crear un correo/ anuncio que se envíe por los canales internos de la organización (correo, chat, plataforma) anunciando el incidente y solicitando que eviten hacer clic en el enlace y pidiendo que todos los miembros cambié sus claves. |
| | Búsqueda en página de Microsoft | Buscar información en los canales / manuales oficiales de Microsoft sobre las acciones y pasos a seguir en caso de identificar un ataque. |
| Capacidades externas | Llamada a un amigo | Activar a los proveedores o asesores externos que se tengan relacionados con el tema para brindar soporte técnico. |
| | Análisis del enlace del email | Pedir que se bloque el link del ataque desde la consola. |

| | | | | | |
|---|---|---|---|---|---|
| | | Verificar el historial de las cuentas afectadas | Verificar los logs o el historial que genera la plataforma para ver posible información que haya sido afectada. | | |
| 3 | | Actividad de sensibilización | Agendar una sesión de sensibilización y capacitación para aprender a identificar posibles casos de phishing o fraude. | 12:09 | 12:13 |
| | | Documentación del caso | Hacer un informe del diagnóstico de la situación y definir posibles acciones de mejora para actuar en caso de que se presente de nuevo. | | |
| | | Documentación adicional | Que presente otras posibles formas en las que se ven ataques como este en la organización. | | |

Nota. Formato diligenciado por los participantes del ejercicio durante la primera medición.

El formato fue diligenciado por uno de los participantes que se ofreció como voluntario para digitar las actividades que el equipo consideraba adecuadas para cada momento del incidente simulado. El formato permitió registrar de manera estructurada las acciones propuestas, así como los tiempos de inicio y finalización que se usaron más adelante para medir el tiempo de respuesta ante la situación planteada.

### 4.4.3 Capacitación del equipo y segunda medición.

Se realizó una segunda sesión en la que se capacitó a los participantes de la actividad. En esta sesión se usó como material de entrenamiento el modelo de atención de incidentes y los protocolos de actuación propuestos. En la tercera sesión se realizó exactamente el mismo ejercicio de mesa usado en la sesión 1 y siguiendo la misma metodología. Las

respuestas proporcionadas por los miembros del equipo para cada uno de los momentos planteados durante esta actividad se encuentran registradas en la Tabla 19.

**Tabla 19.** Respuestas ejercicio de mesa medición 2

| Momento | Etapa | Actividad | Descripción de la Actividad | Hora de Inicio | Hora de finalización |
|---|---|---|---|---|---|
| 1 | Reporte y registro | Documentar el incidente en la bitácora | Registrar el evento en la herramienta que se defina | 2:07 | 2:15 |
| | | Revisión y análisis del incidente reportado | Analizar y tipificar el nivel del incidente | | |
| | | Validar el alcance el incidente con otros colaboradores | | | |
| | Análisis y clasificación | Clasificación y nivel del incidente | | | |
| 2 | Atención del incidente | Activar el protocolo de atención | Listar las cuentas y recursos comprometidos | 2:16 | 2:29 |
| | | Contacto a administradores de plataforma | Gestionar aislar las cuentas comprometidas<br>Gestión de cambios de contraseñas<br>Validar si se requiere apoyo de otro nivel<br>Monitorear a profundidad la actividad de las cuentas y los recursos | | |
| | | Notificación a través de comunicaciones | Comunicar a la organización que se está atendiendo un incidente y brindar recomendaciones mientras se resuelve | | |
| | | Validación de aspectos legales | Validar si se afectó información sensible de clientes | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Documentación del caso | Realizar el registro de todas las acciones llevadas a cabo durante la atención del incidente | | |
| | | Implementar protocolo de comunicación | Correo con información de sensibilización y prevención | | |
| 3 | Acciones post-incidente | Lecciones aprendidas | Reunión sobre lecciones aprendidas | 2:30 | 2:34 |
| | | Formación a colaboradores | Formación sobre distintos tipos de incidentes y recomendaciones | | |

Nota. Formato diligenciado por los participantes del ejercicio durante la segunda medición.

El formato fue diligenciado nuevamente por uno de los participantes, quien asumió el rol de registrar las respuestas acordadas por el equipo durante el desarrollo del ejercicio. Al igual que en la primera medición, se documentaron las actividades que el grupo consideró adecuadas para cada una de las fases del incidente, así como los tiempos de inicio y finalización. Esta información permitió comparar los resultados antes y después de la capacitación, evaluando tanto el tiempo de respuesta como el nivel de comprensión del equipo frente al modelo y los protocolos propuestos.

### 4.4.4 Análisis de resultados obtenidos.

En la Tabla 20 se consolidó la información de las horas de inicio y finalización registradas por los participantes en cada uno de los momentos del ejercicio de mesa. Con esta información se calcularon los tiempos de respuesta, en donde el Tiempo Parcial Invertido es la cantidad de minutos que le tomó al equipo registrar las actividades en el formato de Excel y el Tiempo Total Invertido es la suma de los tiempos parciales, es decir, el Tiempo Total Invertido representa la cantidad de minutos que le tomó el equipo finalizar el ejercicio de mesa planteado.

**Tabla 20.** Matriz de consolidación de tiempos invertidos

| Sesión | Momento | Hora de Inicio | Hora de Finalización | Tiempo Parcial invertido | Tiempo Total Invertido |
|---|---|---|---|---|---|
| 1 | 1 | 11:39 | 11:53 | 14 | 31 |
| | 2 | 11:54 | 12:07 | 13 | |
| | 3 | 12:09 | 12:13 | 4 | |
| 3 | 1 | 2:07 | 2:15 | 8 | 25 |
| | 2 | 2:16 | 2:29 | 13 | |
| | 3 | 2:30 | 2:34 | 4 | |

Nota. Consolidado basado en los tiempos registrados por los participantes en las dos mediciones.

Aunque a simple vista se nota una reducción de 6 minutos en el tiempo de respuesta de la medición final con respecto al tiempo de la medición inicial, para evaluar la efectividad del modelo en términos de porcentaje, se usó la fórmula de variación porcentual (VP) para calcular la diferencia entre estas dos mediciones. Para llevar un orden y tener un mejor entendimiento al aplicar la fórmula, se definió T1 como el tiempo total invertido para la sesión 1, es decir, la medición inicial y T2 como el tiempo total invertido para la sesión 3. Con esto se tiene que:

$$VP = \frac{T2 - T1}{T1} \cdot 100$$

Reemplazando los valores en la fórmula se sigue que:

$$VP = \frac{25 - 31}{31} \cdot 100$$

Por lo tanto, se concluye que:

$$VP = -19.35\%$$

El valor negativo en este resultado indica que hubo un decremento en el tiempo de respuesta de la vez que se realizó el ejercicio en la sesión 3, con respecto a la vez que se hizo en la sesión 1, lo que ratifica la variación en minutos percibida en la columna Tiempo Total Invertido de la TABLA 20. Esto significa que, en teoría, el equipo fue un 19.35% más efectivo después del entrenamiento. Adicional a la mejora en los tiempos, como se puede apreciar al comparar las respuestas del formato diligenciado durante el ejercicio de mesa,

después de la sesión de entrenamiento los miembros de CSIRT tienen un mejor entendimiento sobre la gestión de incidentes de seguridad informática, tienen más claras las actividades que se debe realizar en cada momento y a qué fase del modelo de gestión de incidentes pertenecen. Esto también es un indicador de que el modelo propuesto ayudó a mejorar la respuesta ante la situación planteada.

# 5. Conclusiones y recomendaciones

## 5.1 Conclusiones

- Debido a la relevancia del tema de seguridad informática, existe una gran cantidad de material disponible. Esto se vio reflejado en el total de documentos encontrados al principio de este trabajo durante la fase de caracterización; y aunque inicialmente se consideró incluir fuentes nacionales, se descartaron los recursos de este tipo debido a que los lineamientos de los documentos de organismos internacionales seleccionados no solo enmarcan y resumen buenas prácticas globales, sino que además han servido como referentes para múltiples otras fuentes. La documentación caracterizada permitió construir una base de conocimientos sólida, actualizada y aplicable al contexto de las ONG, brindando a esta tesis una fundamentación teórica sólida y coherente.

- Tomando como base las buenas prácticas caracterizadas en la fase anterior, se logró establecer un modelo para el manejo de incidentes de ciberseguridad aplicable a las ONG. El modelo se diseñó pensando en las limitaciones comunes de este tipo de organizaciones, como la falta de personal especializado y recursos tecnológicos, lo que permitió definir una estructura en la que se tuvieron en cuenta todas las etapas del proceso de gestión de incidentes, desde el reporte inicial hasta las acciones posteriores al cierre del caso. La adaptación de referentes internacionales a este contexto hace que el modelo pueda ser implementado en organizaciones con distintos niveles de madurez tecnológica, contribuyendo así a fortalecer su capacidad de respuesta ante amenazas de seguridad informática.

- Aunque los servicios definidos para el modelo CSIRT propuesto son reducidos, si se realiza una buena planeación y se realizan continuamente actividades como los anuncios sobre amenazas y las jornadas de concientización, el enfoque de las operaciones puede ser no solo reactivo, sino también preventivo ya que estas acciones permiten preparar al grupo de atención y reducir la posibilidad de que ocurran incidentes. Además, dado que los perfiles propuestos para los integrantes del CSIRT no requieren obligatoriamente conocimientos técnicos avanzados, la

mayoría de las acciones que se llevarán a cabo durante un incidente serán estratégicas, como coordinar, comunicar o tomar decisiones, más que resolver problemas técnicos directamente. Esto permite que el modelo sea viable y útil incluso en organizaciones sin personal especializado.

- Aunque en la fase de evaluación del modelo no se alcanzó la meta del 30% de reducción en el tiempo de respuesta planteada en el cuarto objetivo específico, es válido decir que la mejora del 19.35% lograda después de la implementación del modelo se debe a que solo se tuvo una única sesión de entrenamiento. Esta mejora indica que el equipo fue más ágil y eficiente al momento de responder al ejercicio simulado. Además, el análisis de las respuestas registradas en el formato del ejercicio evidenció un mejor entendimiento por parte del equipo sobre el proceso de gestión de incidentes, las actividades a realizar en cada etapa y el uso adecuado de los protocolos definidos. Esto demuestra que el modelo propuesto no solo contribuyó a reducir el tiempo de respuesta, sino también a fortalecer la comprensión y preparación del equipo frente a situaciones de ciberseguridad.

- El modelo de centro de respuesta a incidentes (CSIRT) propuesto fue diseñado para minimizar el impacto de los eventos de ciberseguridad en ONG, a través de la aplicación de protocolos de actuación basados en buenas prácticas recomendadas por organismos reconocidos en el campo. Aunque el objetivo inicial se enfocaba en ONG que prestan servicios de tecnología, el modelo desarrollado puede ser aplicable también en organizaciones que comparten la característica de no contar con equipos de TI ni personal técnico especializado. Su estructura organizativa flexible, los perfiles definidos para los roles del equipo y los servicios planteados permiten su implementación en contextos con recursos limitados.

## 5.2 Recomendaciones

- A medida que el equipo adquiera más experiencia, se recomienda ampliar progresivamente los servicios que se ofrecen desde el CSIRT, para ayudar a fortalecer la postura de seguridad de la organización. Esto les permitirá estar aún más preparados durante un posible incidente.

- Con relación a los servicios prestados, se sugiere complementarlos con la implementación de un plan de continuidad de negocio y el uso de metodologías de análisis de riesgos. Estas herramientas permitirán identificar vulnerabilidades con anticipación y estar mejor preparados para situaciones que puedan afectar la operación.

- Con base en los resultados obtenidos durante la validación del modelo, se recomienda que antes de iniciar formalmente las operaciones del CSIRT, los miembros del equipo reciban una capacitación más completa y práctica. También es importante realizar ejercicios de evaluación que permitan verificar si realmente comprenden el modelo de gestión de incidentes y los protocolos definidos.

- Se aconseja revisar y actualizar periódicamente los protocolos, los materiales de capacitación y los recursos del CSIRT, para que se mantengan alineados con las nuevas amenazas y con las necesidades de la organización.

- Dada la creciente tendencia en el uso de inteligencia artificial (IA) por parte de los atacantes y del reto que esto significa para las organizaciones, se recomienda que el CSIRT considere este tipo de amenazas dentro de sus planes de preparación y respuesta. Esto incluye estar atentos a nuevas técnicas basadas en IA, participar en capacitaciones o talleres especializados y, en la medida de lo posible, explorar herramientas de defensa que también utilicen IA para la detección y mitigación de incidentes. Con ello, la organización podrá anticiparse a escenarios más complejos y garantizar que el modelo de CSIRT se mantenga actualizado frente a la evolución de este tipo de amenazas.

# 6. Bibliografía

[1] E. Caralt, I. Carreras, M. Sureda, “La transformación digital en las ONG. Conceptos, soluciones y casos prácticos”. pwc. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.pwc.es/es/fundacion/assets/transformacion-digital-en-las-ong-pwc-esade-iis.pdf

[2] M Hill, “La ciberseguridad se vuelve esencial para las ONG”. CSO Computerworld. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://cso.computerworld.es/tendencias/la-ciberseguridad-se-vuelve-esencial-para-las-ong

[3] “Perspectivas de CIBERSEGURIDAD de los Líderes de la Industria”. LATAM CISO. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.latamciso.com/Report2023SPA.pdf

[4] J. Giordani, “The Necessity Of Cybersecurity In The Nonprofit Sector”. Forbes. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.forbes.com/sites/forbestechcouncil/2022/11/08/the-necessity-of-cybersecurity-in-the-non-profit-sector/?sh=16de1d5a5588

[5] Microsoft Corp. “Informe de protección digital de Microsoft de 2022”. Microsoft Corp. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.microsoft.com/es-co/security/business/microsoft-digital-defense-report-2022

[6] Nonprofit Tehc for Good, “2023 Nonprofit Tech for Good Report”. Nonprofit Tech for Good. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.nptechforgood.com/wp-content/uploads/2023/02/Nonprofit-Tech-for-Good-Report-Final2-2023.pdf

[7] TicTac, “Estudio anual de Ciberseguridad 2022-2023”. CCIT - Cámara Colombiana de Informática y Telecomunicaciones. Accedido el 30 de septiembre de 2023. [En línea]. Disponible: https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/

[8] Threat Research Team. “Avast Q4/2023 Threat Report - Avast Threat Labs”. Avast Threat Labs. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://decoded.avast.io/threatresearch/avast-q4-2023-threat-report/

[9] “Alerta por el aumento de ciberataques contra las entidades - Gestión Tercer Sector”. Gestión Tercer Sector. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://gestiontercersector.org/alerta-ciberataques-contra-entidades/

[10] M. Szczesny. “Why nonprofits need to be more worried about cybersecurity”. Security Magazine | The business magazine for security executives. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://www.securitymagazine.com/articles/99463-why-nonprofits-need-to-be-more-worried-about-cybersecurity

[11] N. García Cabezas. “Qué es una ONG y cómo funciona | Ayuda en Acción”. Ayuda en Acción. Accedido el 29 de mayo de 2024. [En línea]. Disponible: https://ayudaenaccion.org/blog/solidaridad/que-es-una-ong/#:~:text=Para%20saber%20qué%20significa%20una,que%20no%20tiene%20afán%20lucrativo.

[12] “¿Qué es la ciberseguridad?” Cisco. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

[13] “¿Qué es la ciberseguridad?” Kaspersky. Accedido el 23 de abril de 2024. [En línea]. Disponible: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[14] “¿Qué es un ataque cibernético? | IBM”. IBM in Deutschland, Österreich und der Schweiz. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://www.ibm.com/mx-es/topics/cyber-attack

[15] “ISO 27002 A16 Gestión de Incidentes de la Seguridad de la Información”. Norma ISO 27001. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/

[16] “Buenas Prácticas para establecer un CSIRT nacional”. Organización de los Estados Americanos. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[17] H. Bronk, M. Thorbruegge, M. Hakkaja “CSIRT Setting up Guide in English”. European Union Agency for Cybersecurity. Accedido el 11 de abril de 2024. [En línea]. Disponible: https://www.enisa.europa.eu/publications/csirt-setting-up-guide

[18] F. Salazar “Estándares ISO de Ciberseguridad”. LinkedIn. Accedido el 23 de abril de 2024. [En línea]. Disponible: https://www.linkedin.com/pulse/est%C3%A1ndares-iso-de-ciberseguridad-fernanda-salazar/

[19] NIST “The NIST Cybersecurity Framework (CSF) 2.0”. NIST. Accedido el 23 de abril de 2024. [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[20] “ENISA”. ENISA. Accedido el 30 de mayo de 2024. [En línea]. Disponible: https://www.enisa.europa.eu/

[21] “Information on RFC 2350”. RFC Editor. Accedido el 30 de mayo de 2024. [En línea]. Disponible: https://www.rfc-editor.org/info/rfc2350

[22] “Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales”. Superintendencia de Industria y Comercio. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

[23] “TemáTICas Gestión de incidentes de seguridad”. Incibe. Accedido el 23 de abril de 2024. [En línea]. Disponible: https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

[24] “Gestión de riesgos: ¿Qué es y cómo funciona la gestión de riesgos?” Red Hat - We make open source technologies for the enterprise. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://www.redhat.com/es/topics/management/what-is-risk-management

[25] “Gestión de riesgos” MinEducación. Accedido el 23 de abril de 2024. [En línea]. Disponible: https://www.mineducacion.gov.co/1621/articles-327021_archivo_pdf_Dia2_1_Gestion_Riesgo.pdf

[26] A. B. Team. “Business Continuity Plan (BCP): What Is It and How to Make One”. Business Continuity Plan (BCP): What Is It and How to Make One. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://www.avast.com/c-b-what-is-a-business-continuity-plan

[27] “Guía para la preparación de las TIC para la continuidad del negocio”. MinTIC. Accedido el 23 de abril de 2024. [En línea]. Disponible: https://gobiernodigital.mintic.gov.co/692/articles-150506_G10_Continuidad_Negocio.pdf

[28] “LACNIC CSIRT - El proyecto AMPARO”. LACNIC CSIRT. Accedido el 7 de abril de 2024. [En línea]. Disponible: https://csirt.lacnic.net/el-proyecto-amparo

[29] “Acerca de ColCERT”. ColCERT. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://www.colcert.gov.co/800/w3-article-198657.html

[30] “Documentos CONPES”. Departamento Nacional de Planeación. Accedido el 5 de agosto de 2025. [En línea]. Disponible: https://www.dnp.gov.co/LaEntidad_/subdireccion-

general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

[31] “Home Page | CISA”. Home Page | CISA. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://www.cisa.gov/

[32] G. D. Vargas, “Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT | INF-FCPN-PGI Revista PGI”. Apache HTTP Server Test Page powered by CentOS. Accedido el 8 de abril de 2024. [En línea]. Disponible: https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/55

[33] Y. Z. Giraldo, “Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad”, Tesis de Maestría, Fac. de Ing., ITM, Medellín, Colombia, 2020. [En línea]. Disponible: https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5550/Yenifer_Zulay_Giraldo_Montes_2021.pdf?sequence=8&isAllowed=y

[34] FIRST “FIRST is the global Forum of Incident Response and Security Teams”. FIRST. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://www.first.org

[35] T. Grance, T. Nolan, K. Burke, R. Dudley, G White y T. Good. “Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities”. NIST. Accedido el 11 de mayo de 2025. [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

[36] R. Mooi and R. A. Botha, "Prerequisites for building a Computer Security Incident Response capability," 2015 Information Security for South Africa (ISSA), Johannesburg, South Africa, 2015, pp. 1-8, doi: 10.1109/ISSA.2015.7335057

[37] “A step-by-step approach on how to set up a CSIRT”. ENISA. Accedido el 11 de abril de 2024. [En línea]. Disponible: https://www.enisa.europa.eu/publications/csirt-setting-up-guide/@@download/fullReport

[38] Organización de los Estados Americanos. “Buenas prácticas para establecer un CSIRT nacional”. Organización de los Estados Americanos. Accedido el 10 de mayo de 2024. [En línea]. Disponible: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[39] Organización de los Estados Americanos. “Guía Práctica para CSIRTs”. Organización de los Estados Americanos. Accedido el 10 de mayo de 2024. [En línea].

Disponible: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

[40] Heimdal. “Computer Security Incident Response Team (CSIRT): How to Build One”. Heimdal. Accedido el 10 de mayo de 2024. [En línea]. Disponible: https://heimdalsecurity.com/blog/computer-security-incident-response-team-csirt/

[41] CISA. “Cybersecurity Best Practices”. CISA. Accedido el 10 de mayo de 2024. [En línea]. Disponible: https://www.cisa.gov/topics/cybersecurity-best-practices

[42] A. Nelson, S. Rekhi, M. Souppaya y K. Scarfone. “Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile”. NIST. Accedido el 22 de septiembre de 2025. [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[43] Enisa. “Good Practice Guide for Incident Management”. Enisa. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://www.enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf

[44] G. Killcrece, K. Kossakowski, R. Ruefle y M. Zajicek. “Organizational Models for Computer Security Incident Response Teams (CSIRTs)”. Carnegie Mellon University. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://insights.sei.cmu.edu/documents/1605/2003_002_001_14099.pdf

[45] “FIRST CSIRT Services Framework”. FIRST. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

[46] Lacnic Campus. “Curso básico para la creación y gestión de un CSIRT”. Lacnic. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://campus.lacnic.net/cursos/curso-basico-para-la-creacion-y-gestion-de-un-csirt/

[47] Lacnic. “Manual básico de: Gestión De Incidentes De Seguridad Informática”. Lacnic. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

[48] SIC. “Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales”. SIC. Accedido el 11 de mayo de 2024. [En línea]. Disponible: https://www.sic.gov.co/noticias/superindustria-expide-gu%C3%ADa-para-la-gesti%C3%B3n-de-incidentes-de-seguridad-en-el-tratamiento-de-datos-personales

[49] TechTarget. “How to create a CSIRT: 10 best practices”. TechTarget. Accedido el 12 de mayo de 2024. [En línea]. Disponible: https://www.techtarget.com/searchsecurity/feature/How-to-build-an-incident-response-team-for-your-organization

[50] M. West-Brown, D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle y M. Zajicek. “Handbook for Computer Security Incident Response Teams (CSIRTs)”. Carnegie Mellon University. Accedido el 12 de mayo de 2024. [En línea]. Disponible: https://insights.sei.cmu.edu/documents/1606/2003_002_001_14102.pdf

[51] MinTIC. “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”. MinTIC. Accedido el 12 de mayo de 2024. [En línea]. Disponible: https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

[52] MinTIC. “Guía 21 - Gestión de Incidentes”. MinTIC. Accedido el 12 de mayo de 2024. [En línea]. Disponible: https://gobiernodigital.mintic.gov.co/692/articles-150509_G21_Gestion_Incidentes.pdf

[53] ISO. “ISO/IEC 27035-1:2023 Information technology — Information security incident management Part 1: Principles and process”. ISO. Accedido el 12 de mayo de 2024. [En línea]. Disponible: https://www.iso.org/standard/78973.html

[54] ColCERT. “COLCERT”. ColCERT. Accedido el 13 de mayo de 2024. [En línea]. Disponible: https://www.colcert.gov.co/800/w3-channel.html

[55] Mitre ATLAS. “ATLAS Matrix”. Mitre ATLAS. Accedido el 27 de septiembre de 2025. [En línea]. Disponible: ATLAS Matrix | MITRE ATLAS™