UNIVERSIDAD INTERNACIONAL SEK

DIGITAL SCHOOL

Trabajo de fin de máster titulado:

"IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) EN LA FISCALÍA GENERAL DEL ESTADO"

Realizado por:

LEONARDO RAFAEL CHUQUIGUANCA VICENTE

Director de Proyecto:

Ing. Fabián Hurtado MGS.

Requisito para la obtención del título de:

MAGISTER EN CIBERSEGURIDAD

QUITO, agosto 2020

DECLARACION JURAMENTADA

Yo, **Leonardo Rafael Chuquiguanca Vicente**, con cédula de identidad **1104952708**, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, se cede los derechos de propiedad intelectual correspondientes a este trabajo, a la **Universidad Internacional SEK**, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Leonardo Rafael Chuquiguanca Vicente
C.C.:1104952708

DECLARATORIA

El presente trabajo de investigación titulado:

"**IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) PARA LA FISCALÍA GENERAL DEL ESTADO**"

Realizado por:

Leonardo Rafael Chuquiguanca Vicente

Como requisito para la obtención del título de:

MAGISTER EN CIBERSEGURIDAD

Ha sido dirigido por el docente:

Ing. Luis Fabián Hurtado Vargas, Mgs.

Quien considera que constituye un trabajo original de su autor

Ing. Luis Fabián Hurtado Vargas, Mgs.

DIRECTOR

DOCENTES LECTORES

Los docentes lectores:

Ing. Ernesto Pérez Estévez, Mgs.

Ing. José Vinicio Freire Rumazo, Mgs.

Después de revisar el trabajo presentado, lo han calificado como apto para su defensa oral ante el tribunal examinador.

Ing. Ernesto Pérez Estévez, Mgs. Ing. José Vinicio Freire Rumazo, Mgs.

Quito, agosto 2020

DEDICATORIA

El presente proyecto de tesis ha sido un escalón más en el crecimiento personal y profesional que me he propuesto, por lo cual se lo dedico:

Principalmente a Dios, por guiarme y darme salud y fuerzas para cumplir cada uno de los objetivos que me he planteado.

A mi familia, quienes han sido un apoyo fundamental en la realización de estos estudios. Gracias por sus consejos.

A los docentes de la maestría, quienes fueron una gran guía, compartiendo sus conocimientos y experiencias en este mundo de la ciberseguridad.

AGRADECIMIENTO

Agradezco principalmente a mi familia porque han sido el motor principal en mi vida, por sus consejos, motivación y apoyo incondicional en el trascurso de esta meta planteada.

A mis amigos que siempre han estado ahí para brindarme su apoyo y sus consejos al momento que los he necesitado.

A la Universidad Internacional SEK y a cada uno de los docentes de la Maestría en Ciberseguridad, quienes me han compartido sus conocimientos, consejos y experiencias profesionales.

A la Fiscalía General del Estado, a sus autoridades, y en especial a la Dirección de Tecnologías de la Información y Comunicaciones, a su Director y a sus especialistas y analistas de seguridad informática, quienes apoyaron desinteresadamente la idea de implementar este proyecto en la Institución.

Finalmente, a todos mis compañeros de la maestría con los cuales se ha logrado forjar una buena amistad y compañerismo, amigos con los que se aprendió mucho y se cumplió muchos objetivos en el transcurso de estos estudios realizados.

RESUMEN

La presente tesis tiene como objetivo implementar un Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT) en la Fiscalía General del Estado (FGE), por lo que, para el cumplimiento de este objetivo, inicialmente se ha realizado un análisis del estado del arte, seguido de una revisión bibliográfica y la recolección de información y estudio documental de casos de éxito en la implementación de CSIRT a nivel de Latinoamérica, logrando con esto determinar la importancia que tienen los centros de respuesta de incidentes cibernéticos en el campo de la ciberseguridad en cada uno de sus países, por otra parte, también se realizó un estudio de la situación actual de la Fiscalía General del Estado enfocado a la seguridad informática, consiguiendo tener un detalle de las amenazas cibernéticas que con más frecuencia se dan en la institución.

Basándose en la información obtenida con el estudio documental de centros de respuesta a incidentes cibernéticos en Latinoamérica, y el estado de la situación actual de la Fiscalía General del Estado en temas de seguridad informática, se logra tener la línea base para trabajar en el diseño del CSIRT de la FGE acorde las mejores prácticas definidas por el Foro Mundial de Respuesta a Incidentes y Equipos de Seguridad (FIRST) y el estándar RFC 2350. En este diseño se define, de entre los diferentes puntos, la misión, visión, comunidad objetivo, políticas, procedimientos, servicios, y el equipo inicial con el cual el equipo entrará en operaciones.

Finalmente, con la culminación del diseño, se procede con la implementación de éste en la Fiscalía General del Estado, dentro de esta implementación se define en la estructura orgánica y funcional, la infraestructura tecnológica a utilizar a nivel de hardware y software, el presupuesto necesario para su funcionamiento y las leyes, normativas y reglamentos que debe cumplir el centro de respuesta a incidentes de ciberseguridad en la parte legal.

Palabras Clave: CSIRT, CERT, FIRST, RFC 2350, Gestión de incidentes, Ciberseguridad, Incidentes cibernéticos.

ABSTRACT

The present thesis aims to implement a Computer Security Incident Response Team (CSIRT) in the Fiscalía General del Estado (FGE), so, for the fulfillment of this objective, an analysis of the state of the art has initially been carried out, followed by a bibliographic review and the collection of information and documentary study of success stories in the implementation of CSIRT at the Latin American level, thus managing to determine the importance of cyber incident response centres in the field of cybersecurity in each of their countries, on the other hand, there was also a study of the current situation of the Fiscalía General del Estado focused on computer security, achieving a detail of the cyber threats that occur most often in the institution.

Based on the information obtained with the documentary study of cyber incident response centers in Latin America, and the state of the current situation of the Fiscalía General del Estado on computer security issues, it is possible to have the baseline to work on the design of the FGE CSIRT according to the best practices defined by the Forum of Incident Response and Security Teams (FIRST) and RFC 2350 standard. This design defines, from the different points, the mission, vision, target community, policies, procedures, services, and the initial team with which the team will enter into operations.

Finally, with the culmination of the design, proceeds with the implementation of this in the Fiscalía General del Estado, within this implementation is defined in the organic and functional structure, the technological infrastructure to be used at the hardware and software level, the budget necessary for its operation and the laws, regulations and regulations that must be met by the cybersecurity incident response center in the legal part.

Keywords: CSIRT, CERT, FIRST, RFC 2350, Incident Management, Cybersecurity, Cyber incidents.

Contenido

CAPÍTULO I

INTRODUCCIÓN

1.1. Planteamiento del problema

La ciberseguridad es una de las áreas claves que actualmente todos los países deben tener presente ya que el crecimiento tecnológico que se ha venido suscitando en los últimos años han sido muy importantes y relevantes en la sociedad, a la par de este crecimiento y mejoramiento tecnológico, también existe un incremento en el número de amenazas e incidentes de seguridad en los sistemas y redes informáticos a nivel global; y con ello, términos como: ciberespacio, ciberataques, ciberdelincuentes, ciberdefensa, entre otros, se han ido popularizando (Vargas, Recalde, and Reyes 2017), por lo que las empresas y/o personas enroladas en el campo de las tecnologías y la ciberseguridad deben ir de la mano con este crecimiento tecnológico, con la finalidad de mantener seguras las infraestructuras tecnológicas de información de las organizaciones.

Países considerados potencias en Asia, Europa y América manejan políticas públicas de seguridad cibernética, en Sudamérica, países como Brasil, Colombia, Argentina, Perú y Chile ya cuentan con políticas nacionales de ciberseguridad (Vargas et al. 2017), sin embargo, en Ecuador a partir del año 2018 se comenzó a trabajar en una estrategia pública de ciberseguridad (MINTEL 2018). Actualmente este proceso sigue en marcha y se espera que en los próximos años Ecuador cuente con una política y estrategia pública de ciberseguridad.

El Estado ecuatoriano, con el objetivo de minimizar las amenazas cibernéticas ha implementado proyectos como: (a) El EcuCERT, para el tratamiento de los incidentes cibernéticos en el área de las telecomunicaciones, (b) Políticas para cumplimiento dentro de la administración pública como el Esquema Gubernamental de Seguridad de la Información – EGSI v1 (SNAP 2013), y su actualización “EGSI v2” en enero de 2020, a través de la Edición Especial Nro. 228 – Registro Oficial. Pese a que la implementación del EGSI es de carácter

obligatoria para las instituciones pertenecientes al ejecutivo, muy pocas lo han implementado y sus medidas de control de seguridad aún siguen siendo débiles (MINTEL 2018; Vargas et al. 2017).

Por otra parte, a pesar de los esfuerzos realizados por entidades gubernamentales como: la ex Secretaría Nacional de la Administración Pública (SNAP) y actualmente la subsecretaría de Gobierno Electrónico, del Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), Ecuador aun no trabaja de manera sistematizada con políticas públicas y procedimientos claros a seguir, en lo que correspondiente a incidentes de seguridad informática. Debido a esto, en septiembre de 2019, investigadores de la empresa de seguridad informática vpnMentor expusieron hasta lo que hoy conocemos cómo el incidente de seguridad informática más grande que se ha dado en el Estado ecuatoriano con la filtración de información de más de 20 millones de personas, esto basado en una grave falla informática en uno de los servidores pertenecientes a la empresa ecuatoriana Novaestrat (Rotem and Locar 2019), este incidente informático se pudo tratar y gestionar en días posteriores gracias a la intervención y coordinación del EcuCERT.

Finalmente, Vargas (2017) en su investigación propone la creación de centros de respuesta a incidentes de seguridad informática por sectores (bancarios, telecomunicaciones, seguridad nacional, infraestructuras críticas, e instituciones públicas), mismos que trabajarán de manera coordinada con otros Centros de Respuesta de Incidentes de Seguridad, con el objetivo de: identificar, analizar, responder, recuperar, coordinar e intercambiar información.

En Ecuador existen diferentes tipos de CSIRT, empresas privadas (ofrecen servicios a sus clientes), educativos (enfocadas a la academia) y un CERT coordinador del gobierno (EcuCERT, enfocado con el sector de las telecomunicaciones)(FIRST 2019a). Por lo que la carencia de CSIRT gubernamentales y su difusión a nivel estatal y a nivel de ciudadanía ha

sido una limitante para que se recepten y tramiten los incidentes cibernéticos en el menor tiempo posible y de manera coordinada.

1.2.Formulación del problema

La gestión no oportuna e incorrecta de los incidentes cibernéticos y delitos informáticos en las instituciones públicas conlleva una afectación directa a la integridad, disponibilidad y confidencialidad de sus activos y sistemas de información, por lo que se considera necesario la creación de un equipo de respuesta a incidentes de seguridad Informática (CSIRT) en una institución gubernamental que tenga la capacidad de brindar una pronta respuesta a estos incidentes cibernéticos, cumpliendo las normativas, estándares y mejores prácticas establecidas a nivel global por organismos como el FIRST.

1.3.Objetivos

1.3.1. Objetivo General

Implementar un CSIRT gubernamental que instaure un Equipo de Respuesta a Incidentes de Seguridad Informática en la Fiscalía General de Estado, esto acorde al estándar RFC 2350 y las mejores prácticas definidas por el FIRST.

1.3.2. Objetivos específicos

- Analizar la implementación de CSIRT existentes mediante un estudio documental de casos de éxito, que ayude como punto de partida para la factibilidad de implementación de un CSIRT en la Fiscalía General del Estado.
- Realizar un análisis de la situación actual de la Fiscalía General del Estado, mediante la revisión de eventos de seguridad informática para la determinación de los servicios que ofrecerá el CSIRT.
- Diseñar el CSIRT para la Fiscalía General del Estado acorde el estándar RFC 2350 y las buenas prácticas emitidas por el FIRST que permitan un buen manejo de los incidentes de seguridad informática.

- Aplicar el CSIRT diseñado en la Fiscalía General del Estado mediante los lineamientos establecidos en la institución, que permitan la protección de la información ante posibles eventos cibernéticos.

1.4.Justificación

La Fiscalía General del Estado (FGE) es una Institución de la Función Judicial del Estado ecuatoriano, la cual ofrece sus servicios y cumple con las funciones de dirigir las investigaciones preprocesales e instrucciones fiscales de los procesos judiciales en materia penal a nivel país. La FGE para brindar estos servicios cuenta con 3.799 funcionarios trabajando en todo el territorio ecuatoriano con recorte al mes de abril de 2020, de los cuales aproximadamente 800 funcionarios trabajan en el edifico de planta central (FGE 2020b). Por lo que la cantidad de usuarios que hacen uso de los servicios tecnológicos que ofrece la FGE es bastante alto; esto implica que, la probabilidad para que se generen incidentes informáticos o ciberataques sea igualmente alto, ya sea, debido al mal uso que los usuarios puedan darles a estos recursos informáticos o porque dichos usuarios pueden llegar a ser una fuente primaria para el inicio de amenazas o ataques cibernéticos externos.

La FGE con la finalidad de evitar ciberataques o protegerse de eventos de seguridad informática que puedan suscitarse en la Institución, cuenta con el área de seguridad de la información que trabaja para ello, sin embargo, no cuenta con un área especializada o con las responsabilidades de: emitir alertas (boletines), establecer procedimientos, analizar, gestionar y manejar incidentes de seguridad informática, acorde las mejores prácticas emitidas por entidades y organizaciones reconocidos globalmente como lo son el FIRST, NIST, ISACA, entre otras.

Por lo expuesto, se ve la necesidad de crear un equipo que tenga las competencias para realizar la gestión y respuesta a incidentes de seguridad informática en la FGE acorde a las mejores prácticas y estándares globales. Con la implementación de este equipo, la Fiscalía

General del Estado podrá entre otras actividades, coordinar con otros CSIRT a nivel local y nacional eventos de ciberseguridad con la finalidad de fortalecer la gestión de incidentes relacionados a la seguridad de los activos y sistemas informáticos tanto internos como externos, y a la vez este equipo podrá brindar un apoyo coordinado con el área de seguridad de la información y Dirección de Tecnologías a su comunidad objetivo (funcionarios) mediante la emisión de: reportes, directrices y capacitaciones permanentes en temas de ciberseguridad.

1.5.Estado del arte

Se realizó una búsqueda exhaustiva de información con la finalidad de identificar las fuentes de información relevantes para el establecimiento de un CSIRT, por lo que, las cadenas de búsqueda detalladas en los siguientes puntos fueron aplicadas acorde a las siguientes palabras claves: csirt, cert, computer, security, emergency, incident, response, team.

- (csirt OR cert) AND law
- (computer AND security AND incident AND response AND team) OR (computer AND emergency AND response AND team)
- equipo AND de AND respuesta AND a AND incidentes AND de AND seguridad AND informática
- computer AND security AND incident AND response AND team AND csirt
- (computer AND security AND incident AND response AND team AND csirt) AND PUBYEAR > 2014

Esta aplicación de las cadenas de búsqueda y revisión bibliográfica se la realizó en bases de datos científicas como: Scopus, IEEE Explore, ScienceDirect y Springer Link; logrando obtener como resultado las investigaciones que serán detalladas en los siguientes apartados, mismas que fueron filtradas por su relevancia según el título, seguido del resumen, y número de citaciones.

Mooi y Botha (2015) en su investigación "**Prerequisites for building a computer security incident response capability**" expresan que hay una serie de consideraciones que se deben tener en cuenta previo a implementar y operar un CSIRT. Es decir, la investigación identifica

las características, actividades y procesos que se deben cumplir dentro de 5 áreas catalogadas como primarias para comenzar con el proceso de establecimiento de un equipo de respuesta a incidentes (entorno, circunscripción, financiamiento, autoridad y consideraciones legales).

Por un lado, portales de noticias de tecnologías de la información, conferencias de ciberseguridad, conversaciones de ciberguerra, evidencian la realidad actual de garantizar la seguridad de la información, por otra parte, ataques de denegación de servicios (DDoS), malware, explotación y revelación de vulnerabilidades criticas como "Heartbleed"(vulnerabilidad OpenSSL), "Shellshock" (vulnerabilidad Bash) son principales ejemplos de incidentes de seguridad informática, que han demostrado, cuán frágil es realmente este ecosistema.

La comunidad de Internet y expertos a nivel global en ciberseguridad se han adecuado para conocer y lidiar con estos incidentes, por lo que, a las políticas y procedimientos también se han incluido mecanismos de cómo actuar ante estas situaciones, estos mecanismos involucran personas y algún tipo de estructura de trabajo en equipo. A esta estructura de trabajo en equipo, se le conoce actualmente como equipo de respuesta a incidentes de seguridad informática.

En esta investigación, los autores también expresan que los CSIRT presentan una serie de desafíos a enfrentar al momento de establecer estos equipos de respuesta a incidentes en países en desarrollo. Estos desafíos incluyen, una misión poco clara, falta de apoyo en la gestión, falta de presupuesto y apoyo administrativo y una autoridad rectora no bien definida, por lo tanto, en este artículo los investigadores presentan la primera parte de una solución a este problema, el cual es, tener claro los objetivos de la organización para establecer los requisitos necesarios para la construcción del CSIRT.

Dentro de los requisitos detallados por los autores de la investigación para el establecimiento de un CSIRT, se encuentran, seguir las normas, mejores prácticas, estándares y directrices emitidas por:

- RFC 2350.
- SANS 27002.
- El Instituto Nacional de Estándares y Tecnologías (NIST).
- El Instituto de Ingeniería de Software de la Universidad Carnegie Mellon (CMU-SEI).
- La Agencia de Ciberseguridad de la Unión Europea (ENISA).
- El Foro Global de Respuesta a Incidentes y Equipos de Seguridad (FIRST).

Como se lo expresó en los párrafos anteriores, se debe cumplir con 5 áreas primarias para comenzar con el proceso de establecimientos de un CSIRT, estas áreas son:

I. Entorno

El entorno del CSIRT puede ser definido por el sector o área del negocio al que atenderá el equipo de respuesta a incidentes, así como también por la región geográfica y operaciones, tal como se visualiza en la Tabla 1.

Tabla 1.Entorno de un CSIRT basado en el Sector y Tipo de servicio

Sector	Serving
Academic	Research and education organisations
CIP/CIIP	Critical Information and/or Infrastructure Protection (energy, transportation, critical ICT infrastructure, etc.)
Government	Government agencies (and sometimes citizens)
Military	Military departments
SME	Small and medium enterprises or special interest groups (usually self organised)
Type	**Serving**
National	Whole country (usually in a coordinating/intermediary role)
Commercial	Commercial services to paying clients
Internal	Hosting organisation only
Vendor	Specific hardware or software vendor (also called a Product Security Incident Response Team (PSIRT))
Other	Any type or sector not fitting into the above

***Fuente**: Mooi and Botha (2015)*

El entorno es de vital importancia, ya que revela la circunscripción y proporciona información para el modelo y los servicios del CSIRT.

II. Circunscripción

La circunscripción define la comunidad objetivo (usuarios) a los cuales el CSIRT brindará sus servicios, la circunscripción puede ser interna (dentro de la misma organización) o externa,

centralizada o distribuida (entre ciudades, países), para definir la circunscripción se debe tener claro el entorno del CSIRT.

III. Financiamiento

El presupuesto que necesita el CSIRT debe ser definido acorde sus servicios, sin embargo, se debe contar con el presupuesto para el personal, infraestructura tecnológica y capacitación. Las consideraciones del presupuesto deben ser tomadas en cuenta en la fase de planificación del CSIRT. No obstante, la mayoría de los CSIRT son financiados por la organización matriz (por ejemplo, Universidad o Entidad de Gobierno).

IV. Autoridad

La autoridad describe la capacidad con la que contará el CSIRT para la toma de decisiones relacionadas a la seguridad informática y a la gestión de incidentes. Existen cuatro tipos de relaciones de autoridad que un CSIRT puede tomar sobre su comunidad objetivo (Completo, Compartido, Indirecta y Ninguna).

V. Consideraciones legales

Los CSIRT deben acoplarse a las leyes que regulan cada uno de sus países.

Finalmente, los autores llegan a la conclusión que la relación entre de las 5 áreas expuestas como requisitos para establecer un CSIRT se deben seguir ordenadamente ya que las decisiones tomadas en cada área son fundamental para alimentar las áreas posteriores, permitiendo una mejor planificación y un enfoque más metodológico para la implementación de un CSIRT. Una vez se hayan cumplido estos requisitos de manera satisfactoria, el siguiente paso sería la determinación de los servicios que ofrecerá el CSIRT, así como el personal con el cual iniciara el equipo.

Por otro lado, según Jezreel, Mirna, and Edgar (2015) en su estudio "***Establecimiento de Servicios en Equipos de Respuesta ante Incidentes de Seguridad Informática***" presentan una

revisión sobre los aspectos principales a tomar en cuenta al momento de definir los servicios iniciales que ofrecerá un CSIRT.

En este artículo los autores informan sobre el desarrollo de un sistema para automatizar la extracción de información actualizada de diferentes tipos de CSIRT acorde el formato del RFC 2350. Una vez extraída esta información con esta herramienta, la misma es almacenada en una base de datos, y posteriormente comparada con información que se encuentra en el portal de FIRST, obteniendo los resultados detallados en los puntos siguientes:

A. Listado de Servicios

De los resultados obtenidos, se observa que de entre los servicios primordiales que ofrecen los CSIRT a su comunidad objetivo, se encuentran: gestión de incidentes, y emisión de alertas, advertencias y boletines en temas de ciberseguridad.

En este punto se destaca, que cada CSIRT ofrece diferentes tipos de servicios, esto depende de la misión, propósito y su comunidad objetivo.

B. Recomendaciones al elegir y definir los servicios

Los autores recomiendan que, para una mejor selección de los servicios, el equipo debe ser lo más realista respecto de las capacidades actuales que defina un catálogo de servicios a su comunidad objetivo, por lo que se recomienda que, si se va a ofrecer más servicios, el crecimiento sea paulatino.

C. Errores comunes

De entre los errores más comunes se encuentran:

- Ofrecer servicios antes que el CSIRT entre en marcha oficialmente.
- Ofrecer servicios innecesarios, y
- No ofrecer los servicios requeridos por la comunidad objetivo.

D. Personal y disponibilidad

El personar debe ser calificado y contar con la experiencia necesaria acorde las demandas del CSIRT, es importante también tener en cuenta que el CSIRT debe enfocarse en el tratamiento y gestión de incidentes.

E. Estructura de los sitios web de un CSIRT

El sitio web, es un elemento indispensable con el que debe contar un CSIRT, y en dicho portal se debe detallar por lo menos la misión, objetivos, contactos, servicios y alertas sobre incidentes cibernéticos.

Como punto final, los autores llegan a la conclusión de que existe la necesidad de crear grupos con el objetivo de ayudar a la mitigación de incidentes de ciberseguridad, y para ello los CSIRT han tomado un rol fundamental, ya que han sido adoptados en diferentes países a nivel global como una alternativa viable para combatir organizaciones criminales en temas informáticos.

Por otra parte, Mejía, Muñoz, and Ramírez (2016) en su investigación "***Propuesta de Marco de Trabajo para la Protección de un CSIRT***" expresan que los CSIRT también son vulnerables a ciberataques e incidentes informáticos como cualquier departamento u organización, por lo tanto es importante y necesario establecer controles de seguridad a sus activos de información e infraestructura tecnológica.

Por lo que, en esta investigación se detalla una propuesta de marco de trabajo para la protección de información e infraestructura de TI de un CSIRT.

Los autores, luego de haber realizado una revisión sistemática y un análisis de riesgos de los activos de información e infraestructura tecnológica con las que cuenta un CSIRT, han llegado a obtener como resultado, que el marco de trabajo propuesto debe cumplir con los puntos siguientes:

- Establecer una modelo organizacional acorde a la misión y objetivos del CSIRT.

- Determinar los recursos e infraestructura tecnológica necesaria para la operación del CSIRT.
- Implantar las mejores prácticas en temas de seguridad para los recursos del CSIRT (por ejemplo, hardening, criptografía, respaldos, etc.).
- Implementar controles de seguridad acorde a estándares como la ISO 27002 con el fin de garantizar la confidencialidad, integridad y disponibilidad de información del CSIRT.
- Implementar políticas de (seguridad de la información, gestión de incidentes, tratamiento de información, respaldo, borrado seguro, etc.).
- Implementar metodologías para la gestión de riesgos.

Con los resultados expuestos, finalmente los autores llegan a la conclusión de que, así como los sistemas informáticos han tenido un gran crecimiento, también han surgido grandes problemas tanto para los usuarios como para las organizaciones debido al incremento de ciberataques, sin embargo, aquello ha generado la necesidad de crear equipos de respuesta a incidentes de seguridad informática a nivel local y global, los cuales han sido adoptados por diferentes países como una estrategia de ciberseguridad para prevenir y gestionar incidentes cibernéticos. Estos CSIRT desde el punto de visto de los autores, deben ser provistos por sus organizaciones mediante la implementación y aplicación de controles de seguridad, con el fin de minimizar el riesgo tecnológico que se puede producir en el entorno de estos equipos.

Es importante mencionar que las investigaciones revisadas fueron relevantes para el inicio de esta investigación, tanto por el contenido, así como por los resultados a los que llegaron los autores, y que son relacionados y sirven como base para el desarrollo del presente proyecto.

CAPÍTULO II

MARCO TEÓRICO

En este capítulo se describen los conceptos más relevantes relacionados a un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), siendo esta terminología y conceptualización vital para entender el presente trabajo.

2.1.Seguridad informática

La seguridad informática es el arte o la práctica de proteger un sistema informático y preservar la confidencialidad, integridad y disponibilidad de los recursos de un sistema de información, esto incluye (hardware, software, firmware, datos). Esta definición (Stallings and Brown 2015) que también está basada en el manual de seguridad informática del NIST nos introduce a las tres propiedades que tiene la información como lo son:

- **Integridad**: Implica que la información no sea modificada ni destruida garantizando la autenticidad y no repudio.
- **Disponibilidad**: Garantiza el acceso oportuno y confiable a la información. Una pérdida de disponibilidad es la interrupción de acceso a un servicio o un sistema.
- **Confidencialidad**: Permite resguardar y restringir el acceso a la información o su divulgación, evitando que personas, entidades y/o procesos sin autorización accedan a ella.

Estos conceptos referentes a las propiedades de la información son vitales en el campo de la seguridad informática y la gestión de incidentes, esto con la finalidad de que los activos de información Institucionales cumplan con los estándares adecuados de seguridad, integridad y confidencialidad. Además que son fundamentales e introductorios a la gestión de incidentes cibernéticos (Tejada 2015).

2.2.Incidentes de seguridad informática

Organizar una respuesta o gestión a incidentes cibernéticos de manera efectiva implica una serie de acciones a efectuar. Una de las primeras y muy importantes a considerar es tener una definición clara y especifica del término incidente. Para que el alcance de este término sea claro,

las organizaciones deben definir y decidir qué servicios va a proporcionar el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), considerando la estructura organizacional y modelo gerencial del equipo. La creación de políticas y procedimientos, así como un plan de respuesta a incidentes es una parte vital en la creación de un equipo, por lo que estas políticas deben ser claras y deben reflejar las interacciones con otros equipos de gestión de incidentes, tanto internos como externos, con la finalidad de que la respuesta a un incidente de seguridad informática se realice de manera efectiva y eficiente (Cichonski et al. 2012).

Partiendo de esta conceptualización, los ataques informáticos con frecuencia comprometen los sistemas y datos, tanto personales como organizacionales, y es primordial responder a estos incidentes de manera rápida y efectiva. Uno de los beneficios de la capacidad de respuesta es que permite responder a los incidentes de seguridad de manera sistemática, es decir, siguiendo una metodología consistente de manejo de incidentes con el fin de tomar las medidas apropiadas y uniformes.

La respuesta a incidentes proporciona al personal, la ayuda para minimizar de manera rápida y eficaz la interrupción de servicios institucionales, así como evitar pérdida o robo de información al ocasionarse un incidente. Otro beneficio de la respuesta a incidentes es usar la información obtenida durante un incidente para prepararse a incidentes futuros. La capacidad de una respuesta a incidentes también ayuda a preparar la evidencia y a tratarla de manera adecuada cuando existan o se generen problemas legales durante o posterior a la ocurrencia de un incidente de seguridad.

2.2.1. Terminología

Evento. - Un evento es cualquier ocurrencia observable en un sistema o en la red (Mellon 2015). Los eventos ocurren cuando un usuario comparte archivos, utiliza recursos de los

sistemas, envía o recibe correos, cuando un servidor recibe solicitudes de conexión, o cuando un firewall bloquea intentos de conexión a recursos no autorizados, etc.

Evento de seguridad. - Es un evento u ocurrencia en un sistema y que es relevante para la seguridad de los sistemas y que ocasiona una excepción al normal funcionamiento de los servicios e infraestructura tecnológica (Mellon 2015).

Incidente de seguridad informática. - Es un evento de seguridad que implica la violación o amenaza inminente a las políticas de seguridad informática de una empresa lo cual puede comprometer significativamente las operaciones del negocio (Cichonski et al. 2012), no obstante, no todos los eventos se convierten en incidentes.

2.2.2. Señales e indicios de incidentes

Existen diferentes tipos de señales e indicios que permiten la identificación de incidentes de seguridad, entre los más comunes se cuenta con: alertas de software de seguridad, log de eventos, información disponible públicamente e información de personas (Cichonski et al. 2012), esto acorde lo detallado en la Tabla 2.

Tabla 2. Indicadores de Incidentes

Item	Descripción
	Alertas
IDS / IPS	Los IDS/IPS son sistemas que identifican eventos sospechosos, los registran y emiten alertas, en estas alertas se encuentran incluidos datos como la fecha y hora del evento, tipo de ataque, dirección IP de origen y destino, la mayoría de estos sistemas utilizan firmas para identificar los ataques por lo que es recomendable mantener actualizadas las firmas.
SIEM	Los SIEM son sistemas similares a los IDPS, sin embargo, los SIEM hacen correlación de eventos para generan alertas basadas en un análisis de datos registrados.
Antivirus / Antispam	Los sistemas Antivirus se encargan de detectar varios tipos de malware, generan alertas y a la vez evitan que los hosts se infecten. Los sistemas Antispam se encargan de analizar, detectar y restringir que llegue correo basura a los buzones de correo.

Software de control de integridad	Los softwares de control de integridad detectan cambios realizados en los archivos durante la ocurrencia de un incidente, para esta comprobación se utiliza un algoritmo hash con el fin de obtener una verificación criptográfica de cada fichero.
Monitorización de terceros	Los terceros ofrecen una variedad de servicios de monitoreo ya sea gratuito o basado en suscripción, entre las actividades de monitoreo se cuenta con notificaciones a las organizaciones si las direcciones IP o dominios se han visto involucrados en un incidente de seguridad en otras empresas. Otro ejemplo de monitoreo de tercero son los CSIRT que mantienen una relación de cooperación entre ellos a través de listas de correo electrónico.
Logs	
Sistemas Operativos, Servicios y logs de Aplicaciones	Los registros (logs) de los sistemas operativos, servicios y aplicaciones (en particular, los datos relacionados con auditoria) son de gran valor cuando se produce un incidente de seguridad.
Logs de dispositivos de red	Los registros (logs) de los dispositivos de red como firewalls o enrutadores, no suelen ser fuente primaria de indicadores de incidentes de seguridad, sin embargo, son muy valiosos para identificar tendencias de tráfico de red.
Network flow / Flujos de red	Los flujos de red ocurren cuando existe comunicación entre hosts, los enrutadores y otros dispositivos de red también proporcionan información de flujo de red. Esta información de flujo de red sirve para encontrar actividad anómala causada por malware u otro tipo de actos maliciosos.
Información disponible públicamente	
Información sobre nuevas vulnerabilidades y exploits	Mantenerse al día en las nuevas vulnerabilidades y exploits puede evitar que ocurran incidentes de seguridad en la organización y también ayuda a detectar y analizar nuevos tipos de ataques informáticos. La Base Nacional de Datos de Vulnerabilidades (NVD) y el CERT®/CC proporcionan periódicamente información actualizada sobre vulnerabilidades o amenazas de seguridad.
Gente	
Personas internas	Los usuarios internos como administradores de red, administradores de sistemas, responsables de seguridad y otros miembros de la organización pueden informar de posibles eventos o incidentes de seguridad, esta información proporcionada ayuda considerablemente durante el análisis de incidentes.
Personas externas	Los usuarios externos son importantes ya que pueden informar de un evento o un incidente, por ejemplo: que no se encuentre disponible el portal web o

	algún servicio que ofrece la organización, otros CSIRT también pueden informar de incidentes ocurridos externamente; por lo tanto, los informes de incidentes generados por externos deben ser tomados muy en serio por parte de las organizaciones, mismas que deben contar con los mecanismos necesarios de comunicación para receptar esta información.

Fuente: Traducido de Cichonski et al. (2012)

2.2.3. Taxonomía de incidentes

Howard and Longstaff (1998) en su estudio detallan que, como resultado del trabajo entre el Grupo de Investigación de Seguridad y Redes en los laboratorios nacionales de Sandia y el CERT®/CC Centro Coordinador, de la Universidad Carnegie Mellon, se desarrolló un conjunto de terminología de alto nivel y una estructura que indica su relación taxonómica con la finalidad de que pueda ser utilizada para clasificar y comprender la información sobre incidentes y vulnerabilidades de seguridad informática.

Por otra parte, Robert Vargas and Recalde Luis (2006) expresan que estas taxonomías son consideradas como elementos fundamentales para entender y clasificar la información acerca de ataques e incidentes informáticos, esto con el objetivo de gestionarlos adecuadamente. La Figura 1, presenta la taxonomía completa y/o elementos de seguridad informática aplicada en la gestión de un incidente (Uribe 2014).

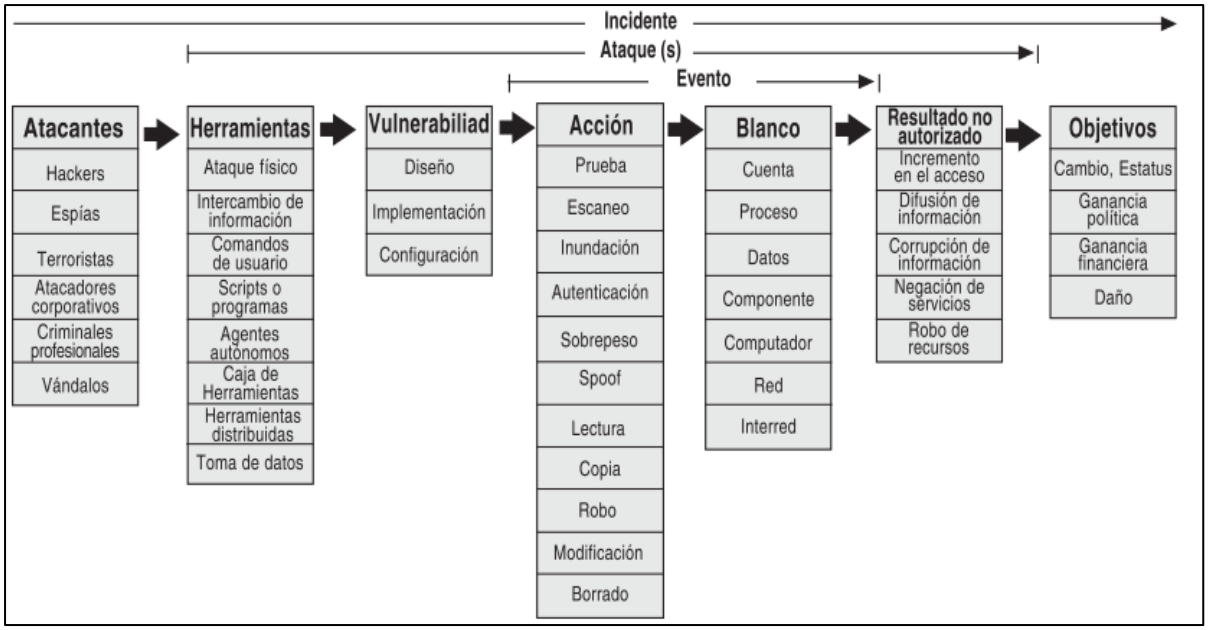


Figura 1. Ilustración de Taxonomía basada en procesos, Fuente: Vargas et al. (2017)

En la Figura 2, se visualiza la descripción de los componentes que conformar la Taxonomía descrita en la Figura 1.

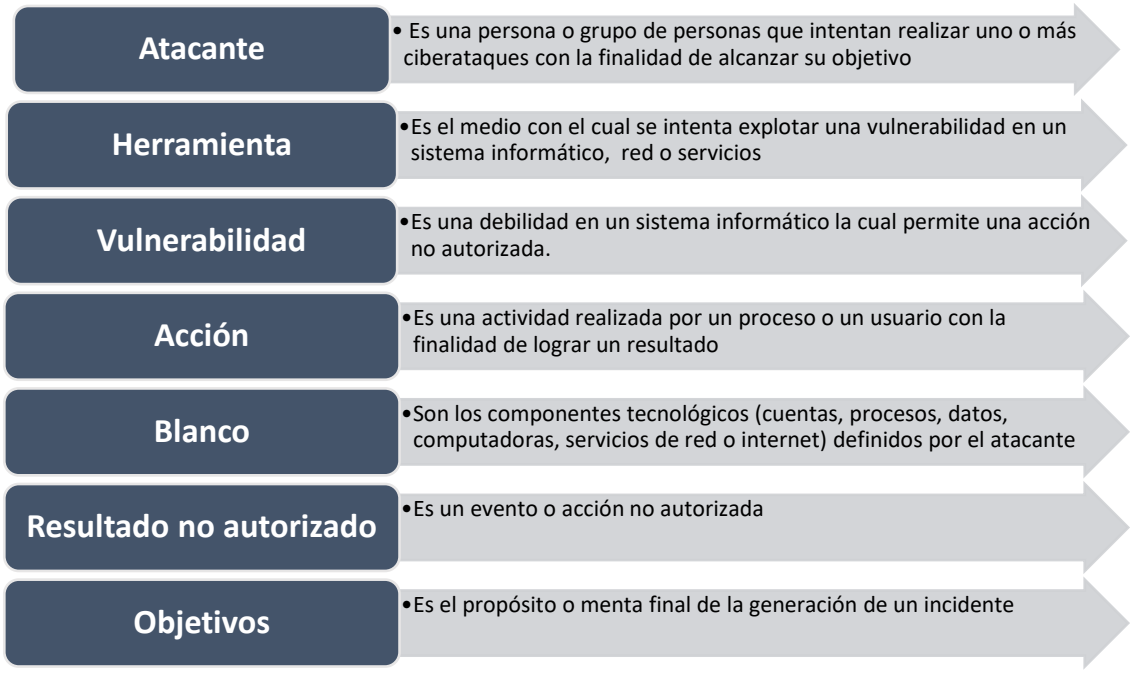


Figura 2. Descripción de los elementos de la Taxonomía, Fuente: adaptada de Vargas et al. (2017)

El éxito de un incidente se logra cuando el atacante cumple con los objetivos de este, esto significa que ha pasado por todo el proceso de la taxonomía detallada en la Figura 2.

Babulak (2011) en su estudio expresa que existen objetos vulnerables que pueden ser explotados para causar un posible incidente, entre estos objetos se cuenta con:

- Software.
- Hardware.
- Factor humano.
- Desastres naturales.

2.2.4. Manejo de incidentes

Para cumplir con el objetivo de un modelo bien planificado y estructurado que permita el manejo adecuado a la hora de realizar la gestión de los incidentes de ciberseguridad, se debe incluir los siguientes procesos: (MINTIC 2016).

- Preparación.
- Detección y Análisis.
- Contención, erradicación y recuperación.
- Actividad Post-Incidente.

2.2.5. Proceso de gestión y manejo de incidentes

El proceso de gestión y manejo de incidentes cibernéticos cuenta con cuatro fases o procesos, tal como se puede visualizar en la Figura 3.

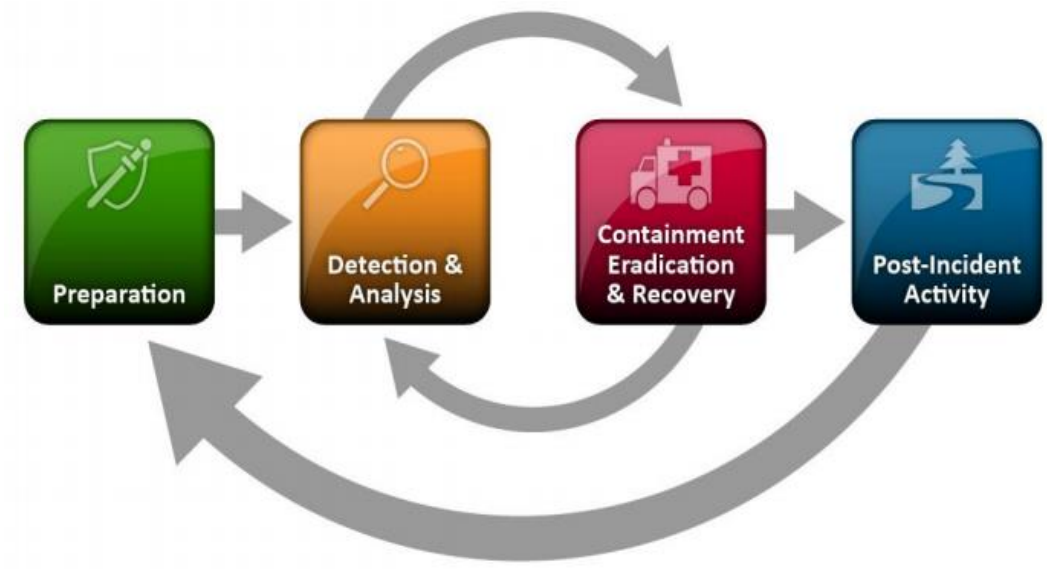


Figura 3. Fases del proceso y gestión de incidentes, Fuente: Cichonski et al. (2012).

En los siguientes apartados, se detalla cada uno de los procesos que involucran las cuatro fases de la gestión de respuesta a incidentes cibernéticos.

2.2.5.1.Preparación

La preparación es un proceso que implica; la creación y capacitación de un equipo de respuesta a incidentes de seguridad informática, y, la adquisición e implementación de herramientas necesarias para el proceso de gestión; durante esta etapa las organizaciones y/o instituciones intentan eliminar al máximo la existencia de incidentes, seleccionando e implementando controles basados en resultados del levantamiento y evaluación de riesgos, sin embargo, aunque dichos controles sean implementados, el riesgo residual persistirá inevitablemente (Cichonski et al. 2012).

Esta fase debe ser apoyada por del área de tecnologías o seguridad informática, aplicando las técnicas correspondientes con la finalidad de proteger los sistemas informáticos, aplicaciones o redes de telecomunicaciones, por ejemplo:

- Aplicación de nuevos parches de seguridad.
- Aseguramiento de las plataformas tecnológicas.
- Seguridad en redes, servidores y aplicaciones.
- Prevención de código malicioso.

Preparación para manejo de incidentes

Para preparar el equipo para el manejo de incidentes, a continuación se detallan cuatro puntos con ejemplos de recursos y herramientas disponibles que pueden llegar a ser valiosos durante el proceso de manejo de un incidente (MINTIC 2016).

1. **Recursos de comunicación**

Los recursos de comunicación son necesarios para comunicar de los incidentes atendidos, por lo que, se debe contar por lo menos con los siguientes elementos:

- Información de contacto del equipo.

- Información para escalar los incidentes.
- Política de comunicación de incidentes.

2. **Recursos tecnológicos**

Para la adecuada gestión de los incidentes cibernéticos la organización debe contar por lo menos con los siguientes elementos:

- Sistema para la gestión de tickets.
- Equipos y software de análisis forense.
- Equipos portátiles para análisis de datos.
- Software para la extracción de evidencia digital.
- Kit de respuesta a incidentes.
- Sistemas de almacenamiento externo.

3. **Recursos para el análisis de incidentes**

Para el análisis de los incidentes cibernéticos la organización debe contar por lo menos con los siguientes elementos:

- Listado de puertos conocidos y utilizados por los servicios.
- Documentación de sistemas operativos, aplicaciones, protocolos de comunicación y productos como IDS y antivirus.
- Diagramas de red y listado de activos de la organización.
- Catálogo de activos de información, sus áreas responsables y custodios.
- Hashes criptográficos de los activos de críticos información.

4. **Recursos para la mitigación y remediación**

Para mitigar y remediar un incidente, se debe contar con el acceso a imágenes de sistemas operativos, e instaladores de aplicaciones (MINTIC 2016).

2.2.5.2.Detección y Análisis

La fase de Detección y Análisis entra en acción alertando a la organización cada vez que se producen incidentes de seguridad, de acuerdo con la gravedad, la organización puede mitigar el impacto del incidente, contenerlo y finalmente recuperarse de él, sin embargo, si la gravedad de los incidentes es mayor, entra en operación la tercera fase (Cichonski et al. 2012).

Detección e Identificación

En la fase de detección, los eventos nos señalan la ocurrencia de un posible incidente de seguridad, entre los elementos más utilizados se encuentran:

- Alertas se sistemas de seguridad.
- Reporte de usuarios.
- Indisponibilidad de servicios.
- Reportes de sistemas de seguridad como antivirus e IDPS.

En esta fase existen elementos tecnológicos que nos ayudan con alertas informativas sobre la ocurrencia de un posible incidente de seguridad, estos elementos nos permiten contar con los procedimientos para minimizar el impacto de un incidente, entre los elementos que nos ayudan con la identificación se encuentran (MINTIC 2016):

- Logs de aplicaciones y servidores.
- Logs de equipos de sistemas de seguridad.
- Sistemas de visualización de eventos correlacionados – SIEM.

Vectores de Ataque

Los incidentes de seguridad pueden ocurrir de diferentes maneras, por lo que el desarrollar instrucciones para el manejo de incidentes es poco factible. Las organizaciones deberían estar preparadas para manejar cualquier tipo de incidente, además deben estar preparadas para resolver incidentes que usan vectores de ataques comunes (Cichonski et al. 2012).

Análisis de incidentes

Las actividades para el análisis de un incidente involucran una serie de componentes, por lo que es recomendable tener en cuenta lo siguiente (Cichonski et al. 2012) :

- Tener conocimiento del estado normal del tráfico de red y operación de sistemas informáticos.
- Tener conocimiento total del comportamiento de la infraestructura tecnológica.
- Toda la información para el análisis de incidentes debe estar centralizada.
- Los productos de correlación de eventos deben estar bien configurados.
- Se debe manejar una correcta base de conocimiento relacionada a incidentes de seguridad y nuevas vulnerabilidades.
- Documentar todos los incidentes ocurridos para los técnicos menos experimentados.

VI. Evaluación

La evaluación de un incidente cibernético debe estar acorde a los niveles de impacto generados a partir del análisis de riegos, estos niveles de impacto pueden ser:

Tabla 3. Niveles de impacto de un incidente

Impacto Alto	El incidente afecta activos de información que influyen directamente en los objetivos misionales de la institución
Impacto Medio	El incidente afecta activos de información que influye directamente en los objetivos de un proceso especifico
Impacto Bajo	El incidente afecta activos de información que no influyen en ningún objetivo

Fuente: MINTIC (2016)

Clasificación y priorización de un incidente

La clasificación del incidente es fundamental en la gestión de este, por lo que a continuación se lista algunos ejemplos de clasificación.

- Accesos no autorizados.
- Modificación de recursos no autorizados.
- Uso inapropiado de recursos.

- Indisponibilidad de recursos, entre otros.

La priorización de un incidente es quizás la actividad más crítica por realizar en el proceso de gestión de incidentes. Los incidentes no deben tratarse por orden de llegada, cada incidente debe ser catalogado acorde su nivel de prioridad y nivel de impacto, con la finalidad de gestionarlos de manera adecuada (análisis, contención, erradicación y recuperación) según sea el caso. La priorización debe manejarse en función de los factores expuestos (Cichonski et al. 2012).

2.2.5.3.Contención, erradicación y recuperación

En la fase de contención, erradicación y recuperación el propósito es mitigar el impacto del incidente conteniéndolo y finalmente recuperarse del mismo, durante esta fase la actividad a menudo regresa a la fase de *Detección y Análisis* después que el incidente se maneja de manera adecuada (Cichonski et al. 2012). A continuación, se describen las actividades que componen esta fase.

Contención. – Esta actividad tiene como objetivo detectar el incidente con la finalidad de que no se propague y pueda generar más impacto negativo a la infraestructura tecnológica de la organización (MINTIC 2016). En la Tabla 4, se detalla un ejemplo de estrategia para la contención de incidentes

Tabla 4. Ejemplo de estrategia de contención de incidentes

Tipo de incidente	Detalle del incidente	Actividad de contención
Reconocimiento	Escaneo de puertos abiertos en un sistema.	Bloqueo de paquetes a través de reglas en el firewall.
Acceso no autorizado	Cuenta de súper usuario comprometida.	Desconexión de la red del sistema informático y/o suspensión temporal de credenciales de acceso.

Fuente: Elaborado por el investigador

Se debe tener presente que, las estrategias en la etapa de contención varían según el tipo de incidente.

Erradicación y Recuperación. – una vez que se ha logrado la contención de un incidente se procede con la acción de erradicar y eliminar todo tipo de rastro y actividad dejado por este, y finalmente se concluye con la recuperación y restauración de los servicios o sistemas afectados (MINTIC 2016). En las Tablas 5 y 6, se detalla un ejemplo de estrategias para la erradicación y recuperación de un incidente.

Tabla 5. Ejemplo de estrategia de erradicación de incidentes

Tipo de incidente	Detalle del incidente	Actividad de erradicación
Ataque de hombre en el medio (MITM)	Interceptación y alteración de mensajes en la red de datos.	Implementar comunicaciones cifradas punto a punto.
Intrusión	Ransomware (secuestro de datos).	Aislamiento, formateo seguro del equipo y recuperación de respaldos.

Fuente: Elaborado por el investigador

Tabla 6. Ejemplo de estrategia de recuperación ante incidentes

Tipo de incidente	Detalle del incidente	Actividad de recuperación
DDoS - Denegación de Servicios	Inundación de paquetes ICMP Echo request (ICMP Flood).	Restauración del servicio web.
Defacement	Modificación de una página web sin autorización.	Arreglo de la página web / Restauración de respaldos.

Fuente: Elaborado por el investigador

Si un incidente afecta gravemente un determinado servicio o sistema, puede verse la necesidad de activar el plan de continuidad del negocio, mismo que debe estar establecido y probado en la organización, en relación con la gestión de riesgos que enfrentan sus activos y sistemas de información.

2.2.5.4.Actividades posteriores al incidente

En la fase de Actividades Post-Incidente la organización emite un informe detallado con las causas del mismo, la solución, los pasos y procedimientos que la organización debe realizar para prevenir incidentes futuros (Cichonski et al. 2012). Las actividades posteriores a un

incidente se componen básicamente de las lecciones aprendidas y el reporte, esto con la finalidad de mejorar el tiempo de respuesta y entrenar al equipo en incidentes similares.

2.2.6. Matriz de clasificación de incidentes

Parte importante de la categorización de un incidente es tener claro como clasificarlos, es por ello que en la Tabla 7, se detalla una de las taxonomías de clasificación de los incidentes de seguridad informática más comunes (ENISA 2018).

Tabla 7. Matriz de clasificación de Incidentes

Clasificación del incidente	Tipo de incidente	Descripción
Contenido Abusivo	Spam	Correo masivo no deseado, esto significa que el destinatario no ha autorizado para que un mensaje sea enviado y mucho menos que se envíen grupos masivos de mensajes, todos con un contenido similar.
	Difamación	Desacreditación o discriminación de alguien (por ejemplo, acoso cibernético, racismo, etc.).
	Pornografía infantil / Contenido sexual / Violencia	Pornografía infantil, glorificación de la violencia.
Código Malicioso	Virus	Software que se incluye o se instala intencionalmente en un sistema con un propósito dañino.
	Gusanos	
	Troyanos	
	Malware	
	Spyware	
	Dialler	
	Rootkit	
Recopilación de Información	Escaneo de servicios y puertos (Scanning)	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Esto incluye también algún tipo de prueba para recopilar información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT), escaneo de puertos.
	Análisis de paquetes (Sniffing)	Observar y registrar del tráfico de red (escuchas telefónicas).
	Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
Intentos de Intrusión	Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, buffer overflow, backdoor, cross site scripting, etc.).
	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
	Nueva firma de ataques (ataques desconocidos)	Un intento de usar un exploit desconocido.
Intrusión	Compromiso de cuentas con privilegios	Comprometer de manera exitosa un sistema o aplicación (servicio). Esto puede haber sido causado remotamente por una

	Compromiso de cuentas sin privilegios Aplicaciones comprometidas	vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet.
	Bots	
Disponibilidad	Ataques DoS/DDoS	En este tipo de ataques, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla. Algunos ejemplos de DDoS son: ICMP flood attack, inundaciones SYN, ataques de teardrop y bombardeos de mails. Los DDoS a menudo se basa en ataques que se originan en botnets, pero también existen otros escenarios como ataques de amplificación DNS, sin embargo, la disponibilidad también se puede ver afectada por acciones como: interrupción del suministro de energía, fallas espontáneas y error humano sin mala intención o por negligencia.
	Sabotaje	
	Intercepción de información	
Seguridad / Confidencialidad de la información	Acceso a información no autorizada	Además del acceso local a los datos y sistemas, la seguridad de la información puede verse amenazada debido a que una cuenta o una aplicación hayan sido comprometidas de manera exitosa. Por otra parte, los atacantes pueden tener la posibilidad de interceptar y acceder a la información durante la transmisión mediante escuchas telefónicas, spoofing o hijacking. El error humano, las configuraciones y el software también puede ser causa de este tipo de incidentes.
	Modificación de información no autorizada	
	Uso no autorizado de recursos	Uso de recursos para fines no autorizados, incluidas empresas con fines de lucro (por ejemplo, el uso del correo electrónico en actividades ilegales o esquemas piramidales).
Fraude	Derechos de autor (Copyright)	Ofrecer o instalar copias de software comercial sin licencia u otros materiales protegidos por derechos de autor.
	Falsificación de registros o identidad	Tipos de ataques en los que una entidad asume ilegítimamente la identidad de otra para beneficiarse de ella.
	Suplantación de identidad (Phishing)	Ataque que permite hacerse pasar por otra entidad con la finalidad de persuadir al usuario de que revele una credencial privada.
Vulnerable	Sistemas y/o software Abiertos	Sistemas «Open Resolvers», impresoras abiertas a todo el mundo, vulnerabilidades detectadas con Nessus u otros aplicativos, firmas de virus no actualizadas, etc.
	Servicios con acceso potencial no deseado	Servicios y protocolos no seguros, por ejemplo: Telnet, FTP, RDP, VNC.
Otros	APTs	Amenazas persistentes avanzadas dirigidos contra organizaciones, sofisticadas y bien planificadas.
	Ciberterrorismo	Uso de las tecnologías de la información con fines de carácter terrorista.
	Todos los incidentes que no encajan en las categorías detalladas	Si el número de incidentes aumenta en esta categoría, es un indicador de que la matriz de clasificación debe ser revisada.
Test	Destinado para pruebas	Destinado para pruebas.

Fuente: Traducción realizada de ENISA (2018)

2.3.Equipos de Respuesta a Incidentes de Seguridad Informática

2.3.1. ¿Qué es un CSIRT?

CSIRT son las siglas de "Computer Security Incident Response Team" también conocido en español como "equipo de respuesta a incidentes de seguridad informática". CSIRT es el término más utilizados a nivel global y principalmente en Europa (Agarwal 2016) ya que el término "CERT" no se lo puede utilizar, debido a que está protegido con derechos de autor en EEUU por el CERT/CC de la Universidad Carnegie Mellon (ENISA 2006). En la actualidad existen diferentes abreviaturas y términos que se utilizan en todo el mundo para describir un equipo de respuesta a incidentes, en la Tabla 8, se detalla algunos de los términos más utilizados (Ruefle 2007).

Tabla 8. Abreviaturas y términos de equipos de respuesta a incidentes

SIGLAS	SIGNIFICADO	SIGNIFICADO
CERT/CC	Computer Emergency Response Team Coordination Center at Carnegie Mellon University	Equipo de respuesta a emergencias informáticas Centro de Coordinación de la Universidad Carnegie Mellon
CSIRT	Computer Security Incident Response Team	Equipo de respuesta a incidentes de seguridad informática
CSIRC	Computer Security Incident Response Capability or Center	Centro o capacidad de respuesta a incidentes de seguridad informática
CIRC	Computer Incident Response Capability or Center	Capacidad o centro de respuesta a incidentes informáticos
CIRT	Computer Incident Response Team	Equipo de respuesta a incidentes informáticos
IHT	Incident Handling Team	Equipo de manejo de incidentes
IRC	Incident Response Center or Incident Response Capability	Centro de respuesta a incidentes o capacidad de respuesta a incidentes
SIRT	Security Incident Response Team	Equipo de respuesta a incidentes de seguridad

Fuente: Traducción realizada de Miora, Kabay, and Cowens (2014)

Dependiendo de la estructura y misión de la organización, algunos equipos de respuesta a incidentes tienen un título más amplio acorde su alcance.

2.3.2. Historia y evolución de los CSIRT

En noviembre de 1988 ocurrió un evento trascendental en la infraestructura global de TI, apareció el gusano llamado "*Gusano Morris*" el cual ocasionó un incidente de seguridad informática que puso de rodillas a partes importantes del internet (FIRST, 2019), este gusano

tuvo una propagación extremadamente rápida infectando numerosos sistemas de TI a nivel mundial.

La gestión a este incidente fue aislada y descoordinada, lo que resultó en duplicación de esfuerzos y en soluciones conflictivas. Así, semanas después del "*Incidente Morris*", se creó el primer CSIRT en la Universidad Carnegie Mellon en Pittsburgh, denominado CERT/CC (ENISA 2006). La misión del CERT/CC era actuar como un nodo central en una red de respuesta a incidentes, mediante la difusión y notificación rápida sobre incidentes y la coordinación de la comunicación durante las emergencias de seguridad informática.

En los años posteriores, la cantidad de equipos de respuesta a incidentes de seguridad cibernética continúo creciendo, cada uno con sus propios propósitos y financiamiento, sin embargo, la coordinación y comunicación de estos CSIRT experimentó dificultades debido a diferencias del idioma y zona horaria.

En octubre de 1989, se generó un nuevo incidente cibernético conocido a nivel global como "*Gusano Wank*", el cual puso en descubierto la necesidad de establecer una mejor comunicación y coordinación entre estos equipos, por lo que, en 1990 se crea el Foro global de respuesta a incidentes y equipos de seguridad (FIRST) en respuesta a este incidente (FIRST 2019b). Estos son los orígenes de una comunidad de equipos de respuesta a incidentes que ha crecido a más de 500 miembros del FIRST (ver Figura 4), y a más CSIRT no miembros de FIRST en todo el mundo.

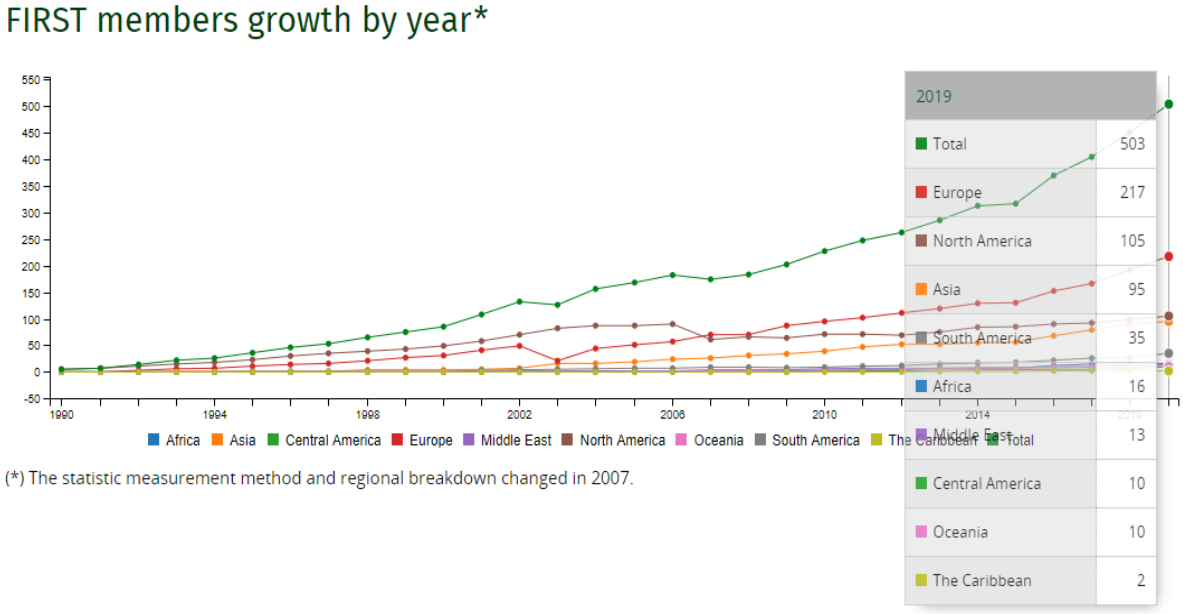


Figura 4. CSIRT miembros de FIRST por región, Fuente FIRST (2019)

En muchos países, los CSIRT surgieron por primera vez como parte de la academia y como redes de investigación, y no en el gobierno ni en las empresas privadas (Skierka et al. 2015).

Después de la primera ola de creación de CSIRT que alcanzó su punto máximo en la década de los noventa, comenzaron a surgir nuevos equipos de respuesta a incidentes en empresas privadas y gubernamentales. En 1996 y 1997 en Asia y América se comenzaron a crear CSIRT financiados por el gobierno, estos primeros CSIRT tenían poca autoridad, solo podían emitir alertas y recomendación a sus organizaciones; sin embargo, a medida que más organizaciones crearon CSIRT, muchos de estos equipos fueron tomando facultades para la toma de decisiones y para manejarse de manera autónoma (Skierka et al. 2015).

Con el creciente interés público y político en el campo de la ciberseguridad, en los países desarrollados los CSIRT también han comenzado a recibir más fondos de fuentes públicas y privadas. Si bien, la financiación sigue siendo un problema para muchos equipos de respuesta a incidentes, una mayor atención política a los incidentes de ciberseguridad que afectan tanto al sector privado, público y especialmente a la ciudadanía, ha llevado a una creciente inversión en equipos de respuesta a incidentes.

Las discusiones internacionales sobre políticas públicas de ciberseguridad incluyen referencias al establecimiento de CSIRT en cada uno de los países, como parte de estas discusiones se encuentra la implementación de normas y desarrollo de capacidades en seguridad informática y respuesta a incidentes.

A nivel mundial, FIRST sigue siendo el foro principal para la coordinación e implementación de buenas prácticas de CSIRT. Para convertirse en un miembro de FIRST, los CSIRT deben pasar por un procedimiento de validación de requisitos acorde la estándar RFC 2350 (FIRST 2019b).

2.3.3. Estándares y buenas prácticas

Desde la creación del primer CSIRT en la Universidad Carnegie Mellon y su posterior repunte y creación de centros de respuesta a incidentes cibernéticos a nivel global, organismos como The Internet Engineering Task Force (IETF) comenzaron a generar documentación técnica que definía estructuras, procesos, políticas y procedimientos a seguir; estos documentos actualmente se los conoce como Request for Comments (RFC), los cuales definen protocolos, conceptos, métodos y programas de Internet (Campis et al. 2015); algunos incluso han sido aprobados oficialmente como estándares.

A nivel de documentación, procedimientos y estándares que orientan a organizaciones, entes gubernamentales y grupos de investigación a la creación de equipos de respuesta a incidentes de seguridad informática, existen diferentes tipos de documentos definidos y enumerados por el RFC; uno de ellos es el “RFC 2350: Expectativas para la respuesta a incidentes de seguridad informática”, que se caracteriza por proporcionar un marco de trabajo para presentar los temas importantes relacionados a incidentes cibernéticos y que en la actualidad son de interés para toda la comunidad en Internet (Brownlee and Guttman 1998). El documento pone a disposición del público una plantilla que comprende: la constitución, políticas y procedimientos que los CSIRT deben cumplir, con la finalidad de proporcionar información detallada a sus clientes,

logrando con esto que su comunidad objetivo tenga claro los servicios a recibir por parte del equipo de respuesta a incidentes.

2.3.4. Definición formal de un CSIRT

Un CSIRT es un equipo dentro de una organización privada o pública que ofrece servicios a un grupo de clientes en particular (comunidad objetivo) tanto internos como externos, con la finalidad de prevenir, gestionar y responder a incidentes de seguridad cibernética. Estos equipos normalmente están conformados por especialistas multidisciplinarios y actúan acorde las políticas y procedimientos ya establecidos, con el fin de responder adecuadamente a un incidente cibernético (OEA 2016).

2.3.5. Ventajas de un CSIRT

Contar con un CSIRT ayuda a las organizaciones a mitigar y evitar incidentes graves de ciberseguridad que puedan afectar los objetivos misionales de la institución, entre las ventajas que se puede obtener se encuentran (ENISA 2006):

- Disponer de una coordinación centralizada para los eventos relacionados a la seguridad cibernética dentro de la organización.
- Reaccionar de manera eficaz y oportuna ante un incidente de seguridad.
- Contar con los cocimientos técnicos necesarios para apoyar en la recuperación rápida de un incidente de seguridad informática.
- Proteger las pruebas y cadena de custodia ante un incidente cibernético.
- Realizar seguimiento a los avances obtenidos en temas de ciberseguridad.
- Fomentar la cooperación con otros equipos de respuesta a incidentes.

2.3.6. Tipos de CSIRT

Previo a la creación de un CSIRT es esencial y fundamental tener claro que lo más importante es la comunidad objetivo (clientes) a la que se prestará los servicios, esta comunidad objetivo es el factor primordial para la clasificación de los CSIRT (ENISA 2006), por lo tanto,

en los siguientes apartados se describe algunos de los principales tipos de clasificación de CSIRT con la finalidad de categorizar y definir a sus clientes (OEA 2016).

CSIRT Académicos

Los CSIRT académicos prestan servicios y atienden a las comunidades académicas como centros de investigación, universidades, facultades, institutos, etc.

CSIRT Comerciales

Los CSIRT comerciales prestan servicios particulares a sus clientes y se rigen normalmente por acuerdos de nivel de servicio (SLA). Estos CSIRT ofrecen servicios de análisis, detección y prevención de ciberataques a sus clientes.

CSIRT Gubernamentales

Los CSIRT gubernamentales sirven a las instituciones del Estado con el fin de garantizar que la infraestructura de TI del gobierno y los servicios que les ofrecen a los ciudadanos tengan niveles de seguridad adecuados. Los CSIRT gubernamentales adaptan sus estructuras al sector del gobierno.

CSIRT Nacionales

Los CSIRT Nacionales además de servir a una comunidad definida, por lo general asumen el papel de coordinador nacional de respuesta a incidentes y es el punto de contacto para incidentes nacionales e internacionales, por ejemplo, en Ecuador se cuenta con el EcuCERT.

CSIRT del sector militar

Los CSIRT de tipo militar proporcionan servicios a las instituciones de defensa de un Estado. Sus actividades se limitan generalmente a la defensa cibernética.

2.3.7. Servicios de un CSIRT

Los CSIRT tienen la facultar de ofrecer diferentes tipos de servicios, acorde su estructura, comunidad objetivo, misión, visión, recursos, etc., sin embargo, ningún CSIRT hasta la fecha ha logrado ofrecer todos los servicios catalogados por el FIRST y otros organismos

internacionales, por lo que la selección de los servicios a ofrecer es vital en el éxito y accionar de un CSIRT (ENISA 2006).

Por lo expuesto, en la Figura 5 y en la Tabla 9, se visualiza una colección de servicios de seguridad cibernética separado por áreas, con la finalidad de que los CSIRT puedan brindar los servicios adecuados de gestión de incidentes de cada organización acorde sus objetivos (Cristine 2019). Estos servicios se encuentran basados en el marco de trabajo de servicios de un CSIRT del FIRST "CSIRT Services Framework", el cual es una recopilación de las mejores prácticas y estándares a nivel global (FIRST 2019a).

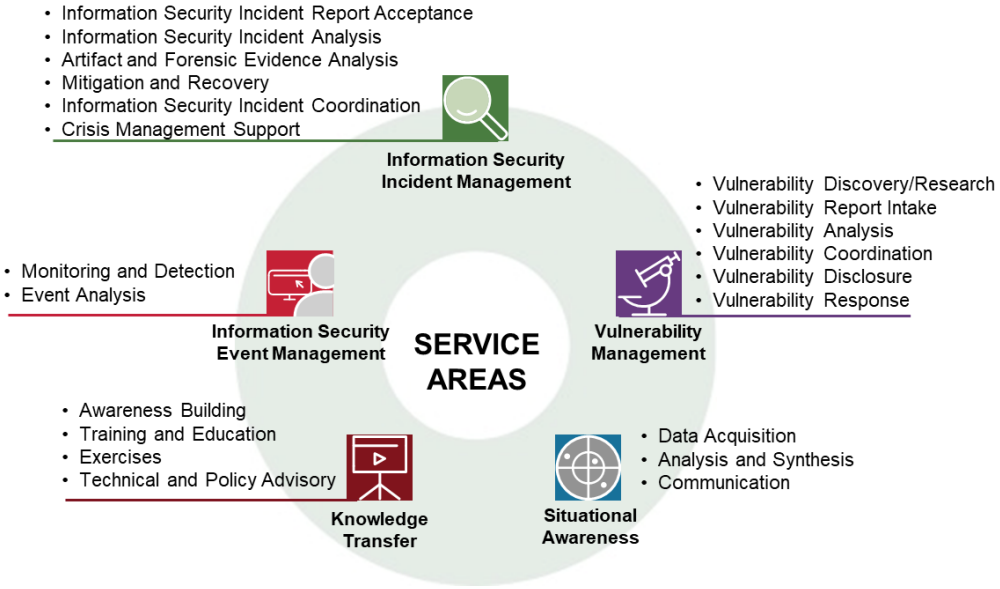
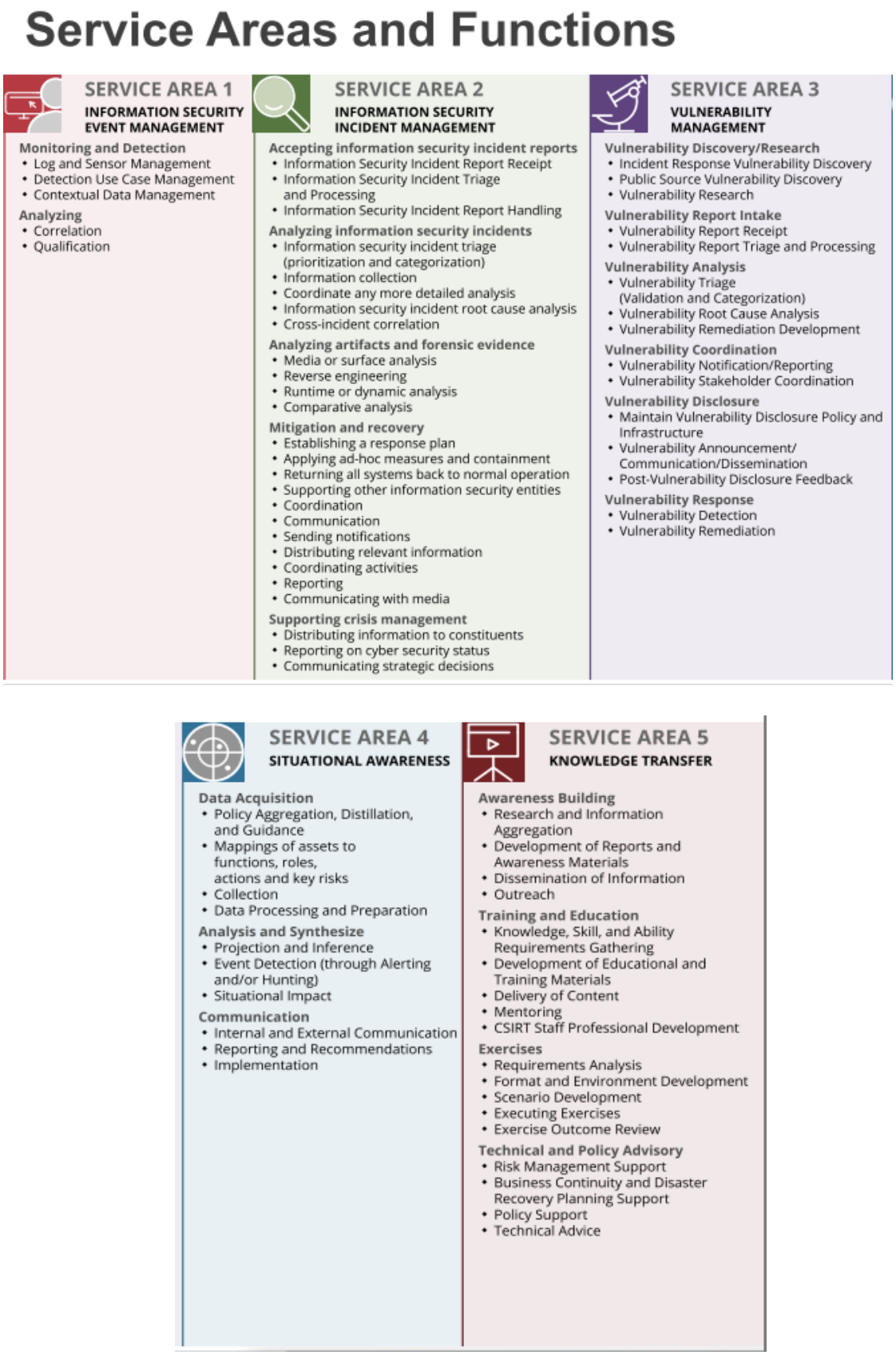


Figura 5. Servicios de un CSIRT por áreas, Fuente: FIRST and Cristine (2019)

Tabla 9. Servicios de un CSIRT por áreas y funciones



Fuente: Cristine (2019)

2.3.8. Centros de coordinación y comunicaciones CERT'S

Uno de los grandes problemas detectados entre los CSIRT es la comunicación y la coordinación al momento de la mitigación de un incidente, es por ello por lo que a nivel global existen centros coordinadores de gran renombre que facilitan estas actividades, estos centros coordinadores se encuentran distribuidos por regiones, acorde los siguientes apartados.

2.3.8.1.FIRST

El Foro Mundial de Respuesta a Incidentes y Equipos de Seguridad (FIRST) es una organización reconocida a nivel mundial como líder en coordinación y comunicaciones de respuesta a incidentes cibernéticos. Ser miembro de FIRST permite a los CSIRT tener la ventaja de responder de manera rápida y eficiente a incidentes cibernéticos mediante el acceso a información técnica, herramientas, metodologías, procesos y mejores prácticas desarrolladas entre los miembros del FIRST (FIRST 2020d).

En la Figura 6, se pude visualizar en color verde los países que cuentan con al menos un CSIRT registrado en el FIRST, y se observar que Ecuador cuenta actualmente con 7 equipos miembros.

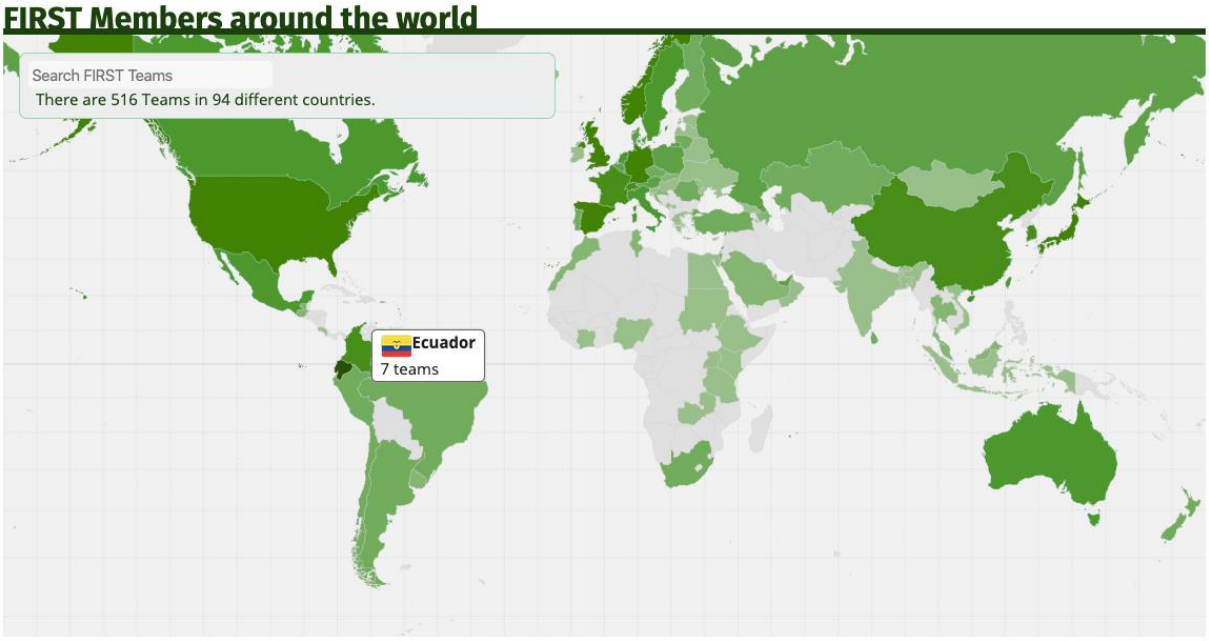


Figura 6. Miembros de FIRST alrededor del mundo, Fuente: FIRST (2019)

2.3.8.2.ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la organización que trabaja para garantizar la seguridad cibernética en Europa desde el 2004, trabaja en estrecha colaboración con sus países miembros y otras partes interesadas para ofrecer soluciones y asesorías en temas relacionados a la ciberseguridad; también apoya a mejorar la gestión de respuesta a incidentes o crisis de seguridad cibernética transfronteriza a gran escala y, desde 2019, ha estado elaborando esquemas de certificación de seguridad cibernética (ENISA 2020).

2.3.8.3.APCERT

El APCERT es una integración entre un equipo de respuesta de emergencias informáticas (CERT) y un equipo de respuesta a incidentes de seguridad informática (CSIRT) (Uribe 2014). El APCERT trabaja para ayudar a crear un ciberespacio seguro, limpio y confiable en Asia a través de la colaboración global de equipos de respuesta a incidentes (APCERT 2020).

2.3.8.4.LACNIC CSIRT

El proyecto para la constitución del CSIRT de LACNIC surge ante la creciente demanda de la comunidad técnica y frente a la madurez alcanzada por los servicios que hasta el momento eran prestados por el WARP de LACNIC a sus miembros, en marzo de 2020 se constituye el CSIRT de LACNIC con la finalidad de consolidar el trabajo profesional del proyecto WARP que durante sus cinco años de existencia gestionó y coordinó más de 600 incidentes informáticos en América Latina y el Caribe (LACNIC 2020).

El CSIRT de LACNIC tiene como misión ser la organización encargada de coordinar las actividades necesarias para el fortalecimiento de la gestión de respuesta a incidentes cibernéticos vinculados a los recursos de internet (IPv4, IPv6) en el marco del fortalecimiento de una Internet segura, estable, abierta y en continuo crecimiento para los países latinoamericanos (C. LACNIC 2020).

Por el trabajo en ciberseguridad, el CSIRT de LACNIC se ha integrado a la élite mundial de las entidades dedicadas a la ciberseguridad, firmando acuerdos de cooperación con organizaciones cómo: FIRST.org, CERT.br, entre otras (LACNIC 2020).

CAPÍTULO III

ANÁLISIS DE SITUACIÓN ACTUAL

El capítulo presenta un estudio documental de casos de éxito de la implementación de centros de respuesta a incidentes cibernéticos en Latinoamérica a nivel de Estado, así como el estudio de la situación actual de la Fiscalía General del Estado en temas de seguridad informática, mismos que serán fundamentales para el posterior diseño del CSIRT a aplicarse en la Fiscalía General del Estado.

3.1.Estudio documental de casos de éxitos de la implementación de CSIRT

Cabe mencionar que, los CSIRT analizados en los siguientes apartados son de carácter estatal, esto debido a que, posterior a la revisión bibliográfica no se encontró información suficiente para documentar CSIRT de Instituciones Judiciales, por lo que, estos Centro de Respuesta a Incidentes analizados son lo más cercanos a una Institución del sector Justicia.

3.1.1. Implementación del EcuCERT (Ecuador)

El Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones ***EcuCERT***, fue creado el 18 de julio de 2014 mediante Resolución No. ST-2014-0247 (ARCOTEL 2017), cuya finalidad es "*Brindar a su Comunidad Objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, sensibilización y soporte técnico*" (ARCOTEL 2020).

Desde el 2 de octubre de 2014, el EcuCERT se incorpora como miembro activo al FIRST, con la finalidad de establecer y mantener una relación colaborativa con sus equivalentes a nivel nacional e internacional, así como, con organismos relacionados a la seguridad informática.(FIRST 2020c).

Por otra parte, el Ministerio de Telecomunicaciones y de la Sociedad de la información a través de su documento "*Libro Blanco de la Sociedad de la Información y del Conocimiento*" publicado en el 2018 señala que el EcuCERT es reconocido como un CSIRT nacional oficial

de acuerdo al índice mundial de ciberseguridad de la Unión Internacional de Telecomunicaciones –UIT (MINTEL 2018) .

En la actualidad el EcuCERT es el CSIRT gubernamental coordinador a nivel nacional, y aunque su comunidad objetivo está enfocado a las telecomunicaciones es un pilar fundamental cuando existen incidentes de ciberseguridad, ya que, aunque no los resuelve, es la entidad que trasmite y coordina con la fuente del incidente para su resolución (ARCOTEL 2019).

Entre los servicios que presta el EcuCERT se encuentran (EcuCERT 2020):

- Proactivos
    - Alertas y advertencias.
    - Identificación de vulnerabilidades.
- Reactivos
    - Comunicados y alertas.
    - Gestión de incidentes.
- Valor agregado
    - Sensibilización y Formación.

En la Tabla 10, se observa las estadísticas de los diferentes tipos de incidentes gestionados por el EcuCERT, estos incidentes van acorde a su comunidad objeto, la cual se enfoca en las telecomunicaciones del Ecuador.

Tabla 10. Tipos de incidentes gestionados por el EcuCERT

	#	Tipo de incidente	Total, direcciones IP
En el 2018, el CERT registró 1’609.997 direcciones IP’s comprometidas con distintos tipos de incidentes, y estos se presentan a continuación:	1	Drones_Botnet	898.512
	2	Sinkhole_HTTP	603.066
	3	Blacklisted	57.893
	4	Bruteforce	32.105
	5	Sinkhole_HTTP_IPv6	12.160
	6	Microsoft_Sinkhole	5.769
	7	Spam	245
	8	Sandbox_URL	150
	9	Compromised_website*	75
	10	CC_Server	22
		Total	**1’609.997**

Fuente: ARCOTEL (2019)

3.1.2. Implementación del ColCERT (Colombia)

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional, ***ColCERT***, surgió en el año 2008 en un taller de seguridad cibernética patrocinado por el Comité Interamericano contra el Terrorismo de la OEA (CICTE) (Mellon 2016), sin embargo, el 2011 mediante la elaboración de los *LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA* por parte del Consejo Nacional de Política Económica y Social, oficialmente es creado el ColCERT como equipo coordinador a nivel nacional en temas de seguridad cibernética (CONPES 3701 2011), cuya finalidad es "*proteger la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad y ciberdefensa que atenten o comprometan la seguridad y defensa nacional*" (ColCERT 2017), adicionalmente presta sus servicio de apoyo al Centro Cibernético Policial y al Comando Conjunto Cibernético de Colombia.

En abril de 2012, el ColCERT fue el primer equipo colombiano en ser aceptado como miembro por el FIRST, y durante ese año el ColCERT realizó talleres y seminarios de ciberseguridad y gestión de incidentes por la inclusión del equipo al FIRST (Mellon 2016), actualmente uno de sus objetivos es brindar asesoría a CSIRT's de instituciones públicas y empresas privadas para responder ante incidentes cibernéticos (ColCERT 2017) .

Entre los servicios que presta el ColCERT (Ministerio de Defensa 2017) se encuentran:

- Proactivos
    - Informes de vulnerabilidades.
    - Auditorias de seguridad y apoyo en inteligencia cibernética.
- Reactivos
    - Gestión de incidentes.
    - Alertas de nuevas vulnerabilidades.
    - Análisis de malware.

- Gestión
    - Concienciación.
    - Eventos de ciberseguridad.

En la Tabla 11 y en la Figura 7, se observa las estadísticas de incidentes gestionados por el ColCERT.

Tabla 11. Tipos de incidentes informáticos gestionados por el ColCERT

CLASIFICACIÓN DE CIBERINCIDENTES	PORCENTAJE
Intrusiones – Defacement	43,0 %
Obtención de información – Phishing	16,1 %
Código Dañino – Malware	14,6 %
Intrusiones – Explotación Vulnerabilidad	10,2 %
Intrusiones – Compromiso Aplicación	6,8 %
Criptojacking	4,7 %
Disponibilidad – Denegación [Distribuida] del Servicio DoS / DDoS	1,3 %
Intrusión – Ataque de fuerza bruta	1,3 %
Información Critica Expuesta	1,0 %
Contenido Abusivo – Spam	0,5 %
Contenido Abusivo – Pederastia	0,3 %
Disponibilidad – Fallo Hardware	0,3 %
Total	**100 %**

Fuente: Prieto (2019)

Figura 7. Clasificación de incidentes informáticos gestionados por el colCERT, Fuente Prieto (2019)

3.1.3. Implementación del CERT.br y CTIR Gov (Brasil)

Brasil cuenta con dos CSIRT nacionales de gran trascendencia.

I. CERT.br

El equipo de respuesta a emergencias informáticas de Brasil respaldado por el Comité Gestor de Internet de Brasil, ***CERT.br***, es el CSIRT responsable principalmente de manejar los incidentes cibernéticos y eventos relacionados con los sistemas y redes de seguridad del sector privado y de las universidades (OCDE/BID 2016).

Desde mayo de 2002, el CERT.br, es uno de los miembros más activos y que más apoya en la elaboración de directrices, marcos de trabajo y mejores prácticas que emite el FIRST a nivel global (FIRST 2020a). Unos de los objetivos principales del CERT.br es apoyar a los CSIRT de Brasil a establecer sus actividades en el país, con la finalidad estratégica de aumentar el nivel de seguridad y mejorar la gestión y manejo de incidentes de las redes conectadas a Internet en Brasil (CERT.br 2020).

En la Figura 8, se observa las estadísticas de incidentes gestionados por el CERT.br en los últimos 10 años.

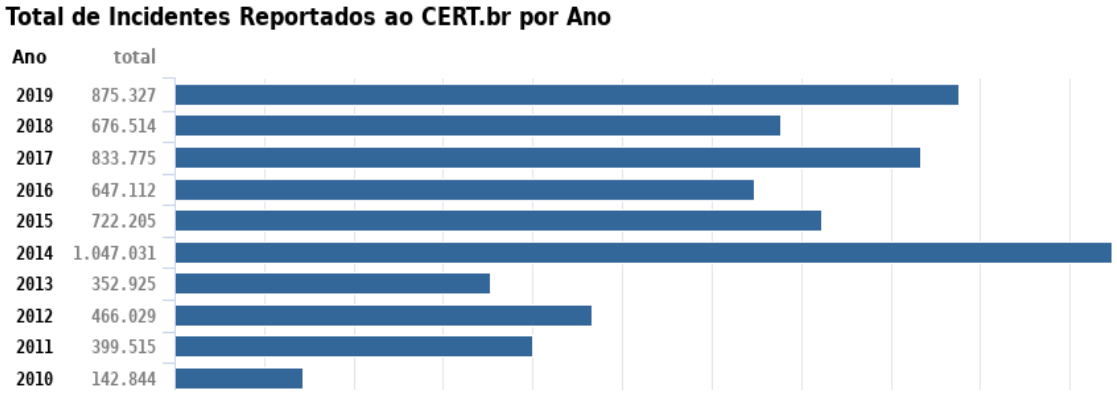


Figura 8. Tipos de incidentes informáticos gestionados por el CERT.br, Fuente: CERT.br (2020)

II. CTIR Gov

El Centro de Tratamiento y Respuesta a Incidentes Cibernéticos de Gobierno, coordinado por el Departamento de Seguridad de la Información y las Comunicaciones de la Presidencia de Brasil***, CTIR Gov***, fue creado formalmente a finales de 2004, con la finalidad principal de

"*supervisar y atender a los incidentes y amenazas a los sistemas en redes informáticas que pertenecen a la Administración Pública Federal (APF)"* (CTIRGov 2019).

Entre los servicios que presta el CTIR Gov (CTIRGov 2019) se encuentran:

- Proactivos
    - Diseminación de informaciones.
    - Recaudación de informaciones.
- Reactivos
    - Tratamiento y gestión de incidentes.
    - Análisis de eventos y patrones de actividad maliciosa.
    - Notificación de incidentes.

En las Figuras 9 y 10, se observan las estadísticas de incidentes gestionadas por el CTIR Gov de Brasil.

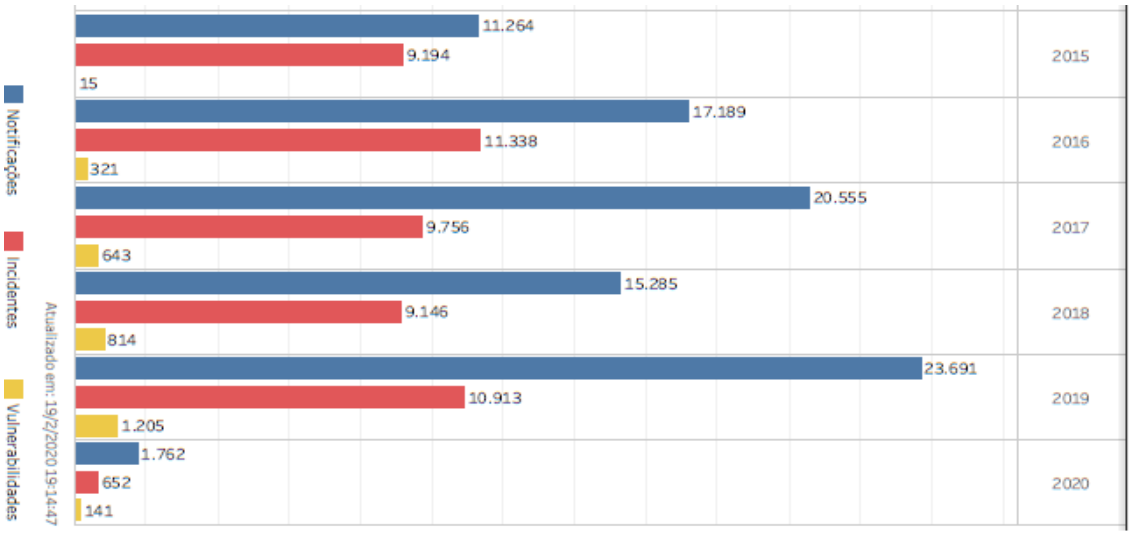


Figura 9. Número de incidentes informáticos gestionados por el CTIR Gov, Fuente: CTIRGov (2020)

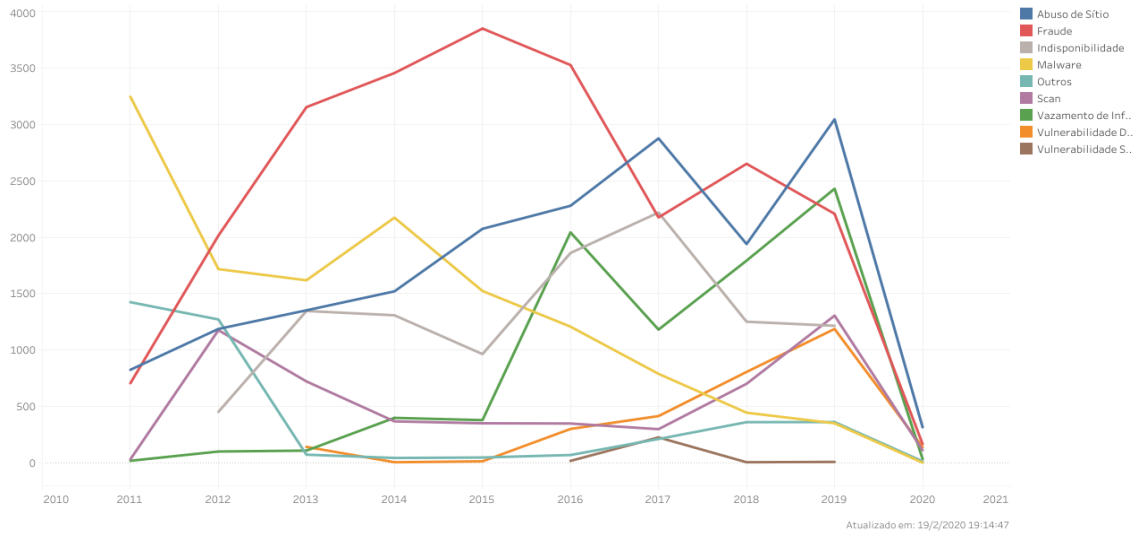


Figura 10. Tipos de incidentes informáticos gestionados por el CTIR Gov, Fuente: CTIRGov (2020)

3.1.4. Implementación del CERTuy (Uruguay)

El Centro Nacional de Respuesta de Incidentes de Seguridad Informática de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica de Uruguay, ***CERTuy***, fue creado el 6 de octubre de 2008 por medio del artículo 73 de la Ley Nro. 18.362 (IMPO 2009), cuya finalidad es: "*difundir las mejores prácticas en seguridad de los activos de información crítica y promover el conocimiento en la materia a fin de responder y prevenir incidentes de seguridad.*"

El CERTuy, desde el 11 de abril de 2014 es miembro oficial del FIRST (FIRST 2020b), y entre sus objetivos principales se encuentra la implementación de estrategias, políticas y buenas prácticas en materia de ciberseguridad y gestión de incidentes, así como fomentar la creación de otros CSIRT en Uruguay, con la finalidad de mejorar el trabajo colaborativo en temas de ciberseguridad (CERTuy 2019).

Entre los servicios que presta el CERTuy (CERTuy 2014) se encuentran:

- Proactivos
    - Gestión de incidentes (análisis forense, respuesta a incidentes on-site y remoto).
    - Monitoreo y correlación de eventos.

- Análisis y gestión de vulnerabilidades.

- Reactivos
  - Detección de anomalías.
  - Boletines de seguridad.
  - Ethical Hacking.

- Valor agregado
  - Concienciación y entrenamiento técnico.
  - Creación de CSIRTs.

En la Figura 11, se observa estadísticas sobre los tipos de incidentes gestionados por el CERTuy de Uruguay.

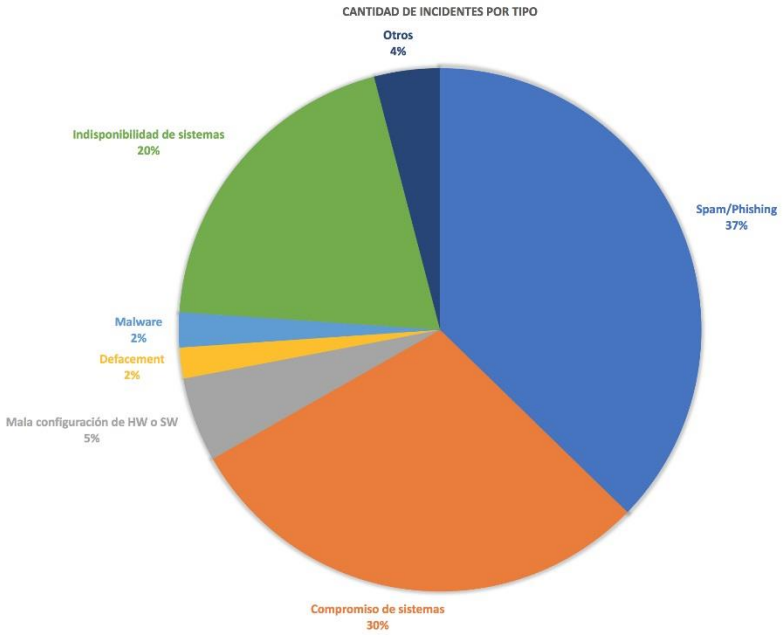


Figura 11. Tipos y porcentaje de incidentes informáticos gestionados por el CERT UY, Fuente: CERTuy (2018)

3.1.5. Implementación del CSIRT GOB CL (Chile)

El equipo de respuesta a incidentes de seguridad informática del Ministerio del interior y seguridad pública de Chile, ***CSIRT GOB CL***, fue oficializado en agosto de 2019 mediante Resolución Exenta 5.006 como un departamento dentro de la estructura del gobierno (CSIRT 2019), con la finalidad de "*promover políticas, reglamentos, planes de capacitación, difusión,*

y educación, en el marco de los objetivos planteados en la Política Nacional de Ciberseguridad" (CHILE 2019).

El objetivo estratégico que tiene el ***CSIRT GOB CL,*** es apoyar el fortalecimiento tecnológico y jurídico del Estado chileno en lo que se refiere a delitos informáticos y cibercrimen, mediante el uso de las tecnologías de la información y comunicación y la aplicación de buenas prácticas de ciberseguridad (CSIRT_GOB 2019).

Entre los servicios que presta el CSIRT GOB CL (CSIRT_GOB 2019) se encuentran:

- Proactivos
    - Gestión de incidentes.
    - Análisis de vulnerabilidades.
- Reactivos
    - Monitoreo de sitios web
    - Análisis de indicadores de compromiso (IoC, por sus siglas en inglés)
    - Boletines de seguridad
- Valor Agregado
    - Concientización

En la Tabla 12 y en la Figura 12, se observan las estadísticas de incidentes gestionados por el *CSIRT GOB CL* de Chile.

Tabla 12. Tickets sobre incidentes informáticos gestionados por el CSIRT GOB CL

Tickets	Privado	Público	Total
Recopilación de Información	0	899	899
Vulnerabilidad	150	120	270
Código Malicioso	36	181	217
Fraude	199	4	203
Disponibilidad	0	149	149
Información de Seguridad de Contenidos	78	10	88
Operaciones Ciberseguridad CSIRT	0	6	6
Contenido Abusivo	0	5	5
Intentos de Intrusión	0	2	2
Intrusión	0	0	0
TOTAL	**463**	**1376**	**1839**

Fuente: CSIRT_GOB (2020)

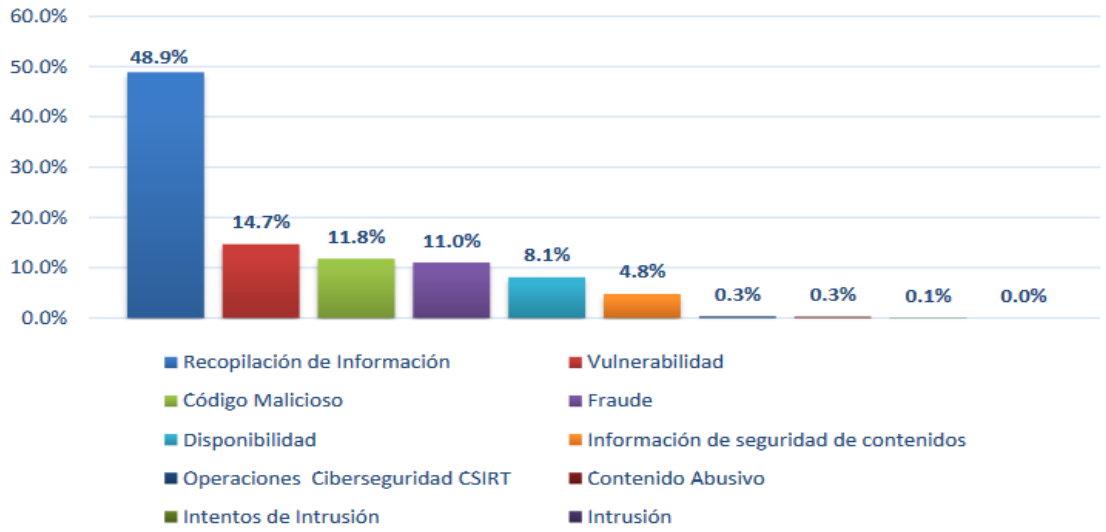


Figura 12. Porcentaje de incidentes informáticos gestionados por el CSIRT GOB CL, Fuente: CSIRT_GOB (2020)

3.2.Fiscalía General del Estado – FGE

El Art. 194, de la Constitución de la República del Ecuador en su Capítulo cuarto, Función Judicial y Justicia Indígena, Sección décima -Fiscalía General del Estado, dispone que: "*La Fiscalía General del Estado es órgano autónomo de la Función Judicial, único e indivisible, funcionará de forma desconcentrada y tendrá autonomía administrativa, económica y financiera. La Fiscal o el Fiscal General es su máxima autoridad y representante legal…*" (Nacional 2008).

Así mismo, el Art. 195 de la Constitución de la República del Ecuador determina que: "*La Fiscalía dirigirá, de oficio o a petición de parte, la investigación pre procesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal*" (Nacional 2008).

3.2.1. Misión

La Misión que la Fiscalía General del Estado se ha planteado es: "*ser una institución autónoma, que dirige la investigación preprocesal y procesal penal, procurando el acceso a la*

justicia con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas"(FGE 2020a).

3.2.2. Visión

La Visión que la Fiscalía General del Estado se ha planteado es: "*ser una institución integrada por personal especializado y comprometido en la procuración de la justicia reconocida por su lucha contra el crimen y la inseguridad, mediante la innovación de procesos y operaciones, la transparencia de la gestión y la efectividad en la reducción de la impunidad*"(FGE 2020a).

3.2.3. Estructura orgánica de la FGE

Mediante Resolución Nro. 012-FGE-2018 de 28 de febrero de 2018, subscrita por el Fiscal General, entra en vigencia el actual Estatuto Orgánico de Gestión Organizacional por Procesos de la Fiscalía General del Estado (FGE 2018). En dicha resolución se establece la estructura institucional de la Fiscalía General del Estado con la que trabaja actualmente para el cumplimiento de sus competencias, atribuciones, misión, visión, gestión de sus procesos y servicios que de estas derivan, ver Figura 13.

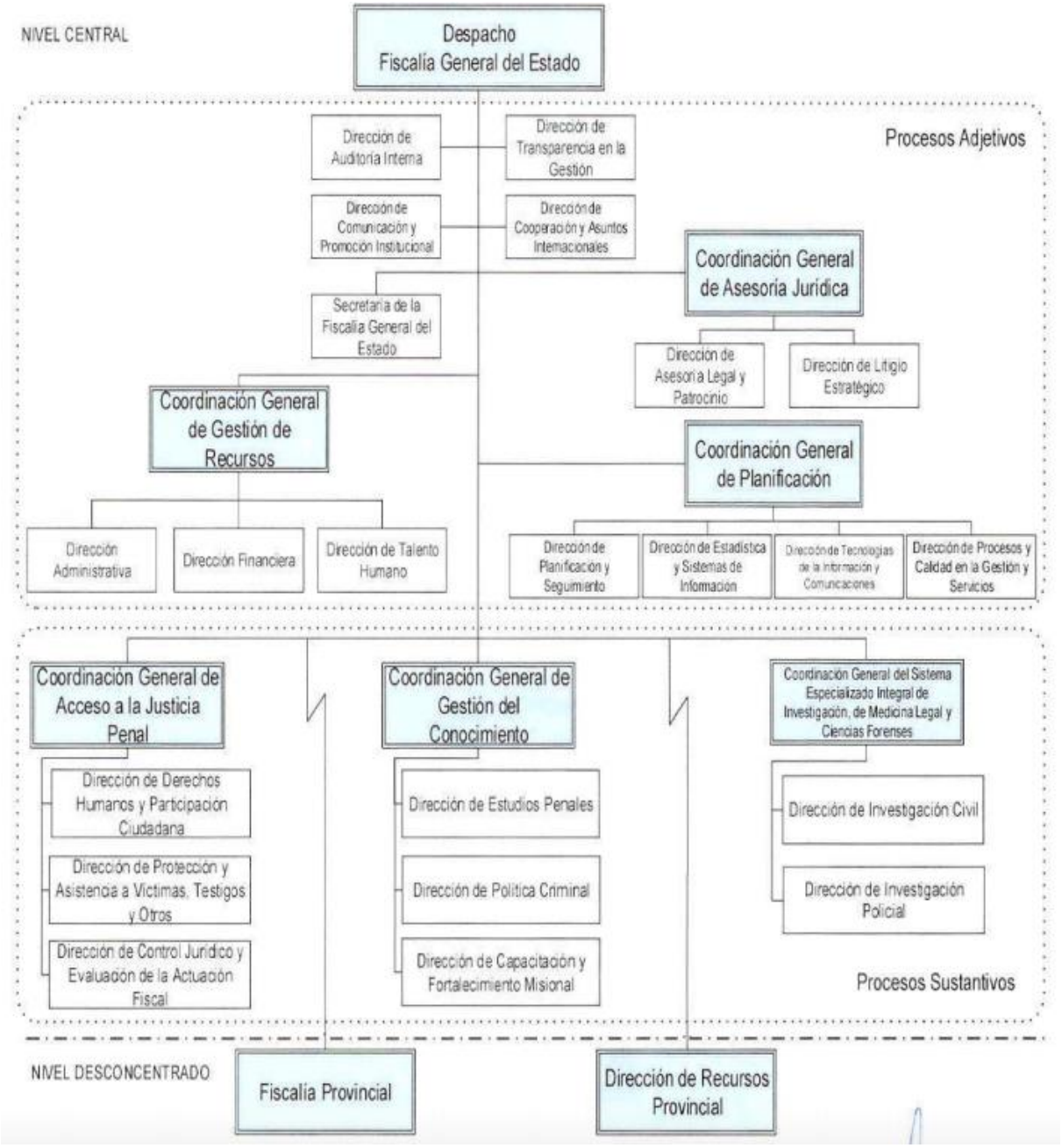


Figura 13. Estructura Organizacional de la FGE, Fuente: FGE (2018)

Como se puede visualizar en la Figura 17, la organización institucional está estructurada acorde los siguientes procesos.

- **Gobernantes**. - Aquellos que encaminan el direccionamiento estratégico de la Institución mediante la disposición de políticas y directrices.
- **Sustantivos**. - Aquellos que coordinan y articulan la misión institucional a través de la operación de directrices generadas en el ámbito de acción.

- **Adjetivos**. - Aquellos que proveen los recursos, asesoramiento y soporte de servicios a los procesos gobernantes y sustantivos.

3.2.4. Dirección de Tecnología de la información

Acorde el Estatuto Orgánico de Gestión Organizacional por Procesos, numeral 1.3.1.1.3. GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, literal a, la misión de la dirección de tecnologías de la informas es: "*mantener la Integridad, Disponibilidad, Privacidad y Control de autenticidad de la información generada por Fiscalía General del Estado a través de sistemas que permitan mantener las aplicaciones web institucionales seguras de amenazas y ataques cibernéticos*" (FGE 2018).

De entre las atribuciones y responsabilidades que mantiene esta dirección con respecto a seguridad de la información y seguridad informática se encuentra:

- Monitorear y evaluar los accesos a los recursos de red, arquitectura de redes y comunicaciones.
- Analizar e implementar un sistema de gestión de seguridad de la información.
- Establecer mecanismos de control de seguridad informática, a fin de identificar vulnerabilidades y riesgos.

3.2.4.1.Área de seguridad de la información

Con el fin de cumplir las atribuciones y responsabilidades que mantiene la Dirección de Tecnologías de la Información y Comunicación (DTIC) respecto a la seguridad de la información, se crean áreas de gestión con sus respectivos productos, de entre estas gestiones se crea el Área de Seguridad de la Información la cual cuenta con las siguientes responsabilidades.

- Establecer políticas, normas e instructivos para garantizar la seguridad de la información.
- Generar informe de vulnerabilidades, riesgos y controles; y

- Generar reporte de implementación de controles de seguridad de la información.

Con esta primicia, el Área de Seguridad de la Información es la responsable de la generación de políticas, normas, procedimientos y controles que tienen como objetivo velar por la seguridad de los recursos de información, redes y sistemas informáticos de la Fiscalía General del Estado.

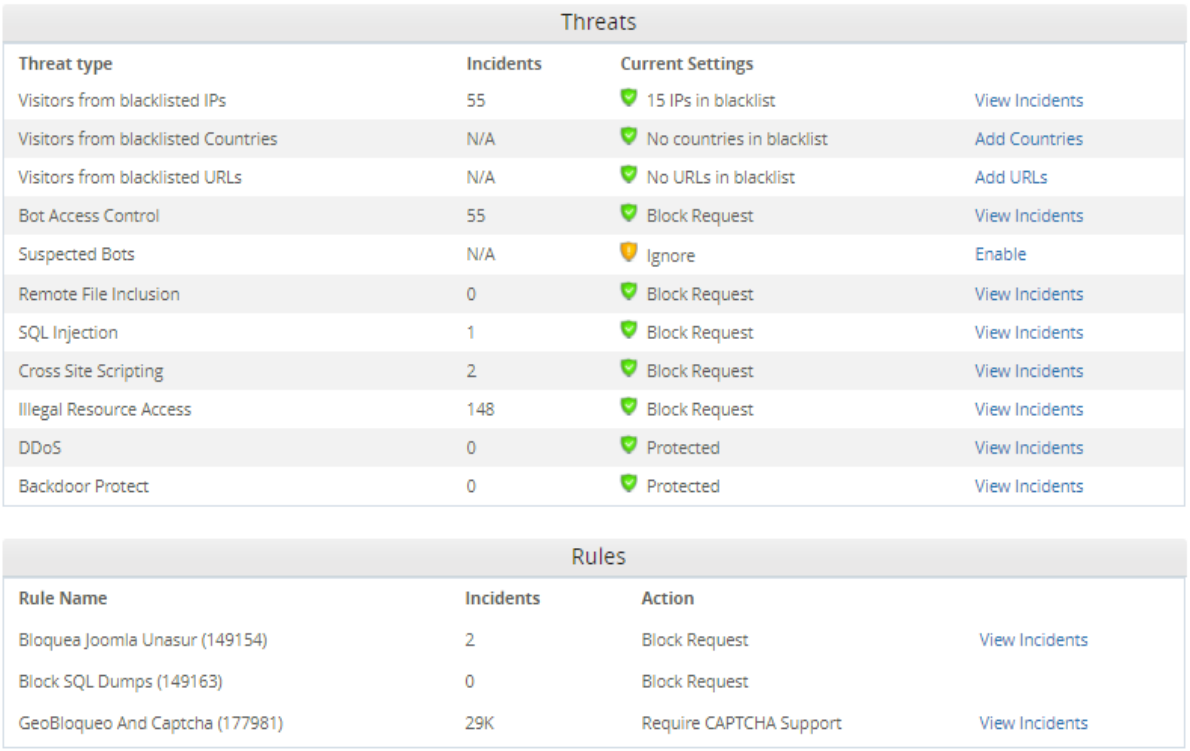
3.2.4.2.Eventos de seguridad informática en la FGE

Dentro de las responsabilidades que tiene el Área de Seguridad de la Información es la expedición de informes de vulnerabilidades, riesgos y controles, por lo que en los siguientes apartados se detallará brevemente los eventos de seguridad informática que con mayor frecuencia se reflejan y se obtienen de los sistemas de seguridad con los que cuenta la Dirección de Tecnologías de la Fiscalía General del Estado.

Informe acorde los sistemas de seguridad informática de la FGE

La Fiscalía General del Estado, cuenta con un servicio de protección en la nube denominado Firewall de Aplicaciones Web (WAF, por sus siglas en ingles) para proteger principalmente el sistema web misional. Esta herramienta, emite reportes gráficos que permiten conocer de manera rápida el estado de la seguridad, desempeño y tráfico de red institucional.

En las siguientes Figuras, se puede visualizar los reportes generados por el firewall de aplicaciones de la FGE, sobre los diferentes tipos de amenazas como: Remote File Inclusion, SQL Injection, Cross Site Scripting, etc., también se puede visualizar la categorización de los diferentes tipos de incidentes (por país, y por bot).



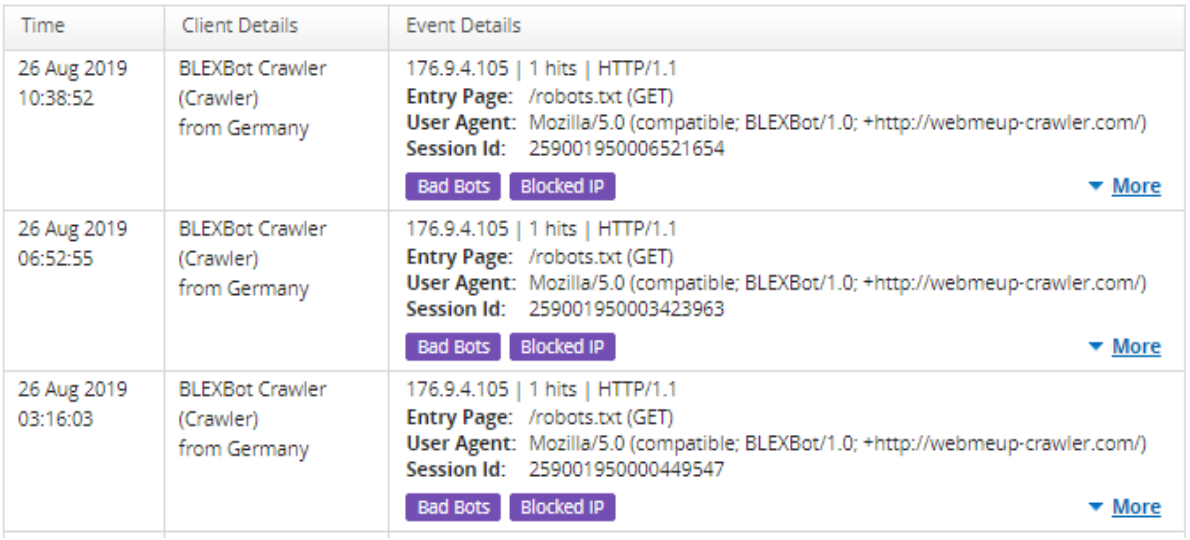
Threats

Threat type	Incidents	Current Settings	
Visitors from blacklisted IPs	55	15 IPs in blacklist	View Incidents
Visitors from blacklisted Countries	N/A	No countries in blacklist	Add Countries
Visitors from blacklisted URLs	N/A	No URLs in blacklist	Add URLs
Bot Access Control	55	Block Request	View Incidents
Suspected Bots	N/A	Ignore	Enable
Remote File Inclusion	0	Block Request	View Incidents
SQL Injection	1	Block Request	View Incidents
Cross Site Scripting	2	Block Request	View Incidents
Illegal Resource Access	148	Block Request	View Incidents
DDoS	0	Protected	View Incidents
Backdoor Protect	0	Protected	View Incidents

Rules

Rule Name	Incidents	Action	
Bloquea Joomla Unasur (149154)	2	Block Request	View Incidents
Block SQL Dumps (149163)	0	Block Request	
GeoBloqueo And Captcha (177981)	29K	Require CAPTCHA Support	View Incidents

Figura 14. Amenazas e incidentes informáticos en la FGE, Fuente: Fiscalía General del Estado



Time	Client Details	Event Details
26 Aug 2019 10:38:52	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001950006521654 Bad Bots Blocked IP ▼ More
26 Aug 2019 06:52:55	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001950003423963 Bad Bots Blocked IP ▼ More
26 Aug 2019 03:16:03	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001950000449547 Bad Bots Blocked IP ▼ More

Figura 15. Bloqueo de IPs de visitantes en lista negra, Fuente Fiscalía General del Estado

Time	Client Details	Event Details
26 Aug 2019 10:38:52	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001950006521654 Bad Bots Blocked IP ▼ More
26 Aug 2019 06:52:55	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001950003423963 Bad Bots Blocked IP ▼ More
26 Aug 2019 03:16:03	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001950000449547 Bad Bots Blocked IP ▼ More
25 Aug 2019 23:40:51	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001940207765744 Bad Bots Blocked IP ▼ More
25 Aug 2019 20:06:23	BLEXBot Crawler (Crawler) from Germany	176.9.4.105 | 1 hits | HTTP/1.1 **Entry Page:** /robots.txt (GET) **User Agent:** Mozilla/5.0 (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/) **Session Id:** 259001940206471698 Bad Bots Blocked IP ▼ More

Figura 16. Control de acceso de bots, Fuente: Fiscalía General del Estado

Time	Client Details	Event Details
26 Aug 2019 10:27:38	Firefox 68.0 from Ecuador	186.46.155.30 | First Visit: 7 months ago | 54 page views | 489 hits | Supports Cookies | Supports JavaScript | HTTP/2 **Entry Page:** /erp_fge/sitio/login_fge/index.php (GET) **Referrer:** https://www.gestiondefiscalias.gob.ec/fgeinicial/index.php **User Agent:** Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 **OS:** Windows **Session Id:** 996014270051644568 1 Illegal Resource Access ▼ More
26 Aug 2019 10:21:30	Firefox 68.0 from Ecuador	186.47.73.102 | First Visit: 3 months ago | 158 page views | 943 hits | Supports Cookies | Supports JavaScript | HTTP/2 **Entry Page:** /fgeinicial/index.php (GET) **User Agent:** Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 **OS:** Windows **Session Id:** 992000860140401645 1 Illegal Resource Access ▼ More

Figura 17. Acceso Ilegal a Recursos, Fuente: Fiscalía General del Estado

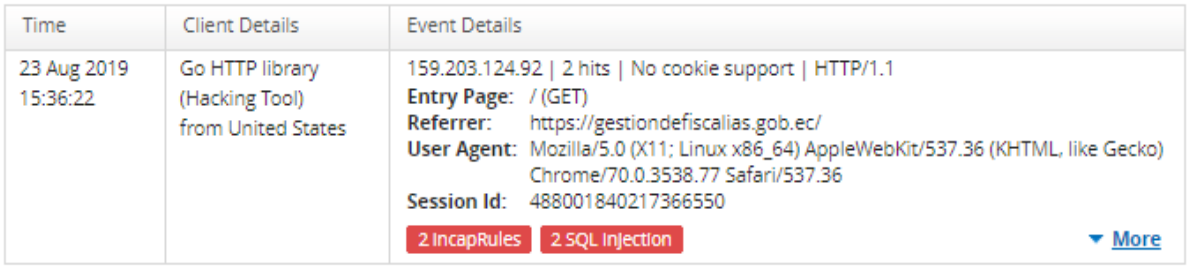


Figura 18. Bloqueo de SQL Injection, Fuente: Fiscalía General del Estado

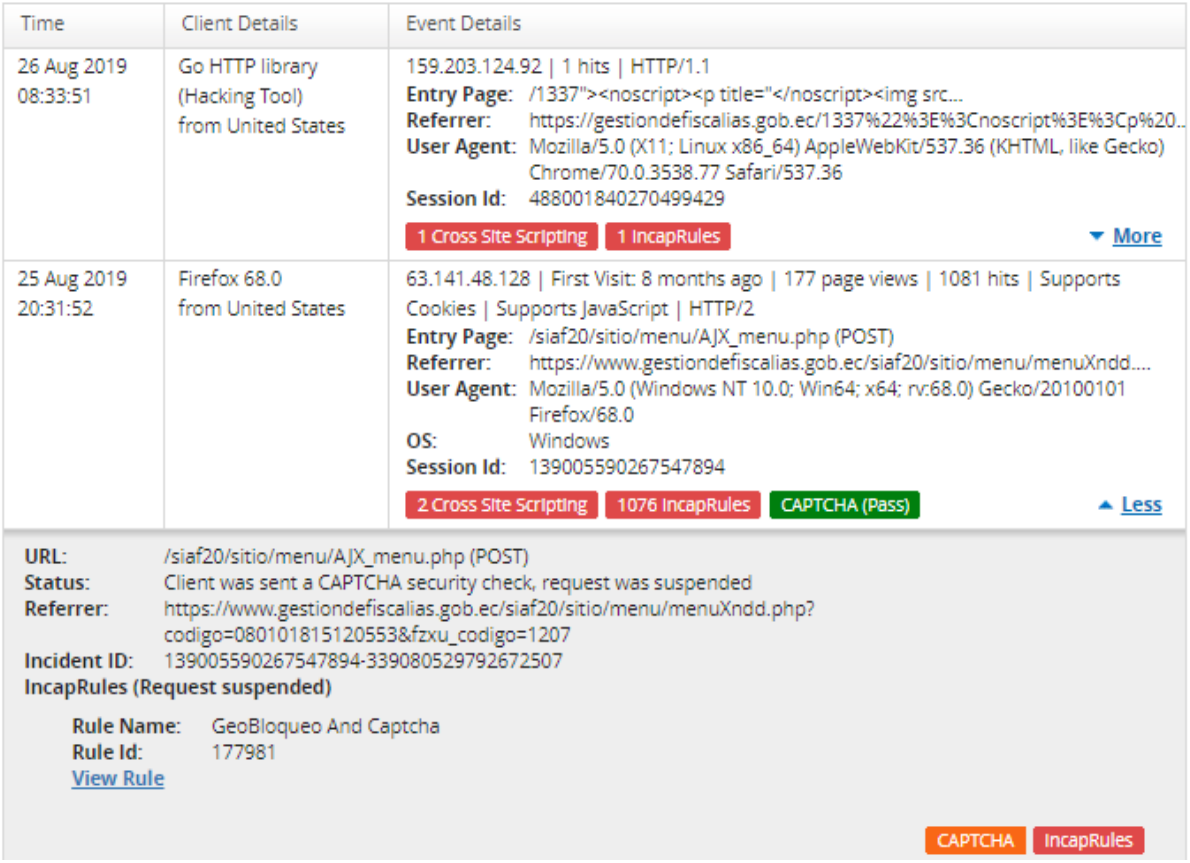


Figura 19. Bloqueo de Cross Site Scripting, Fuente: Fiscalía General del Estado

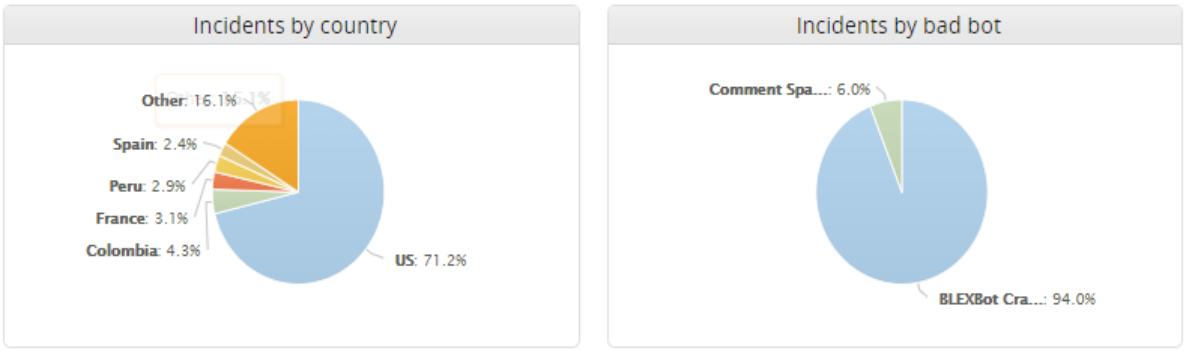


Figura 20. Incidentes por país y por bots, Fuente: Fiscalía General del Estado

Los eventos de seguridad registrados por el firewall de aplicaciones web nos ayudan a tener una visión general de los ciberataques a los que se encuentran expuestos los activos y sistemas de información institucionales de la FGE.

Acorde lo detallado en el apartado "*3.2.4.2. Eventos de seguridad informática en la FGE*", la Fiscalía se encuentra expuesta a una alta cantidad de amenazas e incidentes cibernéticos en sus sistemas web publicados hacia la red de Internet, sin embargo, con la tecnología que la institución cuenta actualmente se ha logrado mitigar en el periodo de un mes lo siguiente:

- 55 amenazas de tipo Visitors from blacklisted IPs.
- 55 amenazas de tipo Bot Access Control.
- 2 amenazas de ataques de tipo Cross Site Scripting.
- 148 amenazas de tipo Illegal Resource Access.
- Los países donde se originan el mayor número de incidentes son: EE. UU. con el 71.2%, Colombia con el 4.3%, y otros países con el 16.1%.

Como puntualización final del presente capítulo, se determinó que existen diferentes tipos de amenazas cibernéticas que han intentado exponer los activos y sistemas de información de la Fiscalía General del Estado, y que gracias a los sistemas de seguridad informática con los que cuenta la institución se han podido evitar que pasen de ser una amenaza, a pesar de ello, existen amenazas que evaden los filtros de los sistemas de seguridad y se convierten en incidentes informáticos, logrando así afectar los sistemas institucionales, por lo tanto, es aquí donde el CSIRT entra en operación para detectar, analizar, mitigar y de ser el caso recuperarse de un incidente informático acorde las mejores prácticas y estándares definidos a nivel global, por otra parte, el CSIRT también tendrá la posibilidad de coordinar acciones con otros equipos de respuesta a incidentes como el EcuCERT, CEDIA, EPN, entre otros, así como también coordinar actividades con responsables de seguridad de otras instituciones públicas y proveedores de servicios de telecomunicaciones.

CAPÍTULO IV

DISEÑO

En el presente capítulo, se realizó el diseño del CSIRT de la Fiscalía General del Estado acorde las mejores prácticas y estándares internacionales, como FIRST y la norma RFC 2350.

4.1.Modelo del CSIRT acorde el estándar RFC2350

Para la creación del CSIRT es importante definir el marco que guiará y regirá el funcionamiento del equipo, este marco de trabajo se refleja acorde el estándar RFC (Request for Comments) 2350 (Brownlee and Guttman 1998).

Por lo tanto, en los siguientes siete apartados, se detalla cada uno de los puntos que debe cumplir el diseño del CSIRT de la FGE basado en el estándar RFC 2350.

4.1.1. Información del Documento

En el presente documento se encuentra una descripción general, canales de comunicación, funciones y responsabilidades del CSIRT de la FGE acorde el estándar RFC 2350.

Fecha de última actualización

18/08/2020

Lista de distribución

No Disponible

Ubicación del documento

La ubicación actual del documento se encuentra en el portal web del CSIRT de la FGE (https://www.fiscalia.gob.ec/csirt).

4.1.2. Información de Contacto

Nombre del equipo CSIRT

Equipo de Respuesta a Incidentes de Ciberseguridad de la Fiscalía General del Estado CSIRT-FGE

- **Dirección**

    - Juan León Mera N19-36 y Av. Patria
    - Edificio, Fiscalía General del Estado
    - Dirección de Tecnologías de la Información y Comunicación, Piso 16
    - Quito – Ecuador

- **Zona Horaria**
  Time zone in Quito (UTC -5)

- **Número de teléfono**
  (+593) 2 3985 800 Ext. 173105
  Disponible durante la jornada laboral

- **Número de Fax**
  No Disponible

- **Otras Comunicaciones**
  Videoconferencia y otras opciones disponibles como twitter "@CSIRT_FGE" y telegram "@CSIRT_FGE".

- **Dirección de correo electrónico**
  csirt@fiscalia.gob.ec

- **Llaves públicas**

El CSIRT de la FGE cuenta con la siguiente llave pública, la misma que puede ser utilizada por los usuarios para enviar información confidencial de manera cifrada al correo electrónico "csirt@fiscalia.gob.ec".

```
0x280A DCB0 C5B3 CFBF 5348 EBDF 15BD 34CE 2E5B 1EA5
```

http://keys.gnupg.net/pks/lookup?search=csirt%40fiscalia.gob.ec%5C&fingerprint=on&op=index

- **Miembros del Equipo**

El CSIRT de la FGE iniciará sus operaciones con cuatro funcionarios especialistas en las ramas de seguridad informática y ciberseguridad y pertenecientes al área de seguridad de la información de la Dirección de Tecnologías de la Información de la Fiscalía General del Estado, estos funcionarios son:

- Jorge Moya – Especialista
- Patricio Guayaquil - Experto

- Carolina Salas – Analista
- Leonardo Chuquiguanca – Analista

- **Otra Información**

Para más información de cómo contactarse con el CSRIT de la FGE, así como acceder a varios recursos de ciberseguridad recomendados por el CSIRT, se puede encontrar en: https://www.fiscalia.gob.ec/csirt

- **Punto de contacto con el cliente**

Para ponerse en contacto con el CSIRT de la FGE respecto a incidentes de ciberseguridad relacionados a los servicios que ofrece, se lo puede hacer por medio del correo electrónico csirt@fiscalia.gob.ec.

En el caso de no ser posible utilizar el correo electrónico (por temas de confidencialidad), puede comunicarse vía telefónica al número (+593) 2 3985 800 Ext. 173105, en el horario establecido.

El CSIRT de la FGE atenderá los requerimientos de gestión de incidentes por los medios electrónicos correspondientes en horario regular de: 08:00 a 17:00 de lunes a viernes.

4.1.3. Constitución

- **Misión**

Apoyar a la Fiscalía General del Estado en la solución y/o mitigación de incidentes de ciberseguridad; realizando labores de coordinación, capacitación y apoyo para la solución de estos.

- **Visión:**

Ser un centro de respuesta a incidentes de ciberseguridad confiable y referente en el sector Judicial, coordinando con otros CSIRT a nivel país con el propósito de actuar de manera rápida y efectiva ante incidentes cibernéticos.

- **Comunidad objetivo**

El CSIRT de la FGE brindará en primera instancia sus servicios a los funcionarios de planta central de la Fiscalía General del Estado.

- **Patrocinio / Afiliación**

El CSIRT de la FGE está patrocinado por la Coordinación de Planificación Estratégica de la Fiscalía General del Estado

- **Autoridad**

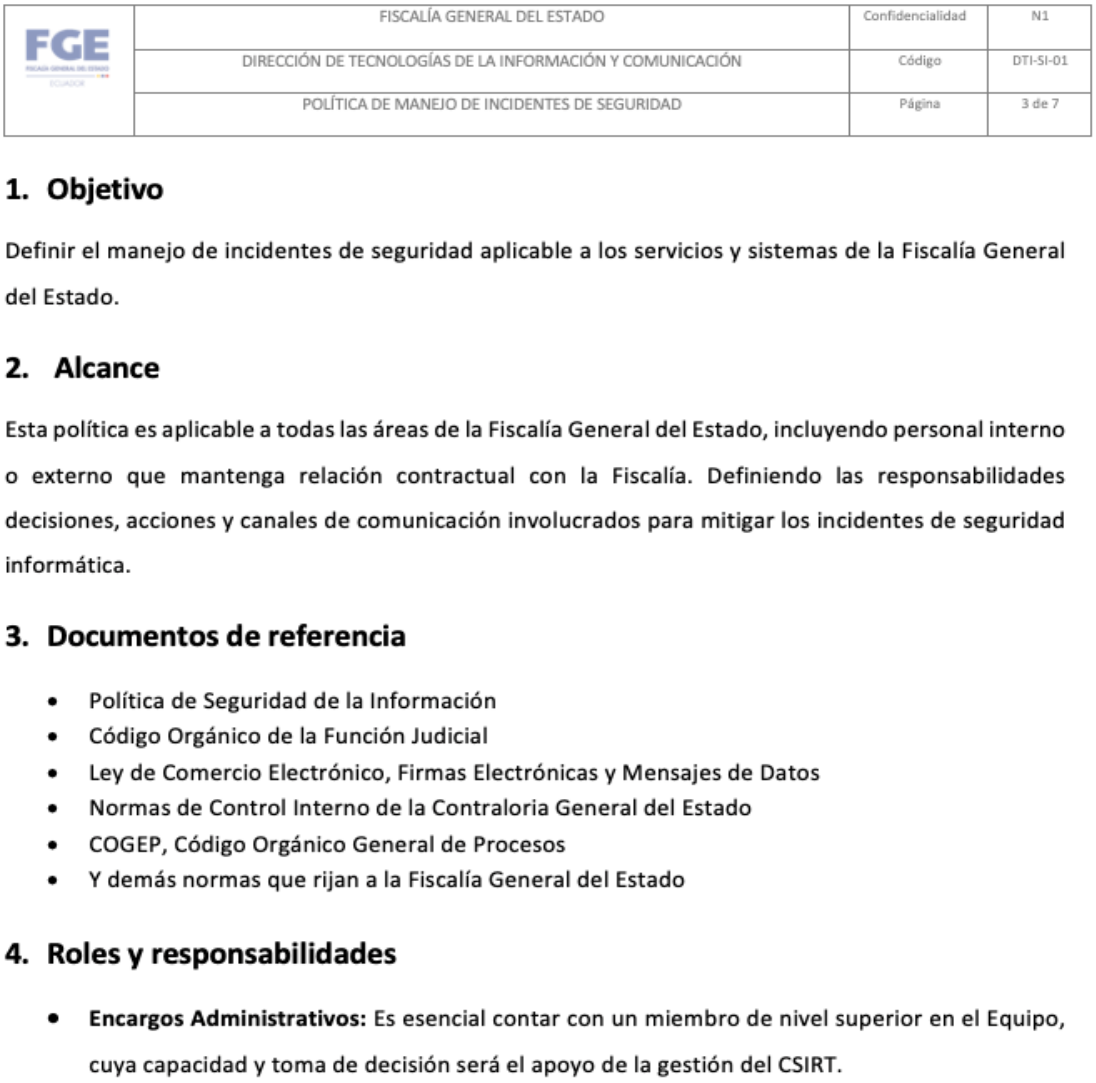
El CSIRT de la FGE tendrá una autoridad compartida con la Dirección de Tecnologías de la Información y Comunicaciones (DTIC), ya que al suscitarte un evento de seguridad informática, en conjunto con la DTIC se pueden tomar decisiones y acoger medidas preventivas sin esperar la aprobación de la máxima autoridad de la institución, por lo que los miembros de la comunidad objetivo están obligados a implantar las medidas propuestas por el CSIRT y la DTIC, con la finalidad resguardar y asegurar los sistemas institucionales.

4.1.4. Políticas

El CSIRT de la FGE se encuentra autorizado para abordar todo tipo de incidentes de ciberseguridad que ocurran en su circunscripción, para ello, cuenta con las siguientes políticas.

- Política de clasificación de información.
- Política de protección, retención y destrucción de información.
- Política de divulgación de información.
- Política sobre el acceso a la información.
- Políticas de uso aceptable de dispositivos electrónicos.
- Política de gestión de incidentes.
- Política de coordinación e intercambio de información con entidades externas.

En la Figura 21, se puede visualizar una estructura de cómo se encuentran desarrolladas las políticas previamente mencionadas para la aplicación en el CSIRT de la FGE. Es importante mencionar que, por temas de confidencialidad, en el presente proyecto se anexaran solamente 3 tipos de políticas (ver ANEXO I), el resto de las políticas se encontraran en la documentación de conformación del CSIRT.



FGE	FISCALÍA GENERAL DEL ESTADO	Confidencialidad	N1
	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	Código	DTI-SI-01
	POLÍTICA DE MANEJO DE INCIDENTES DE SEGURIDAD	Página	3 de 7

1. Objetivo

Definir el manejo de incidentes de seguridad aplicable a los servicios y sistemas de la Fiscalía General del Estado.

2. Alcance

Esta política es aplicable a todas las áreas de la Fiscalía General del Estado, incluyendo personal interno o externo que mantenga relación contractual con la Fiscalía. Definiendo las responsabilidades decisiones, acciones y canales de comunicación involucrados para mitigar los incidentes de seguridad informática.

3. Documentos de referencia

- Política de Seguridad de la Información
- Código Orgánico de la Función Judicial
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Normas de Control Interno de la Contraloria General del Estado
- COGEP, Código Orgánico General de Procesos
- Y demás normas que rijan a la Fiscalía General del Estado

4. Roles y responsabilidades

- **Encargos Administrativos:** Es esencial contar con un miembro de nivel superior en el Equipo, cuya capacidad y toma de decisión será el apoyo de la gestión del CSIRT.

Figura 21. Ejemplo de Política de manejo de incidentes, Fuente: Elaborado por el investigador

4.1.5. Servicios

Para determinar los servicios que ofrecerá el CSIRT de la FGE se toma como base el Framework de Servicios del FIRST, el cual se encuentra dividido en cinco áreas, tal como se lo describió en la sección de servicios de un CSIRT.

Por lo expuesto, y una vez analizados los servicios que ofrecen los diferentes tipos de CSIRT a nivel de Latinoamérica, así como el análisis de la situación actual en el ámbito de la seguridad informática de la Fiscalía General del Estado (ver ANEXO II), se ha llegado a establecer que el CSIRT de la FGE iniciará sus operaciones ofreciendo los servicios descritos en la Figura 22, con la finalidad de cumplir con su misión, visión y comunidad objetivo.

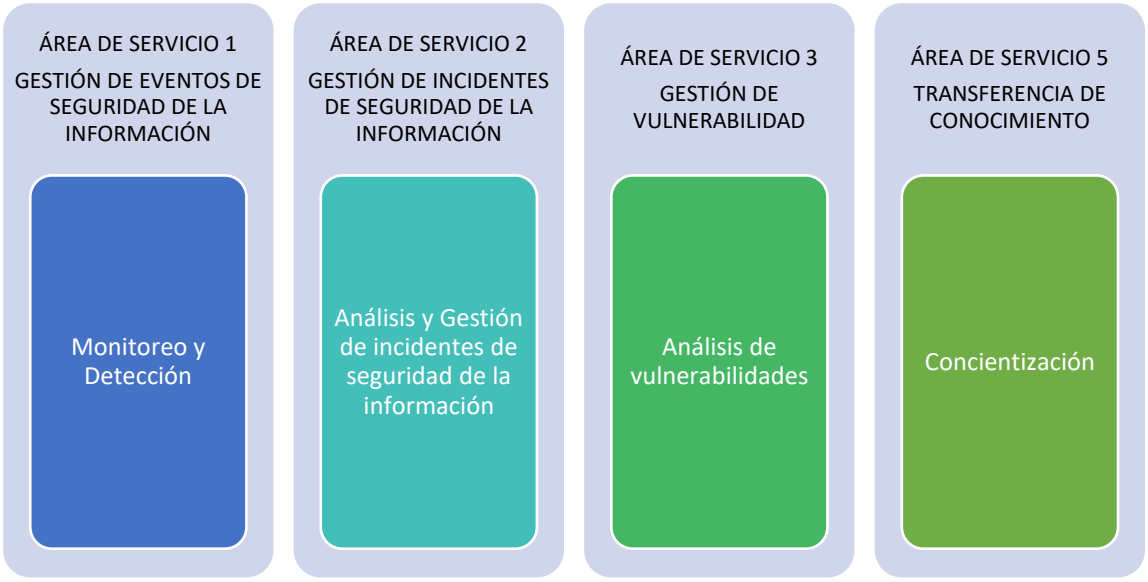


Figura 22. Servicios ofertados por el CSIRT-FGE, Fuente: Elaborado por el investigador

4.1.6. Formularios de notificación de incidentes

La solicitud para la resolución de incidentes cibernéticos llega a los CSIRT por diferentes canales de comunicación, primordialmente por correo electrónico, aunque también puede ser vía telefónica, portal web, etc.

Es importante mencionar que acorde las mejores prácticas, cada detalle del incidente debe ser registrado en un formato estandarizado para su mejor comprensión y con la finalidad de asegurarse de que se registren todos los datos importantes que componen el incidente, por lo que, en la Figura 23, se presenta un formato de formulario, el cual debe ser llenado por los usuarios para el registro del incidente en el CSIRT.

FGE	FISCALÍA GENERAL DEL ESTADO	Confidencialidad	N1
	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN CSIRT - FGE	Código	CSIRT-FGE-01
	FORMULARIO DE SOLICITUD DE MANEJO DE INCIDENTES	Página	1 de 1

Estimado usuario, sírvase rellenar este formulario y enviarlo a la dirección de correo electrónico:
csirt@fiscalia.gob.ec
El símbolo (*) significa que la respuesta es obligatoria.

Datos de la persona que reporta:

1. Nombre completo*:
2. Entidad afectada por el incidente*:
3. Sector:
4. País*:
5. Ciudad*:
6. Correo Electrónico*:
7. Teléfono*:
8. Otros:

Información de sistemas afectados

9. Dispositivos afectados (número de dispositivos, nombre e IPs de los dispositivos, función que realiza cada dispositivo, modelo y sistemas operativos):
10. servicios afectados (ficheros, bases de datos, software, etc.):
11. Protocolo/puerto

Incidente

12. Número de referencia:
13. Tipo de incidente:
14. Fecha de inicio del incidente:
15. El incidente sigue activo Sí ( ) NO ( )
16. Hora y método de detección:
17. Vulnerabilidades conocidas:
18. Ficheros sospechosos:
19. Contramedidas que se hayan aplicado:
20. Descripción detallada del incidente*:

Figura 23. Formulario de solicitud de gestión de incidentes, Fuente: Elaborado por el investigador

4.1.7. Descargos de responsabilidad

El CSIRT de la FGE ofrece sus servicios de manejo y gestión de incidentes informáticos principalmente a su comunidad objetivo, por lo tanto, si bien el equipo tomará todas las precauciones en la preparación de la información, notificaciones y alertas, no se responsabiliza por errores, omisiones o daños causados por el uso de la información que se genera, en relación con la gestión de incidentes de ciberseguridad.

4.2.Proceso para la gestión de incidentes

El proceso para la resolución de un incidente es una de las partes fundamentales que debe manejar un CSIRT, por tal motivo en la Figura 24, se detalla el proceso a seguir por parte del CSIRT de la FGE para la gestión de estos, este proceso se encuentra dividido en tres etapas:

- Detección y Análisis.
- Gestión del Incidente (contención, erradicación y recuperación).
- Actividad post incidente.

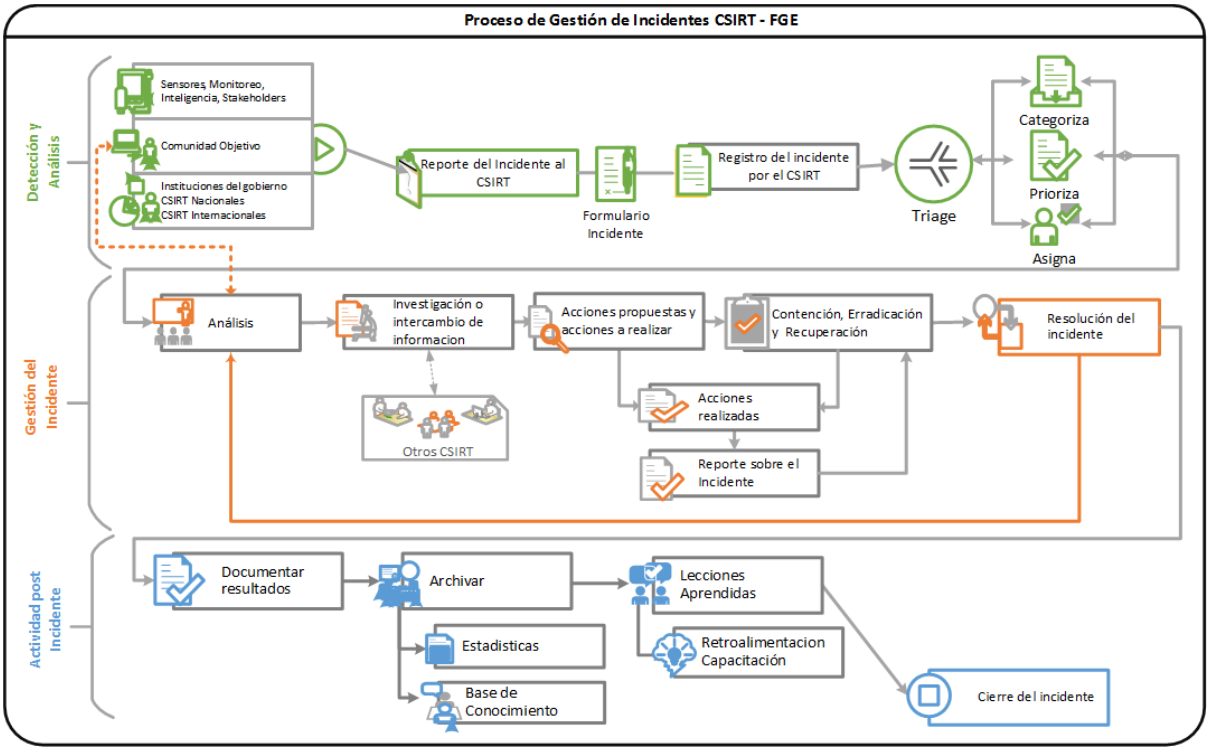


Figura 24. Proceso para la gestión de incidentes en el CSIRT de la FGE, Fuente: Elaborado por el investigador

El proceso de gestión de incidentes inicia con la etapa de detección y análisis, en la cual, se procede con la recolección de información de logs de eventos, monitoreo de redes y sistemas informáticos, solicitud a través de tickets por parte de la comunidad objetivo o solicitud por parte de otros CSIRT, esta información recolectada se la envía al CSIRT para su registro a través de un formulario (*descrito en el apartado 4.1.6. Formularios de notificación de incidentes*), posterior a ello, la información es analizada a través de un proceso que se le conoce

como ***triage***, en el cual, el incidente se categoriza, prioriza, y se asigna recursos humanos y técnicos acorde su nivel de impacto y criticidad, para su posterior tratamiento. En la Tabla 13, se detalla actividades que se deben realizar y tomar en cuenta en cada una de las etapas que componen el proceso de gestión de incidentes y que se visualizan en la Figura 24.

Tabla 13. Actividades relacionadas en cada etapa de un proceso de gestión de incidentes

Detección y Análisis
• Determinar si una ocurrencia es un incidente • Investigar, reunir evidencia y documentar el incidente • Categorizar y priorizar el incidente acorde su criticidad e impacto • Reportar el incidente al personal interno del CSIRT u organizaciones externas
Gestión del incidente (Contención, Erradicación y Recuperación)

• Adquirir, preservar, asegurar y documentar la evidencia
• Contener el incidente
  o Prevenir la difusión del incidente a otras áreas
  o A corto plazo, desconectar de la red
  o A largo plazo, mantener los sistemas en producción mientras se mitiga
• Erradicar el incidente
  o Identificar y mitigar vulnerabilidades explotadas por los atacantes
  o Eliminar todo tipo de malware o componentes de software malicioso
  o Si se descubren más componentes afectados por el incidente (por ejemplo, nuevos malware) realizar las acciones de *Detección y Análisis*, luego Contener y Erradicar.
  o Utilizar información de pasos previos
• Recuperarse del incidente
  o Restaurar los servicios afectados a la normalidad
  o Validar los servicios de los sistemas una vez hayan sido restaurados
  o Monitorización de malware y actividades no autorizadas

Actividad post incidente
• Documentar el proceso completo del manejo del incidente • Organizar reuniones de lecciones aprendidas • Entrenar al equipo en respuestas similares

Fuente: Elaborado por el investigador – basado en el check list NIST

4.3.Clasificación de incidentes acorde su nivel de prioridad

Una de las primeras actividades a realizar, luego de haber recibido y registrado el incidente cibernético, es hacer el triage, lo cual implica clasificar y asociar el incidente acorde criterios definidos previamente con el fin de brindarles un tratamiento adecuado. Estos criterios incluyen determinar el nivel de prioridad e impacto de cada incidente acorde la Tabla 14.

Tabla 14. Nivel de prioridad de una incídete

CRITICO	MUY ALTO	ALTO	MEDIO	BAJO

Fuente: Elaborado por el investigador, basado en la taxonomía de ENISA

En la Tabla 15, se detalla la clasificación de los incidentes de seguridad informática, asociados a los criterios de determinación del nivel de prioridad y peligrosidad de cada incidente cibernético.

Tabla 15. Matriz de clasificación de Incidentes asociados al nivel de criticidad

Matriz de clasificación de Incidentes asociados al nivel de criticidad		
Nivel de criticidad	**Clasificación del incidente**	**Tipo de incidente**
CRITICO	Otros	APTs
		Ciberterrorismo
		Todos los incidentes que no encajan en las categorías detalladas
MUY ALTO	Código Malicioso	Troyanos, Malware, Spyware, Ransomware, Rootkit
	Intentos de Intrusión	Nueva firma de ataques (Ataques desconocidos)
	Intrusión	Aplicaciones comprometidas
		Bots
	Disponibilidad	Sabotaje
ALTO	Contenido Abusivo	Pornografía infantil / Contenido sexual / Violencia
	Código Malicioso	Virus
	Disponibilidad	Ataques DoS/DDoS
		Intercepción de información
	Seguridad / Confidencialidad de la información	Acceso a información no autorizada
		Modificación de información no autorizada
	Fraude	Falsificación de registros o identidad
MEDIO	Contenido Abusivo	Difamación
	Recopilación de Información	Ingeniería Social
	Intentos de Intrusión	Explotación de vulnerabilidades conocidas
		Intentos de acceso
	Intrusión	Compromiso de cuentas con privilegios
	Fraude	Uso no autorizado de recursos
		Derechos de autor (Copyright)
		Suplantación de identidad (Phishing)
	Vulnerable	Sistemas y/o softwares Abiertos
		Servicios con acceso potencial no deseado
BAJO	Contenido Abusivo	Spam
	Recopilación de Información	Escaneo de servicios y puertos (Scanning)
		Análisis de paquetes (Sniffing)
	Intrusión	Compromiso de cuentas sin privilegios
	Test	Destinado para pruebas

Fuente: Elaborado por el investigador, basado en la taxonomía de ENISA

4.4.Tiempo de respuesta a un incidente

Los tiempos para la atención de los incidentes de seguridad informática por parte del CSIRT de la FGE se encuentran definidos acorde su nivel de criticidad, por lo tanto, los tiempos detallados en la Tabla 16, son tiempos aproximados en que un incidente informático debe ser atendido, mas no, el tiempo en el que un incidente debe ser resuelto, ya que los tiempos de solución son variables dependiendo del tipo del incidente.

Tabla 16. Tiempo aproximado de atención a un incidente

Nivel de Criticidad	Tiempo de respuesta
CRITICO	15 min
MUY ALTO	30 min
ALTO	1 hora
MEDIO	4 horas
BAJO	Siguiente día laboral

Fuente: Elaborado por el investigador, basado en la taxonomía de ENISA

4.5.Coordinación con entidades externas

Uno de los factores importantes que manejan los CSIRT es la relación de confianza, ya que, estos equipos muchas de las veces tienen la necesidad de interactuar con otros CSIRT o con varios tipos de organizaciones externas durante el cumplimiento de sus actividades en el manejo de incidentes, esto con la finalidad de que cada parte conozca sus roles y el proceso de gestión del incidente se realice de manera eficaz y oportuna.

En la Figura 25, se puede visualizar algunas de las organizaciones con las cuales el CSIRT de la Fiscalía General del Estado deberá mantener una línea de comunicación efectiva para la coordinación de manejo de incidentes. Esta línea de comunicación se la realizará a través de los medios tecnológicos que garanticen confidencialidad al momento de compartir e intercambiar información.

4.6.Coordinación con entidades externas

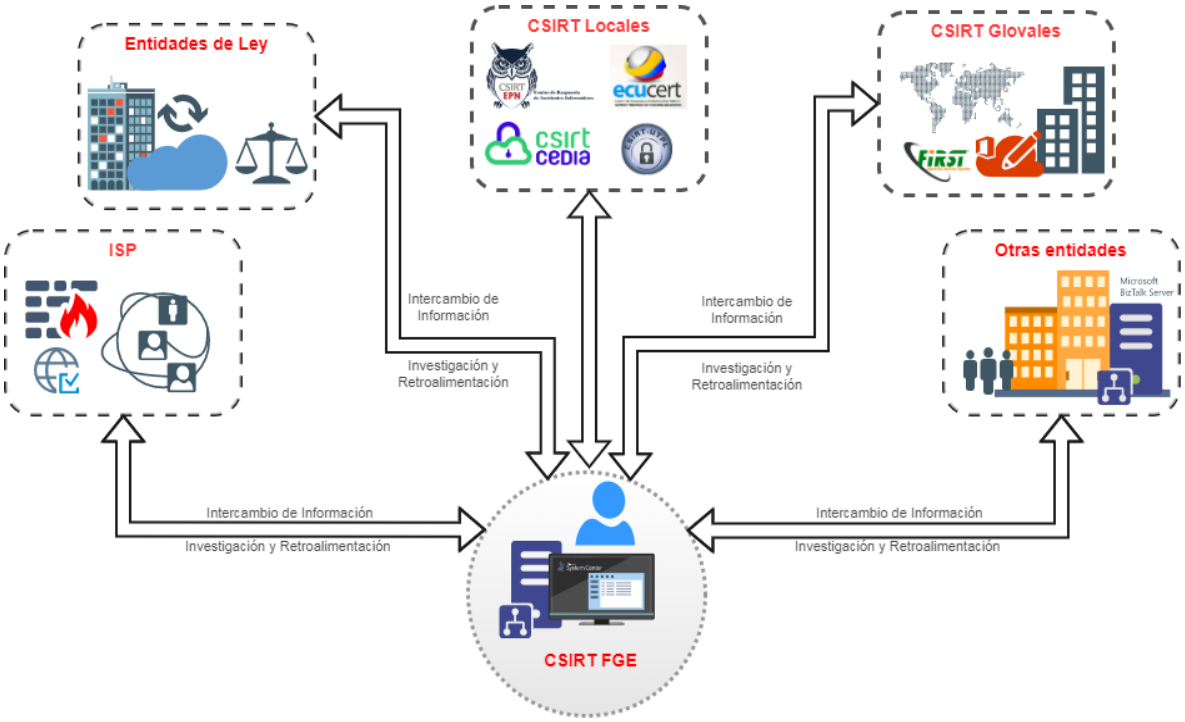


Figura 25. Coordinación del CSIRT con entidades externas, Fuente: Elaborado por el investigador

Pese a que ya existe una cooperación valiosa, los CSIRT siguen encontrando dificultades a la hora de compartir e intercambiar información sobre seguridad de manera fluida. Los obstáculos jurídicos y técnicos, así como la falta de interés de las partes implicadas en la ciberseguridad por compartir información, son los principales obstáculos para un intercambio de información eficaz. Por lo tanto, en el ANEXO III, se adjunta la Política de coordinación e intercambio de información con entidades externas que será ejecutada por el CSIRT de la Fiscalía General del Estado.

4.7.Cierre de un incidente

Durante las diferentes fases del proceso de gestión de un incidente de ciberseguridad, el CSIRT mantendrá el mismo en un estado *abierto*, mientras coordina y realiza acciones para su solución.

El cierre de un incidente informático no supone siempre una solución satisfactoria del problema. En algunos casos y por diferentes razones, no será posible alcanzar una solución adecuada, ya sea por falta de información que permitan identificar el origen del problema o por

parte de algún implicado al no emitir una respuesta (INCIBE 2020a). Por tal motivo, en la Tabla 17, se describe el estado que puede tener un incidente cibernético en un instante dado para su cierre.

Tabla 17. Cierre de un incidente acorde su estado

Estado del Incidente	Descripción
Cerrado - Resuelto y sin respuesta	No existe respuesta por parte de cliente u organización afectada, sin embargo, el incidente parece estar resuelto.
Cerrado - Resuelto y con respuesta	El cliente u organización afectada ha resuelto el incidente, por lo que notifica al CSIRT para su cierre.
Cerrado por falso positivo	La detección del incidente ha sido errada.
Cerrado sin solución y sin respuesta	Si el cliente u organización afectada no ha resuelto el incidente y tampoco ha comunicado al CSIRT, se cierra con este estado.
Cerrado sin solución y con respuesta	Si el cliente u organización afectada no ha resuelto el incidente incluso con las directrices emitidas por el CSIRT, se cierra con este estado.
Abierto	Estado en el que se encuentra el incidente desde que se ha sido notificado al CSIRT y durante todo el proceso de gestión de este, hasta que se produce el cierre por alguna de las causas expuestas.

Fuente: Guía nacional de notificación y gestión de ciberincidentes, INCIBE (2020)

IMPLEMENTACIÓN

Para la implementación del CSIRT en la FGE, se aplicarán las actividades descritas en esta sección, más todas las conceptualizaciones trabajadas en la etapa de diseño.

4.8.Modelo Organizacional y Funcional del CSIRT

El CSIRT de la FGE se encontrará organizado jerárquicamente a nivel institucional tal como se puede visualizar en la Figura 26, y contará con una autoridad compartida con la DTIC para la toma de sesiones y la aplicación de medidas preventivas y correctivas con relación a un incidente cibernético.

Figura 26. Estructura Jerárquica del CSIRT de la FGE, Fuente: Elaborado por el investigador

El CSIRT de la FGE trabajará bajo el liderazgo del responsable del CSIRT y en coordinación con especialistas, analistas y técnicos que conforman la Dirección de Tecnologías de la Información y Comunicaciones de la FGE. Adicionalmente se contará con la colaboración de funcionarios de otras Direcciones como: Jurídico, Comunicación Social e Investigaciones.

Por lo tanto, el CSIRT de la FGE contará con una estructura organizacional tal como se puede visualizar en la Figura 27, el mismo que mantendrá una organización centralizada multifuncional interna.

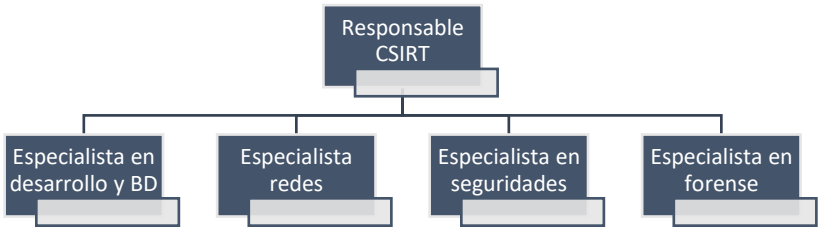


Figura 27. Estructura Organizacional del CSIRT de la FGE, Fuente: Elaborado por el investigador

Finalmente, las funciones y responsabilidades con las que contará el CSIRT de la FGE son:

- Coordinar la gestión de incidentes y vulnerabilidades de seguridad informática.
- Emitir boletines relacionados a eventos de seguridad informática y ciberseguridad.
- Brindar asesoramiento en temas de incidentes de seguridad informática al nivel directivo de la institución.
- Brindar los servicios ofertados a la comunidad objetivo (funcionarios).
- Realizar capacitaciones a la comunidad objetivo en temas de seguridad informática.
- Interactuar con la comunidad de CSIRT a nivel nacional e internacional.

4.9.Infraestructura Tecnológica

La infraestructura tecnológica para implementación del CSIRT depende mucho de los servicios a ofertar, madurez, estructura organizacional, y recursos económicos destinados para el CSIRT, por lo tanto, en los siguientes puntos se detalla el esquema de red, hardware y software a utilizar para el correcto funcionamiento del CSIRT de la FGE.

4.9.1. Diagrama de Red

En la Figura 28, se visualiza la infraestructura de red propuesta para el funcionamiento del CSIRT. Es importante mencionar que los componentes que se detallan en el diagrama son acorde la tecnología con la que actualmente cuenta la Fiscalía General del Estado.

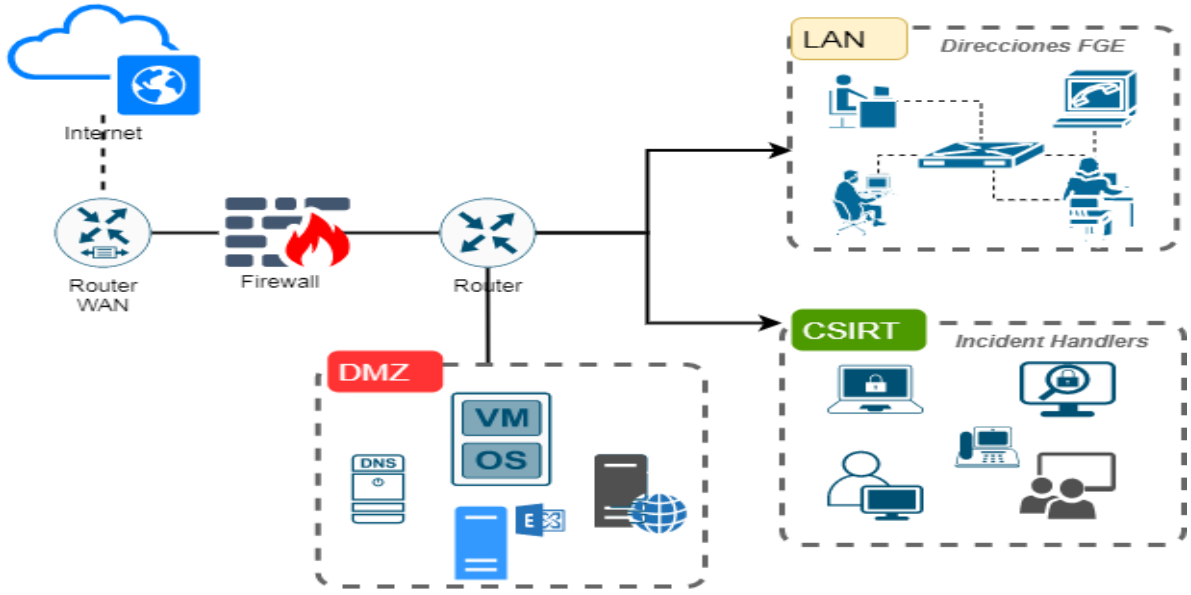


Figura 28. Diagrama de Red del CSIRT de la FGE, Fuente: Elaborado por el investigador

4.9.2. Infraestructura de Hardware

A nivel de infraestructura de hardware, el CSIRT de la FGE, contará con el apoyo de la Dirección de Tecnologías de la Información y Comunicaciones, puesto que, equipos de computación, teléfonos, hardware para servidores, sistemas de almacenamiento, seguridad perimetral, equipos de telecomunicaciones, etc., serán puestos a disposición del CSIRT para el desarrollo de sus operaciones.

4.9.3. Infraestructura de Software

A nivel de software, para el registro de los tickets, la Direcciones de Tecnologías cuenta con un OTRS (Open-source Ticket Request System), el cual se pondrá a disposición del CSIRT, para la gestión de tickets en temas de incidentes informáticos, mismo que será configurado con la finalidad de asegurar la confidencialidad de la información.

Y con respecto al software a utilizar durante el proceso de manejo y gestión de los incidentes de ciberseguridad, en la Tabla 18, se detalla cada una las herramientas especializadas en ciberseguridad y gestión de incidentes.

Tabla 18. Infraestructura de Software para utilizar en el CSIRT

Funcionalidad	Herramienta	Descripción
Escaneo de Puertos	Nmap	Herramienta para escaneo de puertos.
	SonarQube	Análisis estático de código fuente.
Escaneo de vulnerabilidades	Burp suite	Análisis de vulnerabilidad web.
	OpenVAS	Escaneo de vulnerabilidades.
	Nexpose	Análisis y gestión de vulnerabilidades.
Análisis de Malware	Cuckoo	Sistema para análisis de malware.
	MISP	Plataforma de intercambio de información de malware, amenazas inteligentes e indicadores de compromiso.
IDS	Prevención de Amenazas - PaloAlto Network	IDS basado en host. IDS basado en red.
Monitoreo	HP IMC	Sistema de monitoreo de servidores y equipos de networking.
Sniffer	Wireshark	Análisis de tráfico de red.

Criptografía	GnuPG	Herramienta de cifrado y firmas digitales.
Análisis forense	CAINE	Sistema Operativo orientado al análisis forense.
	Kali Linux	Herramienta orientada a la gestión de seguridad informática y análisis forense.
	Autopsy	Herramienta de análisis forense digital.
	FTK Imager Line	Herramienta para la creación y análisis de imágenes forense.

Fuente: Elaborado por el investigador

En el ANEXO IV, se adjunta una Tabla con una diversidad de sistemas y herramientas especializadas en seguridad informática, ciberseguridad y gestión de incidentes cibernéticos, y que en algún momento pueden también ser implementadas o utilizadas en el CSIRT de la FGE.

4.10. Financiamiento inicial del CSIRT

El CSIRT de la FGE al ser un área que integra la Dirección de Tecnologías de la Información y Comunicaciones, su financiamiento será a través de esta Dirección, tanto en talento humano como en recursos tecnológicos, acorde lo descritos en la Figura 29.

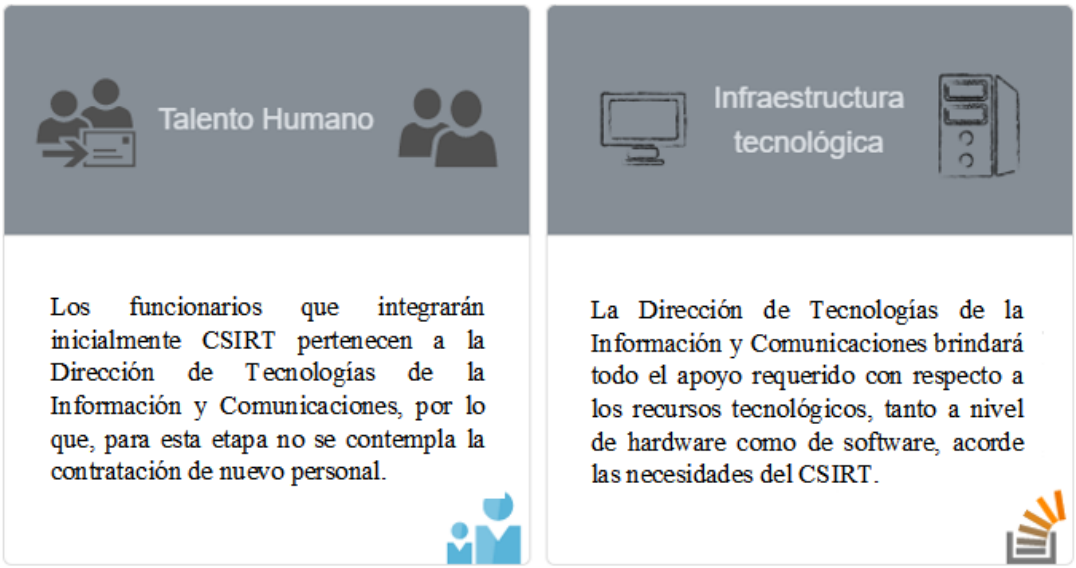


Figura 29. Financiamiento inicial del CSIRT, Fuente: Elaborado por el investigador

4.11. Apartado Legal

El CSIRT de la FGE cumplirá con toda la normativa legal vigente ecuatoriana que rige a las Entidades Públicas, con la finalidad de que en todo el proceso de manejo y gestión de un

incidente de seguridad informática no se infrinja ningún reglamento, normativa o ley que perjudique a la Institución, su comunidad objetivo y usuarios en general que hagan uso de los servicios que ofrecerá el CSIRT.

Por tal motivo, en los siguientes puntos se listan los reglamentos, normativas y leyes a las cuales el CSIRT de la FGE se regirá.

- Política de Seguridad de la Información de la FGE
- Código de ética de la Fiscalía General del Estado
- Código Orgánico de la Función Judicial
- Normas de Control Interno de la Contraloría General del Estado
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- COGEP, Código Orgánico General de Procesos
- COIP, Código Orgánico Integral Penal
- Y demás normas y leyes que rijan a la Fiscalía General del Estado

4.12. Documento de constitución

En el ANEXO V, se adjunta memorandos de autorización para la constitución e implementación del CSIRT de la FGE, el cual cuenta con, la misión, visón, servicios, comunidad objetivo y otros datos importantes para el inicio de operaciones del CSIRT.

4.13. Ejemplo de resolución de un incidente

Si bien, se ha tratado de documentar el ejemplo con un incidente de seguridad ocurrido en las instalaciones de Fiscalía General del Estado, por temas de confidencialidad no ha podido ser incluido documentalmente en el presente trabajo de investigación, sin embargo, el ejemplo descrito en esta sección está basado en un incidente cibernético gestionado por el CERT del Instituto Nacional de Ciberseguridad de España (INCIBE 2020b), y adaptado y documentado acorde los procedimientos que maneja el CSIRT de la FGE para gestionar sus incidentes de ciberseguridad.

Incidente:

Ransomware Sodinokibi

Proceso de manejo de incidentes de ciberseguridad por parte del CSIRT de la FGE

1. **Detección y análisis**

La fase de *Detección y Análisis* (Figura 30) está compuesta por la identificación de una ocurrencia, continuando con el análisis para determinar si esa ocurrencia es un incidente, y de confirmarse de que la ocurrencia si es un incidente, se procede con el reporte de este al CSIRT. El equipo técnico del CSIRT analiza el incidente y realiza el triage para categorizarlo y priorizarlo, inmediatamente es asignado a un técnico para su análisis y posterior gestión.

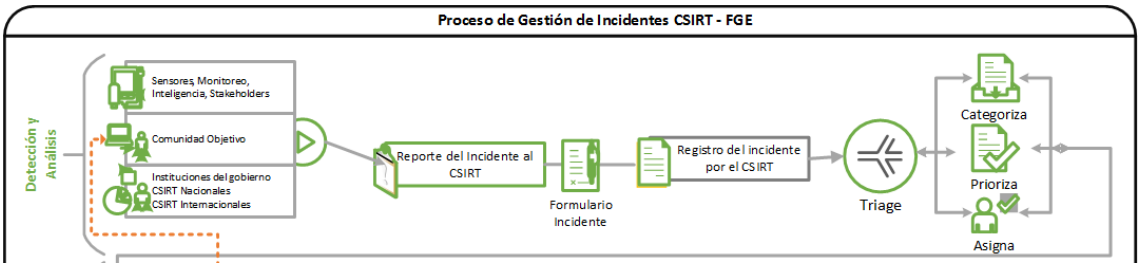


Figura 30. Proceso de gestión de incidentes - Detección y Análisis, Fuente: Elaborado por el investigador

Acorde este proceso, a continuación, se detalla las actividades realizadas en esta fase.

a. **Identificación y análisis**

La identificación temprana de un ransomware es vital para brindar una respuesta oportuna y eficaz a la infección y así evitar su propagación, no obstante, la detección de este tipo de incidentes con herramientas de seguridad como antivirus o sistemas de detección de intrusos (IDS) es muy complejo, por lo que, la identificación la mayoría de las veces se da por parte del usuario, al visualizar comportamientos fuera de lo común en su estación de trabajo.

En este caso el computador de la víctima del ransomware ha sufrido un comportamiento fuera de lo normal, ya que a primera vista el fondo de pantalla del escritorio ha sido modificado y agregado el mensaje "*All of your files are encrypted*", tal como se puede ver en la Figura 31.

Figura 31. Mensaje emitido por el ransomware una vez infectado un equipo, Fuente: INCIBE-CERT

Una vez que la víctima se ha dado cuenta del mensaje y al validar que efectivamente sus archivos se encuentran cifrados, procede a leer el documento con las instrucciones que el ciberdelincuente ha dejado para recuperar la información, ver Figura 32.

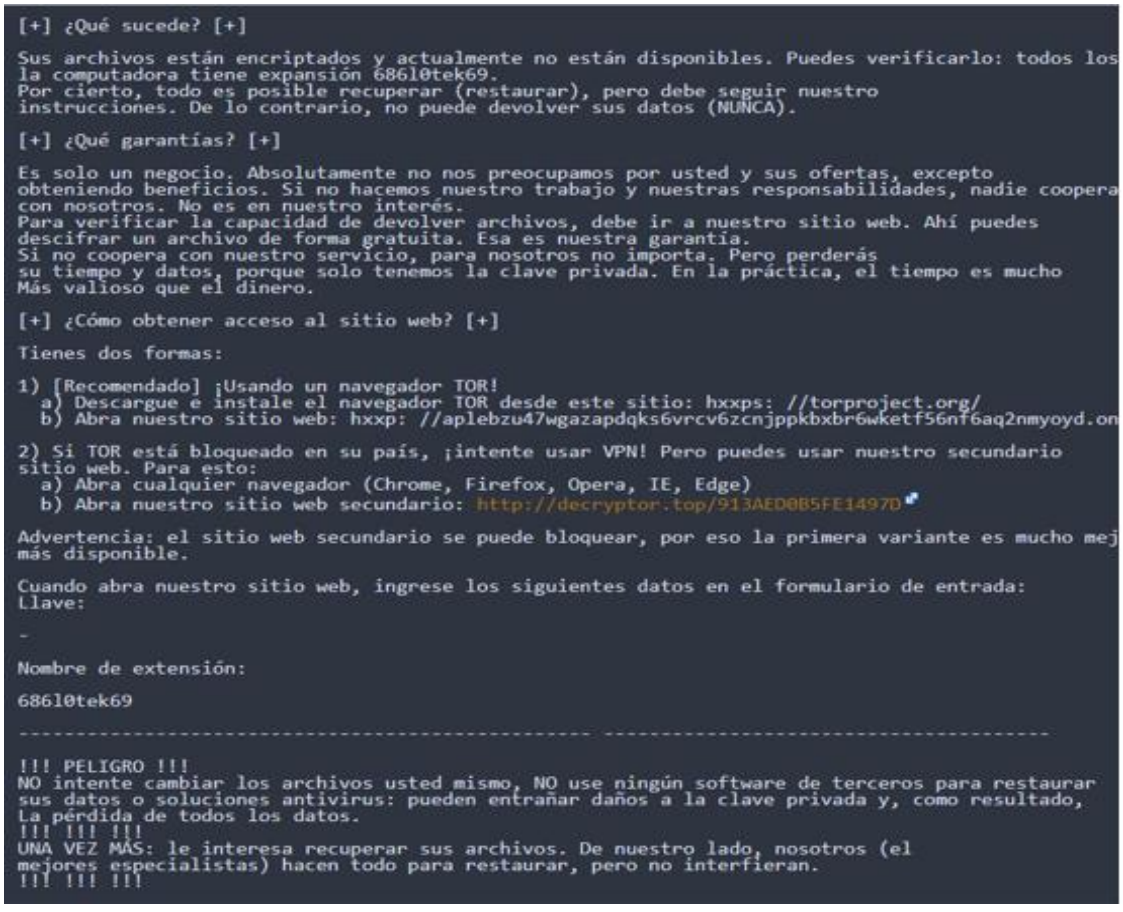


Figura 32. Nota de recuperación de datos del cibercriminal, Fuente: INCIBE-CERT

Con la información validada, se llegó a la conclusión que el evento no es un falso positivo, confirmando que la ocurrencia es efectivamente un incidente cibernético, por tal motivo, el siguiente paso es reportar el incidente al CSIRT para su tratamiento.

a. Reporte del incidente

El reporte del incidente al CSIRT se lo realiza a través del correo electrónico, en el cual se adjunta el formulario de solicitud de gestión de incidentes (ver Figura 33), así como toda la documentación de respaldo con la que se cuenta.

CSIRT FGE	FISCALÍA GENERAL DEL ESTADO	Confidencialidad	N1
	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN CSIRT - FGE	Código	CSIRT-FGE-01
	FORMULARIO DE SOLICITUD DE MANEJO DE INCIDENTES	Página	1 de 1

Estimado usuario, sírvase rellenar este formulario y enviarlo a la dirección de correo electrónico:
csirt@fiscalia.gob.ec
El símbolo (*) significa que la respuesta es obligatoria.

Datos de la persona que reporta:

1. **Nombre completo*:** Juan Pérez
2. **Entidad afectada por el incidente*:** Corporación APT S.A.
3. **Sector:** Privado
4. **País*:** NA
5. **Ciudad*:** NA
6. **Correo Electrónico*:** perezj@corporacionapt.com
7. **Teléfono*:** 35424819
8. **Otros:** NA

Información de sistemas afectados

9. **Dispositivos afectados (número de dispositivos, nombre e IPs de los dispositivos, función que realiza cada dispositivo, modelo y sistemas operativos):**
   Un equipo afectado, 10.10.15.18, servidor de impresión, Windows server.
10. **servicios afectados (ficheros, bases de datos, software, etc.):**
    Ficheros de configuración
11. **Protocolo/puerto**
    NA

Incidente

12. **Número de referencia:** inc001
13. **Tipo de incidente:** Ransomware
14. **Fecha de inicio del incidente:** NA
15. **El incidente sigue activo**: Sí (x) NO ( )
16. **Hora y método de detección: 06/04/2020**
17. **Vulnerabilidades conocidas:** NA
18. **Ficheros sospechosos:** NA
19. **Contramedidas que se hayan aplicado:** Desconectar de la red
20. **Descripción detallada del incidente*:** El administrador abrió su correo electrónico desde el servidor para revisar uno documentos de procedimientos que le habían hecho llegar, los cuales al descargarlos y abrirlos se ejecutó el Ransomware y los archivos del servidor se encriptaron.

Figura 33. Formulario de gestión del incídete ocurrido por un ransomware, Fuente: Elaborado por el investigador

Una vez reportado el incidente cibernético por parte del usuario, el personal técnico del CSIRT registra y genera un ticket para posteriormente continuar con el análisis y realización del triage.

b. Triage

El triage es una de las primeras actividades fundamentales que se realiza por parte del CSIRT, ya que acorde la matriz de clasificación de incidentes (*ver Tabla 15*) se puede determinar el tipo de incidente, su clasificación y el nivel de criticidad. En este incidente de tipo ransomware, el mismo se encuentra clasificado como *código malicioso* y tiene un nivel de criticidad *MUY ALTO*, tal como se lo puede visualizar en la Tabla 19.

Tabla 19. Clasificación del ransomware para determinar su nivel de criticidad

Nivel de criticidad	Clasificación del incidente	Tipo de incidente
MUY ALTO	Código Malicioso	Troyanos, Malware, Spyware, Ransomware, Rootkit

Fuente: Elaborado por el investigador

El siguiente paso es asignar el incidente a un técnico del CSIRT para su tratamiento, sin embargo, es importante tener en cuenta que, al ser categorizado este incidente con un nivel de criticidad MUY ALTO el tiempo de respuesta para iniciar con su gestión es de 30 minutos, esto acorde lo descrito en la Tabla 16 (*Tiempo aproximado de atención a un incidente*).

2. Gestión del incidente

Como se visualiza en la Figura 34, la fase de *Gestión del Incidente* se compone del análisis, investigación e intercambio de información para coordinar las acciones que se van a ejecutar durante la gestión del incidente, entre estas acciones se puede realizar la contención, erradicación y recuperación.

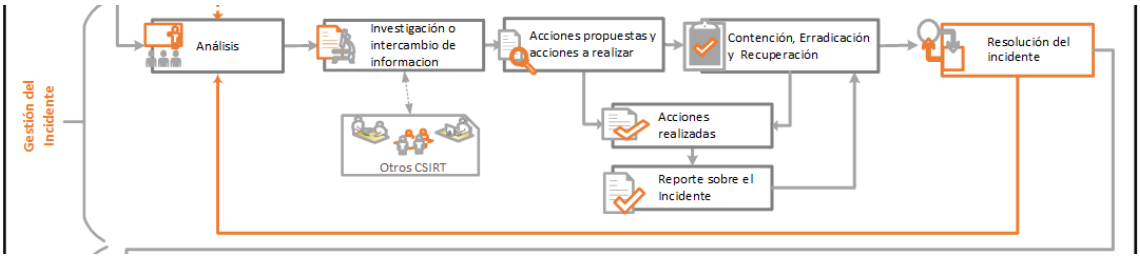


Figura 34. Proceso de gestión de incidentes - Gestión del Incidente, Fuente: Elaborado por el investigador

Por lo expuesto, a continuación, se detallan las actividades realizadas en esta fase.

a. Análisis e investigación

En los últimos años, el ransomware se ha convertido en una amenaza constante para las organizaciones y usuarios finales, esto debido a que las víctimas siguen siendo un factor importante de fuente de ingresos para los ciberdelincuentes, ocasionando grandes pérdidas económicas a las organizaciones y usuarios.

Con el pasar de los años estos tipos de ataques han ido evolucionando, por lo que en la actualidad se encuentra gran variedad de familias de ransomware, a pesar de ello, la tendencia es desarrollar malware dedicado y enfocados a organizaciones específicas en busca de obtener mejores beneficios económicos.

El desarrollo dedicado supone un mayor esfuerzo por parte de los ciberdelincuentes, ya que tienen que implementar nuevas técnicas y de mayor complejidad con la finalidad de crear malware sofisticado y persistente en su propagación, un ejemplo de esto es el ransomware Sodinokibi.

Sodinokibi es un ransomware dedicado a sistemas operativos Windows y cuyo modelo de propagación es Ransomware como Servicio (RaaS, por sus siglas en inglés), es decir, este código malicioso se comercializa de manera personalizada, ajustándose a las necesidades de cada cliente; para la propagación utiliza técnicas de ofuscación bastante robustas basadas en criptografía, con la finalidad de que el análisis e identificación por parte de los diferentes tipos de software de seguridad como antivirus o sistemas de detección de intrusos (IDS) sea más complejo, logrando así, tener una característica considerablemente peligrosa porque pude pasar desapercibido ante diferentes tipos de soluciones de seguridad.

En la Figura 35, se visualiza el esquema de funcionamiento del Ransomware Sodinokibi.

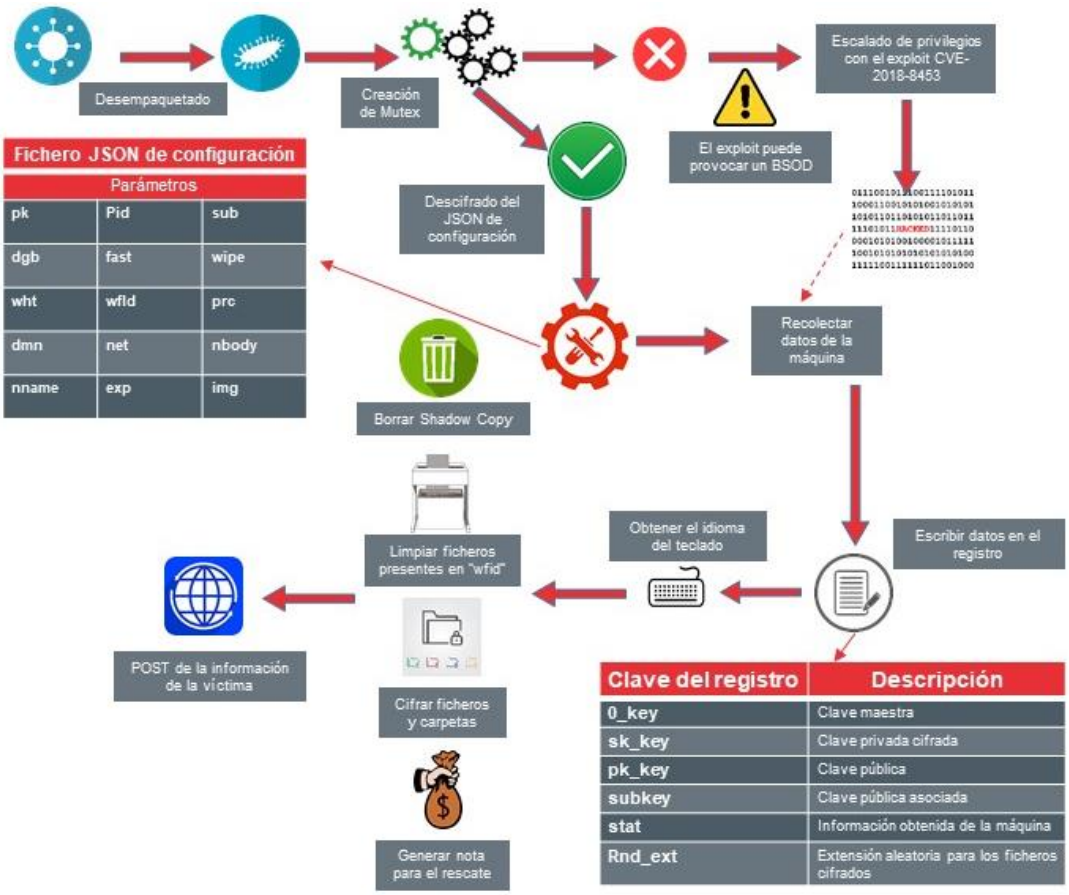


Figura 35. Esquema de funcionamiento del ransomware Sodinokibi, Fuente: INCIBE-CERT

Entre los principales vectores de ataque y propagación utilizados por este ransomware se encuentran:

- Envió de correos maliciosos a través de campañas de spam.
- Publicidad maliciosa conocida como adware.
- Fuerza bruta al protocolo de escritorio remoto (RDP, por sus siglas en inglés).
- Explotación de la vulnerabilidad CVE-2019-2725 que afecta a los sistemas Oracle.

El ejecutable del ransomware Sodinokibi es empaquetado de forma sofisticada y personalizada, en este empaquetamiento se incluyen todas las librerías, cadenas de texto y ficheros DLL mediante el algoritmo de cifrado RC4, este algoritmo emplea claves aleatorias de longitud variables para cada elemento cifrado, por lo que se hace casi indetectable por los diferentes tipos de software y sistemas de seguridad.

Una vez que este ransomware se ejecuta en el equipo de la víctima por alguno de los vectores de ataque descritos, realiza dos acciones fundamentales: (a) crea un identificador único o *mutex* para evitar que se ejecuten más procesos a la vez en la sección critica del equipo, logrando con esto que el computador no sufra fallos y la detección del código malicioso sea más compleja, y (b) descifra la configuración incrustada en el ransomware en formato JSON, con la finalidad de ejecutar las operaciones configuradas en el malware.

Posteriormente comienza con el escalonamiento de privilegios, esto lo realiza a través de la explotación de la vulnerabilidad CVE-2018-8453 siempre y cuando el sistema no haya sido actualizado o parchado, si el sistema se encuentra actualizado o parchado, el ransomware se ejecuta nuevamente mediante la función de Ransomware como Servicio (RaaS) mismo que permite forzar la ejecución del código malicioso con privilegios elevados, sin embargo, si no se obtiene privilegios elevados, el programa finaliza y el ataque fracasa.

Previo a proceder con el cifrado de los archivos, el ransomware desactiva todas las copias de seguridad y elimina todas las instancias de restauración almacenadas, una vez eliminadas las copias se seguridad, comienza a cifrar los archivos locales y las unidades conectadas a la red mediante la utilización de los algoritmos de cifrado simétrico como AES y Salsa20. La característica que lo hace letal es que maneja persistencia en sus ataques, para ello incrusta código malicioso en los registros de del sistema operativo Windows.

b. Acciones para realizar

Al detectar que el incidente corresponde a una infección por ransomware, en este caso por el ransomware Sodinokibi se debe planificar las acciones que se van a efectuar, estas acciones corresponden a realizar una gestión adecuada y eficiente al incidente, por lo tanto, se debe trabajar en las diferentes fases de contención, erradicación y recuperación.

I. Contención

Esta primera acción está enfocada a que el ransomware no se propague a otros sistemas por medio de la red, por lo que su objetivo primordial es reducir el alcance y detener su propagación, dicho esto, de entre las medidas a realizar en esta fase se encuentran las siguientes:

- **Aislar el dispositivo afectado. –** una de las primeras actividades a realizar luego de detectar que un equipo ha sido infectado con ransomware, es desconectar el dispositivo de la red y demás dispositivos conectado a él en el menor tiempo posible.
- **Detener su propagación. –** el ransomware tiene la habilidad de propagarse rápidamente por la red, por lo que, el equipo que se encuentra infectado no siempre puede ser el punto inicial de la infección y su aislamiento inmediato no siempre garantiza que el malware se haya detenido, por lo que se recomienda desconectar de la red todos los dispositivos sospechosos que pudieron ser punto de entrada del malware.
- **Evaluación de los daños. –** para evaluar los daños ocasionados por el ransomware, se recomienda revisar todos los equipos sospechosos para verificar que los archivos no hayan sufrido cambios recientes en su nombre o extensión, también es importante contar con un listado de todos los dispositivos infectados localmente o por medio de la red.
- **Localizar el origen de la infección**. – una de las actividades que nos permite identificar el origen del malware es revisar alertas de los sistemas de seguridad con los que cuenta la organización, otra actividad importante es analizar los dispositivos infectados para revisar posibles rastros, y como un tercer punto y no menos importante, se puede conversar con los usuarios sobre las actividades recientes realizadas en los equipos infectados; ya que un punto principal de ingreso e inicio de operación del ransomware proviene de ejecutar archivos que llegan a través de correo electrónico u otros vectores de ataque en los cuales hay intervención de los usuarios.
- **Identificar el Ransomware. -** es importante identificar si la variante del ransomware que ha infectado el equipo es Sodinokibi, para proceder con la gestión de mitigación correspondiente, esta identificación se la puede realizar revisando los datos de la nota de rescate que deja el

ransomware o a través de portales o bases de datos de sistemas antivirus que permiten detectar la variante del código malicioso.

II. Erradicación

Una vez identificado el ransomware, en este caso Sodinokibi, el siguiente paso es proceder con la erradicación, la forma más eficaz de lograr esto es reinstalando el sistema operativo, ya que este ransomware crea diferentes entradas de registro, guarda ficheros ocultos o incluso es capaz de realizar otro tipo de acciones como volver a ejecutarse.

III. Recuperación

La gestión del incidente se concluye con la recuperación, en esta fase el objetivo es restaurar el servicio o sistema, por lo que, para recuperar los archivos cifrados por el ransomware, en primer lugar, no debe tomarse como solución realizar el pago exigido por los cibercriminales, ya que no existe ninguna garantía de que se pueda recuperar la información tras haber realizado dicho pago.

Previo a la restauración del sistema es recomendable realizar una copia completa del disco duro con la información cifrada, para que, en el caso de que en el futuro exista una solución libre y gratuita se pueda hacer uso de aquella para descifrar y recuperar la información. Finalmente, para culminar la fase, se debe validar si existen respaldos disponibles del sistema que no hayan sido afectadas para proceder con el proceso de recuperación, no obstante, previo a realizar esta actividad, el ransomware debe estar completamente erradicado, por lo que, el sistema operativo y aplicaciones complementarias deben ser reinstaladas para su funcionamiento.

3. Actividad post incidente

En la Figura 36, se visualiza que la fase de *Actividad post Incidente* se compone de documentar todo el proceso de gestión, esta fase entra en acción una vez verificado que no exista rastro del ransomware, y que el sistema o servicio haya sido restaurado y validado por parte del usuario de la organización afectada.

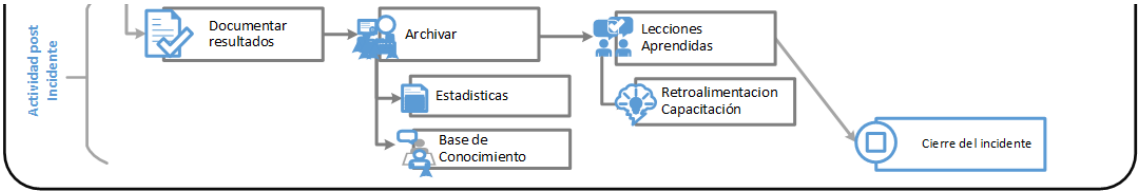


Figura 36. Proceso de gestión de incidentes - Actividad post Incidente, Fuente: Elaborado por el investigador

En esta fase se maneja toda la documentación generada durante el proceso de resolución del incidente, permitiendo manejar estadísticas y generando una base de conocimientos sobre los incidentes resueltos. Además se maneja el termino de lecciones aprendidas, ya que permite la realización de un análisis completo de las causas que provocaron la infección del sistema con el ransomware Sodinokibi, esto con la finalidad de: definir un plan de acción e implementar políticas y procedimientos, que permitan incrementar la seguridad de los sistemas para evitar o prevenir incidentes similares; por otro lado, esto también permite fomentar la concienciación hacia los usuarios y la formación o capacitación técnica del personal.

Por otro lado, previo al cierre del incidente el CSIRT emite recomendaciones y buenas prácticas a implementar para la protección y prevención de ataques de código malicioso como el ransomware Sodinokibi, entre estas recomendaciones se encuentra:

- Realizar copias de seguridad frecuentas y mantenerlas desconectadas de la red.
- Mantener los sistemas operativos y aplicaciones actualizadas y parchadas.
- Mantener buenos sistemas de seguridad.
- Otorgar mínimos privilegios a usuarios.
- Segmentación de la red.
- Concienciación.

La mejor estrategia para defenderse de este tipo de ataques de ransomware es estar preparados para su llegada. Una buena preparación ayuda favorablemente a evitar la afectación, y en el caso de no haber podido evitar la infección, su recuperación sea favorable en el menor tiempo posible.

CAPÍTULO V

CONCLUSIONES RECOMENDACIONES Y TRABAJOS FUTUROS

En este capítulo se presentan las conclusiones, recomendaciones y trabajos futuros a los cuales se llegó luego de haber concluido con la implementación del presente trabajo técnico investigativo.

Conclusiones

Como primer punto, se logró cumplir con los objetivos planteados al inicio de esta investigación, ya que luego de realizar todos los procesos técnicos y administrativos se implementó el centro de respuestas a incidentes de seguridad informática en la Fiscalía General del Estado, esto basado en las mejores prácticas, estándares y directrices emitidas por organismos internacionales que trabajan en coordinación con los CSIRT. Con la implementación de este centro de respuestas a incidentes de ciberseguridad la Fiscalía tiene la facultad de gestionar y coordinar el manejo de los incidentes cibernéticos al más alto nivel y siguiendo todos los protocolos y procesos correspondientes, logrando así, que la institución incremente su nivel de ciberseguridad antes, durante y después de un incidente informático.

Por otro lado, del estudio realizado sobre los casos de éxito en la implementación de CSIRT a nivel de Latinoamérica, se pudo determinar la gran importancia que tiene cada uno de estos centros de respuestas dentro de sus áreas y países, ya que son fundamentales en la prevención y gestión de incidentes de ciberseguridad, así mismo cumplen roles importantes de concienciación y capacitación a sus comunidades objetivos sobre incidentes cibernéticos y ciberseguridad.

Finalmente, el diseño del CSIRT se lo pudo realizar siguiendo las mejores prácticas, estándares y normas como el RFC 2350, este diseño fue aprobado por las autoridades de la Fiscalía General del Estado, ya que es la parte medular de cómo funcionará el centro de respuesta a incidentes de ciberseguridad de la Institución. Durante esta etapa de diseño se

determinó la misión, visión, objetivos, comunidad objetivo, servicios y los funcionarios que integraron el equipo inicial para el inicio de las operaciones del CSIRT.

Recomendación

Se recomienda realizar los procedimientos administrativos correspondientes para que el CSIRT de la FGE sea miembro del FIRST, esta membrecía le permitirá al centro de respuestas de incidentes de ciberseguridad de la Fiscalía formar parte de la comunidad más grande a nivel global de centros de respuesta a incidentes cibernéticos.

Trabajos Futuros

Como trabajos futuros, se puede crear una guía de procesos o mecanismos que permitan una comunicación integral entre los diferentes tipos de CSIRT del Ecuador, con la finalidad que la gestión y manejo de incidentes de ciberseguridad sea mejor coordinada entre los diferentes tipos de CSIRT a nivel nacional, logrando así, que los centros de respuesta a incidentes sean el pilar fundamental en la política pública de ciberseguridad en la cual se encuentra trabajando actualmente el estado ecuatoriano.

ANEXO I.

Políticas implementadas en el CSIRT de la FGE

FGE FISCALÍA GENERAL DEL ESTADO ECUADOR

POLÍTICA DE DIVULGACIÓN DE INFORMACIÓN

CSIRT-FGE

Código:	DTI-CSIRT-FGE-01
Versión:	1.0
Fecha de la versión:	05 de enero de 2020
Nivel de confidencialidad:	1

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
05/01/2020	1.0	Leonardo Chuquiguanca	Elaboración

Tabla de contenido

1. Objetivo

Definir qué información puede ser revelada a quién, cómo y en qué circunstancias, incluyendo las partes interesadas, socios CSIRT, otros órganos del gobierno, o incluso otros miembros del CSIRT-FGE. La manera en que se comparta la información se hará de acuerdo con su nivel de clasificación

2. Alcance

Toda la información generada o en poder del Equipo de Repuesta a Incidentes de Seguridad Informática de la Fiscalía General del Estado (CSIRT-FGE)

3. Documentos de referencia

- Política de Seguridad de la Información
- Código Orgánico de la Función Judicial
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Normas de Control Interno de la Contraloría General del Estado
- COGEP, Código Orgánico General de Procesos
- Y demás normas que rijan a la Fiscalía General del Estado

4. Política

Información pública

La divulgación de la información pública está autorizada, aunque debe ser difundida por medio de los canales oficiales autorizados del CSIRT-FGE y gestionados por la Dirección de Comunicación Social de la Fiscalía General del Estado.

Información clasificada

La información clasificada solo podrá ser divulgada cuando sea autorizada por el responsable del CSIRT-FGE o su delegado. En todos los casos, se firmará un acuerdo de no divulgación, que establece que cualquier destinatario de información clasificada será debidamente notificado de la clasificación de la información que está recibiendo.

Información clasificada de uso comunitario

La información que es clasificada pero aprobada para su difusión dentro de la comunidad objetivo, es un tipo especial de información. Todas las consideraciones anteriormente mencionadas siguen

siendo válidas, salvo que la divulgación que realizan ciertos miembros de la comunidad objetivo sea autorizada por el responsable del CSIRT-FGE.

Información confidencial

El CSIRT-FGE y su personal no divulgarán información confidencial. Si, por razones operativas, se hace necesario compartir información confidencial con terceros, usted deberá obtener el consentimiento del propietario de la información, quien será el que podrá o no autorizar su divulgación. Si el propietario autoriza su divulgación, se le exigirá al receptor firmar un acuerdo de no divulgación, este acuerdo podrá ser emitido por el propietario de la información o por el CSIRT.

Información Secreta

En ningún caso el CSIRT-FGE revelará información secreta por ley.

Información incompleta / no terminada

La información que se encuentra en borrador, y que no contiene información confidencial, puede ser revelada individualmente siguiendo las directrices definidas para este fin.

5. Divulgación interna

Dentro del equipo del CSIRT-FGE no habrá limitaciones en la divulgación ni en el intercambio de información, a menos que se haga una petición expresa por parte del responsable del CSIRT con respecto a una acción en específica. El CSIRT podrá divulgar cierta información a los miembros de la organización siempre y cuando se tenga en cuenta y se cumpla con los procedimientos establecidos de acuerdo con la clasificación de la información. La divulgación de la información debe ser autorizada por el responsable del CSIRT-FGE o su delegado.

6. Aspectos Legales

El CSIRT de la FGE cumplirá con toda la normativa legal vigente ecuatoriana que rige a las Entidades Publicas incluida la Fiscalía General del Estado para responder a todas las peticiones de información por parte de terceros. Dichas solicitudes de información deben hacerse por medio del departamento jurídico o el responsable del CSIRT-FGE.

7. Información de pedidos

Grupos de respuesta a incidentes

La cooperación y el intercambio de información con otros equipos de respuesta a incidentes son vitales para el funcionamiento y la supervivencia del CSIRT-FGE y la comunidad nacional e internacional más amplia de los equipos de respuesta a incidentes de seguridad informática. La mayor cantidad de información posible será compartida con otros equipos de respuesta a incidentes, de acuerdo con esta política, mediante la divulgación de cada caso de forma individual y con la autorización del responsable del CSIRT-FGE o su delegado.

8. Comunicado de prensa de información sensible

Cuando sea necesario, la información confidencial será divulgada de tal manera que se evite el acceso a esta por un tercero no autorizado.

9. Incumplimiento

El incumplimiento de la Política tendrá como resultado la aplicación de diversas sanciones las que pudieran ser administrativas o legales, conforme a la magnitud y característica del aspecto no cumplido. Esto en conformidad a lo establecido dentro de las leyes, normas y reglamentos.

10.Validez y gestión de documentos

Este documento es válido desde la aprobación del mismo.

El propietario de este documento es el Equipo de Repuesta a Incidentes de Seguridad Informática de la Fiscalía General del Estado, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Todas las políticas, normas, procedimientos y directrices deben ser especificadas, escritas, aprobadas y publicadas.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de documentos obsoletos o desactualizados
- Cantidad de documentos que no han sido distribuidos a los funcionarios para los que estaban destinados
- Cantidad de documentos para los que no se lleva un registro o que no están archivados adecuadamente

Estado	Nombre / Cargo	Firma
Elaborado	Leonardo Chuquiguanca	

	Analista de Infraestructura Tecnológica 2	
Revisado	Jorge Moya Especialista de Seguridades Informáticas	
Aprobado	Fabián Moreano Director de Tecnologías de la Información	

Figura 37.Política de divulgación de información, Fuente: Elaborado por el investigador

FISCALÍA GENERAL DEL ESTADO
ECUADOR

POLÍTICA DE MANEJO DE INCIDENTES DE SEGURIDAD

CSIRT-FGE

Código:	DTI-CSIRT-FGE-01
Versión:	1.0
Fecha de la versión:	05 de enero de 2020
Nivel de confidencialidad:	1

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
05/01/2020	1.0	Leonardo Chuquiguanca	Elaboración

Tabla de contenido

1. Objetivo

Definir el manejo de incidentes de seguridad aplicable a los servicios y sistemas de la Fiscalía General del Estado.

2. Alcance

Esta política es aplicable a todas las áreas de la Fiscalía General del Estado, incluyendo personal interno o externo que mantenga relación contractual con la Fiscalía. Definiendo las responsabilidades decisiones, acciones y canales de comunicación involucrados para mitigar los incidentes de seguridad informática.

3. Documentos de referencia

- Política de Seguridad de la Información
- Código Orgánico de la Función Judicial
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Normas de Control Interno de la Contraloria General del Estado
- COGEP, Código Orgánico General de Procesos
- Y demás normas que rijan a la Fiscalía General del Estado

4. Roles y responsabilidades

- **Encargos Administrativos:** Es esencial contar con un miembro de nivel superior en el Equipo, cuya capacidad y toma de decisión será el apoyo de la gestión del CSIRT.
- **Analistas de Seguridad de la Información:** Los miembros del equipo, deberán ser capacitados en el área de manejo de incidentes de seguridad, capacidad reactiva del manejo de múltiples incidentes, proporcionando opciones e implicaciones a la gestión.
- **Analistas de TI:** Los analistas deberán conocer desde dónde se accederá a los datos, y qué áreas de la red están fuera de los limites del incidente.
- **Analista función auditor:** El papel del auditor es el aseguramiento de los procedimientos, y en caso de un incidente su rol es observar, asegurar de que se esté siguiendo los procedimientos, y trabajar con el analista de seguridad para evitar problemas a corto plazo.
- **Responsable de Seguridad Física:** Es responsable de la seguridad física, en un incidente implica la relación directa con el sistema, la seguridad del equipo y/o del área. La evaluación del daño físico, la investigación de la evidencia física.

5. Política

El CSIRT-FGE, entiende que la seguridad dentro de la organización es un elemento fundamental, ya que se debe proteger dentro de la esfera de resguardo los activos. Siendo los activos, cualquier bien que tiene valor para la organización [ISO/IEC 133355].

El CSIRT-FGE, declara que el incidente de seguridad de la información es una evento único o una serie de eventos, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar las seguridad de la información [ISO/IEC TR 18044]

Asimismo, el evento de seguridad de la información será la ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de la salvaguardias o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información [ISO/IEC TR 18044]

Para el CSIRT-FGE, se establece que un incidente de seguridad es una violación a los controles de seguridad establecidos dentro del perímetro de acceso a los sistemas de la Fiscalía General del Estado. Algunos ejemplos de incidentes a considerar son:

- Ataques de denegación de servicios
- Daños físicos a sistemas de tratamiento de información
- Infección maliciosa (virus, malware, spyware, entre otros)
- Escaneo de puertos
- Pruebas de vulnerabilidad sin autorización
- Otros

El CSIRT-FGE, considera que los incidentes pueden tener una clasificación de critico y No critico, dependiendo de esta clasificación el tiempo de respuesta variará, siendo una respuesta inmediata por parte del equipo CSIRT para los incidentes críticos, ya que representa situaciones de alto riesgo. Para el caso de los incidentes No críticos, se presentan como un nivel aceptable de riesgo, por ende, podrá atenderse dentro de una margen mayo de tiempo.

Los tipos de incidentes presentan diferentes problemáticas, por ende, la interpretación del responsable hacia el tipo de evento es un papel importante, ya que se establece la criticidad, el impacto, las acciones y el personal requerido. A continuación, se menciona algunos tipos de incidentes:

- Interrupción de programas
- Accesos no autorizados a plataformas, sistemas y otros
- Uso inapropiado de los recursos de red
- Violación a la propiedad intelectual e industrial
- Fallo de las redes de la Fiscalía
- Fallas en los sistemas de comunicaciones
- Modificación de base de datos
- Interceptación de información
- Usurpación de identidad
- Entre otros.

EL CSIRT-FGE, declara que la severidad del incidente y los tiempos de respuesta se considerará en tres niveles:

1. Cualquier evento/incidente que afecte parcial o totalmente a uno o mas sistemas críticos de la Fiscalía General del Estado
2. Cualquier evento/incidente que afecte parcial o totalmente a un sistema utilizado por el usuario
3. Cualquier evento/incidente que afecte a algún recurso o sistema de prioridad baja para el CSIRT FGE.

SEVERIDAD	CATEGORÍA	TIEMPO DE RESPUESTA	ACCIÓN
1	CRÍTICO	Inmediata	Operaciones continua hasta el cierre del ticket en el día.
2	NORMAL	Hasta dos días laborables	Resolución dentro del horario regular del servicio
3	NO CRÍTICO	Hasta cuatro días laborables	Resolución dentro del horario regular del servicio

Nota: Se señala que, si bien se encuentran definidos los tipos de incidentes y el tiempo de respuesta del equipo CSIRT FGE, se debe evaluar estos puntos pensado en las actividades realizadas por el CSIRT FGE

Una vez identificado el incidente, comienza el proceso de comunicación, manejo y mitigación del evento/incidente del posible daño, por ende, se menciona las siguientes acciones para la respuesta correspondiente.

- Determinar si efectivamente es un incidente
- Mantener el control del incidente e involucrar al personal correspondiente
- Mantener informado al Encargado Administrativo
- Abrir un ticket de incidencia
- Recopilar la información ya sea por entrevistas al usuario, reguardar y analizar los archivos logs, proteger evidencias, etc.
- Controlar el daño que provoca el incidente
- Ejecutar el procedimiento de respuesta o resolución de incidentes
- Documentar todas las acciones realizadas y cerrar el ticket de incidencia
- Evaluar la eficiencia de las acciones realizadas en el incidente.

6. Incumplimiento

El incumplimiento de la Política tendrá como resultado la aplicación de diversas sanciones las que pudieran ser administrativas o legales, conforme a la magnitud y característica del aspecto no cumplido. Esto en conformidad a lo establecido dentro de las leyes, normas y reglamentos.

7. Definiciones

Termino	Definición
CSIRT	Centro de Respuesta a Incidentes de Seguridad Informática
ISO/IEC TR 18044	Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información
ISO/IEC 133355	Tecnología de la información - Directrices para la gestión de la seguridad de TI - Parte 5: Guía de gestión sobre seguridad de la red

8. Validez y gestión de documentos

Este documento es válido desde la aprobación del mismo.

El propietario de este documento es el Equipo de Repuesta a Incidentes de Seguridad Informática de la Fiscalía Generala del Estado, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Todas las políticas, normas, procedimientos y directrices deben ser especificadas, escritas, aprobadas y publicadas.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de documentos obsoletos o desactualizados
- Cantidad de documentos que no han sido distribuidos a los funcionarios para los que estaban destinados
- Cantidad de documentos para los que no se lleva un registro o que no están archivados adecuadamente

Estado	Nombre / Cargo	Firma
Elaborado	Leonardo Chuquiguanca Analista de Infraestructura Tecnológica 2	
Revisado	Jorge Moya Especialista de Seguridades Informáticas	
Aprobado	Fabián Moreano Director de Tecnologías de la Información	

FGE	FISCALÍA GENERAL DEL ESTADO	Confidencialidad	N1
	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN CSIRT	Código	CSIRT-SI-01
	POLÍTICA DE MANEJO DE INCIDENTES DE SEGURIDAD	Página	8 de 8

Procedimiento para control de documentos y registros ver. 1.2 del 19 de junio 2019

Figura 38. Política de manejo de incidentes, Fuente: Elaborado por el investigador

ANEXO II.

Análisis de servicios a ofertar por el CSIRT de la FGE

En la Tabla 20, se pude visualizar a detalle los servicios que ofrecen los diferentes tipos de CSIRT analizados como casos de éxito de implementación en la presente investigación, en la cual se evidencia que el promedio de servicios ofrecidos es de siete, y entre los servicios más ofertados se encuentran: Gestión de incidentes, Alertas y notificaciones de eventos, Análisis de vulnerabilidades, Monitoreo, Concientización, Entrenamiento, entre otros.

Tabla 20. Servicios de CSIRT a nivel de Latinoamérica

Servicios	CSIRT a nivel de Latinoamérica				
	EcuCERT Ecuador	ColCERT Colombia	CTIR Gov Brasil	CERTuy Uruguay	CSIRT GOB CL Chile
			Proactivos		
Gestión de Incidentes	x	x	x	x	x
Análisis de vulnerabilidades	x	x	x		x
Alertas / notificaciones de eventos	x	x	x	x	x
Auditorias de seguridad		x			
Diseminación y Recaudación de informaciones			x		
			Reactivos		
Monitoreo y alertas de incidentes	x	x	x	x	x
Boletines de seguridad	x			x	x
Gestión de Incidentes		x	x	x	
Ethical Hacking, Análisis de malware, IoC		x	x	x	x
			Valor Agregado		
Concientización	x	x		x	x
Entrenamiento / Formación técnica	x	x	x	x	

***Fuente**: Elaborado por el investigador*

Por otro lado, en la Figura 39, se detalla los eventos de seguridad informática que con mayor frecuencia se dan en la red y en los servicios de la Fiscalía General del Estado, esto basado en el análisis de la situación actual de la Institución.

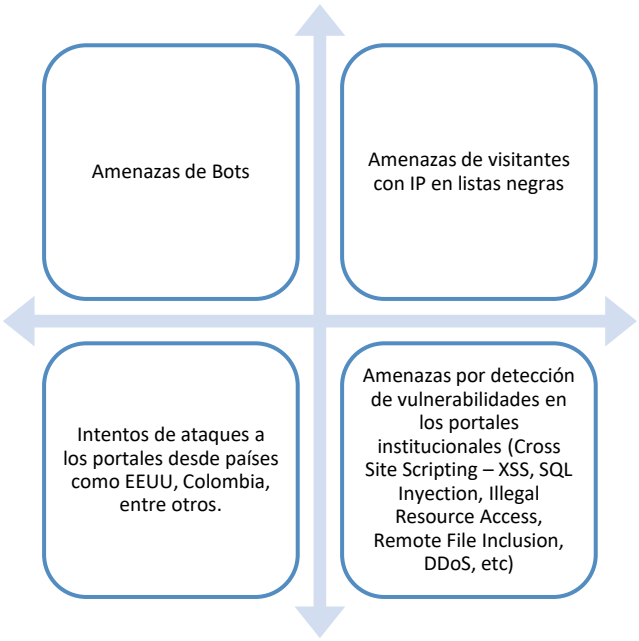


Figura 39. Eventos de seguridad informática generados con mayor frecuencia en la FGE, Fuente: Elaborado por el investigador

Con estos antecedentes, conociendo los servicios más brindados por los CSIRT y los eventos de seguridad que se dan con mayor frecuencia es la Fiscalía General del Estado, en coordinación con la Dirección de Tecnologías de la Información y Comunicaciones se ha seleccionado los servicios descritos en la Figura 40, con la finalidad de cumplir con la misión, visión y objetivos propuestos por parte del CSIRT de la FGE.

Figura 40. Servicios ofertados por el CSIRT-FGE, Fuente: Elaborado por el investigador

ANEXO III.

Política de coordinación e intercambio de información con entidades externas

FGE FISCALÍA GENERAL DEL ESTADO ECUADOR

POLÍTICA DE COORDINACIÓN E INTERCAMBIO DE INFORMACIÓN CON ENTIDADES EXTERNAS

CSIRT-FGE

Código:	DTI-CSIRT-FGE-01
Versión:	1.0
Fecha de la versión:	19 de agosto de 2020
Nivel de confidencialidad:	1

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
19/08/2020	1.0	Leonardo Chuquiguanca	Elaboración

Tabla de contenido

1. Objetivo

Definir el procedimiento para la coordinación y compartición de datos entre el CSIRT y entidades externas con la finalidad de manejar un intercambio de información seguro y eficaz mediante el uso de normas y estándares.

2. Alcance

Toda la información generada por el Equipo de Repuesta a Incidentes de Seguridad Informática de la Fiscalía General del Estado.

3. Documentos de referencia

- Política de Seguridad de la Información.
- Código Orgánico de la Función Judicial.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Normas de Control Interno de la Contraloría General del Estado.
- COGEP, Código Orgánico General de Procesos.
- Y demás normas que rigen a la Fiscalía General del Estado.

4. Política

4.1.Manejo de información interna

Dentro del equipo del CSIRT-FGE no habrá limitaciones en el manejo ni en el intercambio de información, a menos que se haga una petición expresa por parte del responsable del CSIRT con respecto a una acción en específica. El CSIRT podrá divulgar cierta información a los funcionarios de la institución siempre y cuando se tenga en cuenta y se cumpla con los procedimientos establecidos de acuerdo a la política de clasificación de la información. La divulgación de la información debe ser autorizada por el ***responsable del CSIRT-FGE o su delegado***.

4.2.Coordinación de respuesta a incidentes

La cooperación y el intercambio de información con otros equipos de respuesta a incidentes son vitales para el funcionamiento y la supervivencia del CSIRT-FGE y la comunidad nacional e internacional más amplia de los equipos de respuesta a incidentes de seguridad informática. La mayor cantidad de información posible será compartida con otros equipos de respuesta a incidentes, de acuerdo con esta política, mediante la divulgación de cada caso de forma individual y con la autorización del responsable del CSIRT-FGE o su delegado.

4.2.1. Áreas para una cooperación efectiva en el intercambio de información

Compartir información sobre amenazas de seguridad supone un gran beneficio siempre que recoja contenido de valor y se difunda de forma estructurada, la compartición de información debe incluir avisos de seguridad sobre vulnerabilidades, informes y estudios sobre protocolos, sistemas y prácticas de seguridad, pero, sobre todo, información preventiva y reactiva para enfrentar ciberamenazas e incidentes de seguridad.

De entre la información que, potencialmente, se puede compartir de forma colaborativa entre los diferentes CSIRT y entidades externas, se encuentran:

- Avisos de seguridad
  - Monitorización y alertas se seguridad
  - Vulnerabilidades en sistemas informáticos
- Informes
  - Guías de estudio detalladas
  - Recomendaciones y buenas practicas
- Estudios y Herramientas
  - Análisis de productos y/o sistemas de seguridad
  - Herramientas de ciberseguridad y auditoria
- Incidente y ciberamenazas
  - Indicadores de compromiso
  - Procedimientos de respuesta a incidentes
  - Alertas tempranas sobre nuevas ciberamenazas

4.2.2. Formato de intercambio de información

Uno de los principales problemas al intercambiar información, de forma que pueda ser procesada por el receptor e integrada en su arquitectura de ciberseguridad, es el formato adoptado. Por lo tanto, la finalidad de esta política es establecer un formato común y reconocido entre los beneficiarios de la información. En este sentido, existen múltiples formatos que estandarizan los mecanismos de intercambio de información cómo: STIX, CIF, OPENIOC, CybOX, VERIS, IODEF, TAXII o TLP.

En la presente política se aplica el estándar de clasificación de información TLP (Traffic Light Protocol). Este protocolo de comunicación proporciona un esquema simple e intuitivo, para que quien origina la información, indique cuándo y cómo se puede compartir información sensible y confidencial; y, cuán ampliamente quiere que su información se distribuya más allá del destinatario inmediato.

Este protocolo emplea cuatro colores para indicar el grado de confidencialidad y las consideraciones que debe tomar el usuario final para compartir el documento. El protocolo de intercambio de información se basa en un código de colores acorde la siguiente tabla.

Código	Cuándo utilizarlo	Cómo compartirlo	Ejemplo
TLP:RED	DIFUSIÓN RESTRINGIDA Cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente. En caso de que se necesite dar a conocer a otra persona se deberá pedir autorización al emisor de la información. En la mayoría de los casos, TLP:ROJO debe intercambiarse de manera verbal o en persona.	1. Información compartida en una reunión o conversación. 2. Correo electrónico directo. (Con etiqueta TLP:ROJO)
TLP:AMBER	DIFUSIÓN LIMITADA Cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor tiene la libertad de especificar límites adicionales para compartirla	Acuerdos de confidencialidad entre CSIRT
TLP:GREEN	DIVULGACIÓN LIMITADA DENTRO DE LA COMUNIDAD Cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones miembros del mismo sector, pero nunca a través de canales públicos	Compartir un análisis de un incidente o vulnerabilidad dentro de una comunidad objetivo especifica
TLP:WHITE	DIVULGACIÓN SIN RESTRICCIÓN Cuando la información no supone ningún riesgo de mal uso.	La información TLP:WHITE puede ser distribuida sin restricciones, respetando los derechos de autor.	Publicación en foros sobre ciberseguridad

4.2.3. Utilización del estándar TLP para el intercambio de información vía correo electrónico

Para el intercambio de información vía correo electrónico el destinatario debe indicar el color TLP de la información en el Asunto y en el cuerpo del correo electrónico, antes de la información designada en sí. El color TLP debe estar en letras mayúsculas: TLP: ROJO, TLP: AMBER, TLP: VERDE o TLP: BLANCO.

4.2.4. Utilización del estándar TLP para el intercambio de información mediante documentos

Para el intercambio de información mediante documentos, se debe indicar el color TLP de la información en el encabezado y pie de página de cada página. Para evitar confusiones con los esquemas de marcado de control existentes, es aconsejable justificar a la derecha las designaciones de TLP. El color TLP debe aparecer en letras mayúsculas y un tamaño de fuente de 12 puntos o más.

Si el receptor necesita difundir dicha información con terceros, más allá del alcance de la designación TLP indicada, debe remitirse a la fuente original.

Nota:

Aunque pueda ser tentador usar TLP:RED para algo sensible, esto puede evitar que sus destinatarios realicen una investigación adecuada o alertas en su entorno, ya que evitaría que sus destinatarios traten esta información con su equipo o personal técnico para un análisis posterior.

4.2.5. Autorización para el intercambio de información

EL responsable del CSIRT o su delegado es el único responsable de autorizar que información cumple con los protocolos correspondientes para iniciar con el proceso de intercambio de información.

5. Aspectos Legales

El CSIRT de la FGE cumplirá con toda la normativa legal vigente ecuatoriana que rige a las Entidades Públicas.

6. Incumplimiento

El incumplimiento de la Política tendrá como resultado la aplicación de diversas sanciones las que pudieran ser administrativas o legales, conforme a la magnitud y característica del aspecto no cumplido, esto en conformidad a lo establecido dentro de las leyes, normas y reglamentos.

7. Validez y gestión de documentos

Este documento es válido desde la aprobación del mismo.

El propietario de este documento es el Equipo de Repuesta a Incidentes de Seguridad Informática de la Fiscalía General del Estado, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Todas las políticas, normas, procedimientos y directrices deben ser especificadas, escritas, aprobadas y publicadas.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de documentos obsoletos o desactualizados
- Cantidad de documentos que no han sido distribuidos a los funcionarios para los que estaban destinados
- Cantidad de documentos para los que no se lleva un registro o que no están archivados adecuadamente

Estado	Nombre / Cargo	Firma
Elaborado	Leonardo Chuquiguanca Analista de investigación	
Revisado	Jorge Moya Especialista de Seguridades Informáticas	
Aprobado	Fabián Moreano Director de Tecnologías de la Información	

REFERENCIAS:

- INCIBE - Traffic Light Protocol (TLP): https://www.incibe-cert.es/tlp
- FIRST - Traffic Light Protocol (TLP): https://www.first.org/tlp/docs/tlp-v1.pdf
- ARCOTEL - GUÍA DE USO DEL PROTOCOLO TLP: https://www.arcotel.gob.ec/wp-content/uploads/2018/11/Guia-de-uso-del-protocolo-TLP.pdf
- Miguel Rego Fernández and Pedro Pablo Pérez García - El intercambio de información de ciberamenazas - Capítulo cuarto – 2017.

Figura 41. Política de coordinación e intercambio de información con entidades externas, Fuente: Elaborado por el investigador

ANEXO IV.

Sistemas y herramientas de gestión de incidentes y ciberseguridad

En la Tabla 21, se describe diferentes tipos sistemas y herramientas utilizadas en la seguridad informática, ciberseguridad y gestión de incidentes informáticos.

Tabla 21. Herramientas de ciberseguridad y gestión de incidentes

Herramienta	Descripción	Enlace
	Herramientas para análisis de seguridad	
ArchStrike	Repositorio Arch Linux para profesionales de la seguridad informática.	https://archstrike.org/
Backbox	Distribución Linux enfocando a la seguridad informática en entornos tecnológicos.	https://www.backbox.org/
Blackarch Linux	Distribución Linux para pruebas de penetración e investigadores de seguridad.	https://blackarch.org/
Dracos Linux	Distribución Linux para pruebas de penetración.	https://dracos-linux.org/
Fedora Security Lab	Plataforma de entorno de pruebas para auditorias de seguridad, análisis forense, recuperación de sistemas, etc.	https://labs.fedoraproject.org/
Kali Linux	Distribución para auditoria, seguridad informática y pruebas de penetración	https://www.kali.org/
Parrot OS	Distribución Linux, enfocada a la privacidad y seguridad informática, incluye laboratorio para pruebas de ciberseguridad.	https://www.parrotsec.org/
Security-Onion	Distribución Linux para la búsqueda de amenazas, monitoreo y seguridad empresarial.	https://securityonion.net/
TAILS	Distribución Linux enfocada a la privacidad y el anonimato en la red.	https://tails.boum.org/
QUBES	Distribución Linux orientada a la seguridad y privacidad en la red	https://www.qubes-os.org/
Wifislax	Distribución Linux orientada a la auditoria de redes inalámbricas	https://www.wifislax.com/
Weakerthan	Distribución de Linux enfocada a las pruebas de penetración y capture the flag (CTF).	http://www.weaknetlabs.com/
	Herramientas de análisis forense y respuesta a incidentes	
Santoku Linux	Distribución Linux enfocada al análisis forense, análisis de malware y análisis de seguridad de dispositivos móviles.	https://santoku-linux.com/
SIFT	Distribución Linux enfocada a la gestión y repuesta de incidentes informáticos e informática forense.	https://digital-forensics.sans.org/

Tsurugi Linux	Distribución de Linux enfocada a la investigación de análisis forense digital y respuesta ante incidentes (DFIR), análisis de malware y OSINT.	https://tsurugi-linux.org/

***Fuente**: Elaborado por el investigador*

ANEXO V.

Memorandos de autorización para la implementación del proyecto

Memorando Nro. FGE-CGI-DIC-2020

Quito, 13 de mayo de 2020

PARA:
Director de Talento Humano
FISCALÍA GENERAL DEL ESTADO

ASUNTO: AUTORIZACIÓN PARA IMPLEMENTACIÓN DE TRABAJO DE FIN DE MÁSTER EN LA FISCALÍA GENERAL DEL ESTADO.

De mis consideraciones.

Reciba un cordial y fraterno saludo, yo Leonardo Rafael Chuquiguanca Vicente con C.I. 1104952708, servidor de la Fiscalía General del Estado, con la finalidad de concluir con mis estudios de la Maestría en Ciberseguridad en la Universidad Internacional SEK he planteado como trabajo de fin de máster la "***IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) EN LA FISCALÍA GENERAL DEL ESTADO***" el cual tiene como objetivo principal:

- *Implementar un CSIRT gubernamental que instaure un Equipo de Respuesta a Incidentes de Seguridad Informática en la Fiscalía General de Estado, esto acorde al estándar RFC 2350 y las mejores prácticas definidas por el FIRST.*

Al ser este, un trabajo técnico tecnológico que debe implementarse en la institución, solicito de la manera más cordial **su autorización** para realizar la implementación del proyecto en coordinación con la Dirección de Tecnologías de la Información y Comunicaciones, esto siguiendo todos los estándares de seguridad informática y normativa legal vigente.

Por la atención que le brinde a la presente, desde ya le agradezco por su colaboración.

Saludos cordiales,

Atentamente,

Documento firmado electrónicamente

Ing. Leonardo Rafael Chuquiguanca Vicente

FISCALÍA GENERAL DEL ESTADO

Figura 42. Memorando de solicitud de autorización para implementar el proyecto en la FGE, Fuente: Elaborado por el investigador

FGE
Fiscalía General del Estado
ECUADOR

182 - AV. PATRIA Y 12 DE OCTUBRE, ESQ.

Memorando Nro. FGE-CGGR-DTH-2020

Quito, 22 de mayo de 2020

PARA:
Director/a de Tecnologías de la Información y Comunicaciones
FISCALÍA GENERAL DEL ESTADO

ASUNTO: SOLICITANDO PRONUNCIAMIENTO RESPECTO A PEDIDO DE ING. LEONARDO RAFAEL CHUQUIGUANCA VICENTE PARA REALIZAR SU TRABAJO DE FIN DE MAESTRIA EN CIBERSEGURIDAD EN LA DIRECCIÓN DE TICS

De mi consideración.-

En atención al Memorando Nro. FGE-CGI-DIC-2020-01442-M, suscrito por el ingeniero Leonardo Rafael Chuquiguanca Vicente, Analista de Investigación 2 de la Dirección de Investigación Civil de la Fiscalía General del Estado, mediante el cual manifiesta *"...con la finalidad de concluir con mis estudios de la Maestría en Ciberseguridad en la Universidad Internacional SEK he planteado como trabajo de fin de máster la "IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) EN LA FISCALÍA GENERAL DEL ESTADO" el cual tiene como objetivo principal:*

- *Implementar un CSIRT gubernamental que instaure un Equipo de Respuesta a Incidentes de Seguridad Informática en la Fiscalía General de Estado, esto acorde al estándar RFC 2350 y las mejores prácticas definidas por el FIRST.*

Al ser este, un trabajo técnico tecnológico que debe implementarse en la institución, solicito de la manera más cordial su autorización para realizar la implementación del proyecto en coordinación con la Dirección de Tecnologías de la Información y Comunicaciones, esto siguiendo todos los estándares de seguridad informática y normativa legal vigente..." Al respecto me permito manifestar lo siguiente:

De conformidad con lo prescrito en el Estatuto Orgánico de Gestión Organizacional por Procesos de la Fiscalía General del Estado, el cual en su artículo 9, numeral 1.3.1.1.3, literal c), la Dirección de Tecnologías de la Información y Comunicaciones tiene entre sus atribuciones y responsabilidades:

"1. Planificar y controlar la infraestructura, instalación, configuración y mantenimiento de los recursos tecnológicos requeridos para los servicios de los sistemas informáticos.

2. Monitorear los accesos a los recursos de red, arquitectura de redes y comunicaciones, de acuerdo a los niveles de servicio de la institución;

4. Proponer y desarrollar mediante la innovación de nuevas tecnologías, la automatización de los procesos institucionales"

En virtud de la normativa citada, previo a autorizar al ingeniero Leonardo Rafael Chuquiguanca Vicente, Analista de Investigación 2 de la Dirección de Investigación Civil, la *"IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) EN LA FISCALÍA GENERAL DEL ESTADO"* como su trabajo de fin de Maestría en Ciberseguridad, se solicita a la Dirección de Tecnologías de la Información a su cargo, se sirva emitir su pronunciamiento sobre dicho petitorio.

Una vez está Dirección de Talento Humano cuente con dicho pronunciamiento, procederá a disponer lo que en derecho corresponda.

Particular que solicito para los fines pertinentes.

Atentamente,

Documento firmado electrónicamente

Director de Talento Humano
FISCALÍA GENERAL DEL ESTADO

Figura 43. Memorando de solicitud para pronunciamiento de la dirección de tecnologías con respecto a la implementación del proyecto, Fuente: Fiscalía General del Estado - TTHH

Memorando Nro. FGE-CGP-DTIC-2020-

Quito, 27 de mayo de 2020

PARA:
Director de Talento Humano
FISCALÍA GENERAL DEL ESTADO

ASUNTO: AUTORIZO IMPLEMENTACION

De mi consideración

Autorizo, que el Ing. Leonardo Rafael Chuquiguanca Vicente con C.I. 1104952708, servidor de la Fiscalía General del Estado, realice la implementación de su proyecto "***IMPLEMENTACIÓN DE UNEQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) EN LA FISCALÍAGENERAL DEL ESTADO***", respetando los estándares de seguridad informática y normativa legal vigente, con la finalidad de contribuir con sus estudios finales en la Maestría en Ciber-Seguridad, para el efecto se le ofrece todo lo esté al alcance de nuestra tecnología, bajo la coordinación del Ing. Jorge Moya Polanco, responsable del área de seguridad informática de la dirección, correo electrónico: moyapj@fiscalia.gob.ec.

Atentamente,

Documento firmado electrónicamente

Director/a de Tecnologías de la Información y Comunicaciones
FISCALÍA GENERAL DEL ESTADO

Figura 44. Pronunciamiento y autorización para implementar el proyecto por parte de la dirección de Tecnologías, Fuente: Fiscalía General del Estado - DTIC

BIBLIOGRAFÍA:

Agarwal, Tarun. 2016. "A Basic Collection of Good Practices for Running a CSIRT." 7(11):4585.

APCERT. 2020. "Vision of APCERT." Asia Pacific Computer Emergency Response Team. Retrieved (https://www.apcert.org/about/index.html).

ARCOTEL. 2017. RESOLUCIÓN ARCOTEL-2017-0734. ECUADOR.

ARCOTEL. 2019. "Arcotel Informa - Revista Institucional No.20." ARCOTEL, 12.

ARCOTEL. 2020. "EcuCERT." Agencia de Regulación y Control de Las Telecomunicaciones. Retrieved (http://www.arcotel.gob.ec/ecucert/).

Babulak, E. 2011. "Tutorial 3: Cyber Security: The Importance of CERTs (Computer Emergency Response Teams)." Pp. xxxi–xxxii in 2011 UkSim 13th International Conference on Computer Modelling and Simulation.

Brownlee, N., and E. Guttman. 1998. "RFC 2350: Expectations for Computer Security Incident Response." IETF.

Campis, Luis Eduardo Meléndez, Rafael Domínguez Jiménez, Lina Matoso, and Camilo Castro Escorcia. 2015. "CENTROS DE RESPUESTA ANTE INCIDENTES INFORMÁTICOS: GENERALIDADES Y PROPUESTA METODOLÓGICA." Investigación En Ingeniería de Sistemas e Informática 115.

CERT.br. 2020. "About CERT.Br." Brazilian National Computer Emergency Response Team. Retrieved (https://www.cert.br/about/).

CERTuy. 2014. "Uruguay. Agencia de Gobierno Electrónico y Sociedad de La Información." ITU - Impact Alert Workshop.

CERTuy. 2018. "Estadísticas de Incidentes Del Primer Semestre de 2018." Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Retrieved (https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas).

CERTuy. 2019. "División Centro de Respuesta a Incidentes de Ciberseguridad (CERT)." Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Retrieved (https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/institucional/cometidos/division-centro-de-respuesta-incidentes-de-ciberseguridad).

CHILE, GOBIERNO. 2019. Creación Del Equipo de Respuesta Ante Incidentes de Seguridad Informática (CSIRT). Chile.

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. 2012. "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology." NIST Special Publication 800–61:79.

ColCERT. 2017. "Acerca de ColCERT." Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Retrieved (http://www.colcert.gov.co/?q=acerca-de).

CONPES 3701. 2011. "Lineamientos de Política Para Ciberseguridad y Ciberdefensa." Internet 43.

Cristine, Hoepers. 2019. "FIRST CSIRT Services Framework." LAC-CSIRTs Meeting, LACNIC 32 / LACNOG 2019.

CSIRT_GOB, CHILE. 2019. "Quienes Somos, Visión, Misión , Alcance, Objetivos." Equipo de Respuesta Ante Incidentes de Seguridad Informática. Retrieved (https://www.csirt.gob.cl/quienes-somos/).

CSIRT_GOB, CHILE. 2020. Informe de Seguridad Gestión CSIRT Enero 2020. Santiago.

CSIRT, CHILE. 2019. "Chile Formaliza Creación Del CSIRT de Gobierno." Ministerio Del Interior y Seguridad Pública. Retrieved (https://www.csirt.gob.cl/noticias/chile-formaliza-creacion-del-csirt-de-gobierno/).

CTIRGov. 2019. "Acerca CTIR Gov." Centro de Tratamento e Resposta a Incidentes

Cibernéticos de Governo.
CTIRGov. 2020. “Estatísticas Resultantes Do Trabalho de Detecção, Triagem, Análise e Resposta a Incidentes Cibernéticos.”
EcuCERT. 2020. “EcuCERT - Nosotros.” Centro de Respuesta a Incidentes Informáticos Del Ecuador. Retrieved (https://www.ecucert.gob.ec/nosotros.html).
ENISA. 2006. “Cómo Crear Un CSIRT Paso a Paso.” ENISA I:90.
ENISA. 2018. “Reference Incident Classification Taxonomy Task Force Status and Way Forward.” European Union Agency For Network and Information Security (January):20.
ENISA. 2020. “About ENISA.” The European Union Agency for Cybersecurity. Retrieved (https://www.enisa.europa.eu/about-enisa).
FGE. 2018. Estatuto Orgánico de Gestión Organizacional Por Procesos. Ecuador.
FGE. 2020a. “¿QUÉ ES LA FISCALÍA?” Fiscalía General Del Estado. Retrieved (https://www.fiscalia.gob.ec/institucion/).
FGE. 2020b. Distributivo de Personal de La Institución. Quito.
FIRST. 2019a. Computer Security Incident Response Team (CSIRT) Services Framework Version 2 . 0. Vol. 0.
FIRST. 2019b. “FIRST History.” Forum of Incident Response and Security Teams, Website. Retrieved (https://www.first.org/about/history).
FIRST. 2020a. “CERT.Br Team Information.” Forum of Incident Response and Security Teams, Website. Retrieved (https://www.first.org/members/teams/cert-br).
FIRST. 2020b. “CERTuy Team Information.” Forum of Incident Response and Security Teams, Website. Retrieved (https://www.first.org/members/teams/certuy).
FIRST. 2020c. “EcuCERT Team Information.” Forum of Incident Response and Security Teams, Website. Retrieved (https://www.first.org/members/teams/ecucert).
FIRST. 2020d. “FIRST Vision and Mission Statement.” Forum of Incident Response and Security Teams, Website. Retrieved (https://www.first.org/about/mission).
Howard, John D., and Thomas A. Longstaff. 1998. A Common Language for Computer Security Incidents. (No. SAND98-8667). Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US).
IMPO. 2009. CENTRO NACIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMATICA. FUNCIONAMIENTO Y ORGANIZACION. Uruguay.
INCIBE, CERT. 2020a. Guía Nacional de Notificación y Gestión de Ciberincidentes. Madrid.
INCIBE, CERT. 2020b. “Sodinokibi: Prevención, Identificación y Respuesta.” INCIBE. Retrieved (https://www.incibe-cert.es/blog/sodinokibi-prevencion-identificacion-y-respuesta).
Jezreel, M., M. Mirna, and U. Edgar. 2015. “Services Establishment in the Computer Security Incident Response Teams: A Review of State of Art.” Pp. 1–6 in 2015 10th Iberian Conference on Information Systems and Technologies (CISTI).
LACNIC. 2020. “LACNIC Anuncia La Constitución de Su CSIRT.” LACNIC NEWS. Retrieved (https://prensa.lacnic.net/news/ciberseguridad/lacnic-anuncia-la-constitucion-de-su-csirt).
LACNIC, CSIRT. 2020. “LACNIC CSIRT.” LACNIC CSIRT. Retrieved (https://csirt.lacnic.net/acerca).
Mejía, J., M. Muñoz, and H. Ramírez. 2016. “Proposed Framework for the CSIRT Protection.” Pp. 1–7 in 2016 11th Iberian Conference on Information Systems and Technologies (CISTI).
Mellon, Carnegie. 2015. “Computer Security Incident Response Plan.” Information Security Cffice.
Mellon, Carnegie. 2016. “Columbia Csirt Case Study.” COLUMBIA CSIRT CASE STUDY.
Ministerio de Defensa. 2017. “Grupo de Respuesta a Emergencias Ciberneticas de Colombia.”

ColCERT.
MINTEL. 2018. Libro Blanco de La Sociedad de La Información y Del Conocimiento. Primera ed. Quito.
MINTIC, Ministerio de Tecnologías de la Información y Comunicaciones. 2016. “Guía Para La Gestión y Clasificación de Incidentes de Seguridad de La.” (21).
Miora, Michael, M. E. Kabay, and Bernie Cowens. 2014. “COMPUTER SECURITY INCIDENT RESPONSE TEAMS 1.” 2.
Mooi, R., and R. A. Botha. 2015. “Prerequisites for Building a Computer Security Incident Response Capability.” Pp. 1–8 in 2015 Information Security for South Africa (ISSA).
Nacional, Asamblea. 2008. Constitución de La República Del Ecuador. Ecuador.
OCDE/BID. 2016. Políticas de Banda Ancha Para América Latina y El Caribe.
OEA. 2016. “Buenas Prácticas Para Establecer Un CSIRT Nacional.” Organización de Los Estados Americanos 55.
Prieto, Wilson. 2019. “La Ciberseguridad y Ciberdefensa En Colombia y Los Esfuerzos Interinstitucionales Para Afrontar Las Nuevas Amenazas Emergentes En El Ciberespacio.”
Robert Vargas, Recalde Luis, Reyes Rolando. 2006. “Hacia Una Taxonomía de Incidentes de Seguridad En Internet.” Ingeniería 11(1):37–42.
Rotem, Noam;, and Ran Locar. 2019. “Ecuadorian Breach Reveals Sensitive Personal Data.” VpnMentor. Retrieved (https://www.vpnmentor.com/blog/report-ecuador-leak/).
Ruefle, Robin. 2007. “Defining Computer Security Incident Response Teams.” (January).
Skierka, Isabela, Robert Morgus, Mirko Hohmann, and Tim Maurer. 2015. “CSIRT Basics for Policy-Makers.” Researchgate (May 2015):29.
SNAP. 2013. “Esquema Gubernamental de Seguridad de La Información EGSI.” 1–47.
Stallings, William;, and Lawrie Brown. 2015. Computer Security Principles and Practice. Third Edit.
Tejada, Ester Chicano. 2015. Gestión de Incidentes de Seguridad Informática. IFCT0109. IC Editorial.
Uribe, Edgar. 2014. “Proceso Para La Definición de Servicios Iniciales En Un Equipo de Respuesta Ante Incidencias de Seguridad Informática (CSIRT).” CIMAT Zacatecas.
Vargas, Robert;, Luis; Recalde, and Rolando Reyes. 2017. “Ciberdefensa y Ciberseguridad, Más Allá Del Mundo Virtual: Modelo Ecuatoriano de Gobernanza En Ciberdefensa.” URVIO - Revista Latinoamericana de Estudios de Seguridad (20):31.