Noviembre de 2019

Equipo de intervención en caso de incidente de seguridad informática (EIISI) Marco de servicios

Versión 2.1

Notice: This document describes what the Forum of Incident Response and Security Teams, Inc. (FIRST.Org) believes are best practices. These descriptions are for informational purposes only. FIRST.Org is not liable for any damages of any nature incurred as a result of or in connection with the use of this information.

Índice

Marco de servicios del EIISI

1 Finalidad

El marco de servicios de los equipos de intervención en caso de incidentes de seguridad informática (EIISI) es un documento conceptual que describe de manera estructurada una serie de servicios de seguridad informática y funciones conexas que pueden ofrecer los equipos de intervención en caso de incidentes de seguridad informática y otros equipos que prestan servicios relacionados con la gestión de incidentes. El marco ha sido elaborado por reconocidos expertos de la comunidad FIRST con la firme colaboración de la comunidad de Grupos de Trabajo EIISI (TF-EIISI) y la Unión Internacional de Telecomunicaciones (UIT).

El cometido y finalidad del marco de servicios del EIISI es facilitar el establecimiento y la mejora de las operaciones del EIISI, especialmente para los equipos que están en proceso de elegir, ampliar o mejorar su cartera de servicios. Se describen los posibles servicios que podría prestar un EIISI. No cabe esperar que todos los EIISI presten todos y cada uno de los servicios descritos. Cada equipo tendrá que elegir los servicios necesarios para su cometido y sus integrantes, con arreglo a su mandato.

El marco tiene por objeto ayudar a los equipos, para lo cual se identifican y definen categorías básicas de servicios y sus subcomponentes. Se incluye un título y una descripción para cada servicio, subservicio, función y, opcionalmente, subfunción, según proceda. Este documento constituye el punto de partida para proporcionar un marco de servicios coherente que identifique un conjunto normalizado de términos y definiciones para toda la comunidad. Obsérvese que en este documento no se explica cómo construir o mejorar un EIISI o equipo correspondiente. Este tipo de información está disponible en otros documentos, algunos de los cuales se enumeran en el Anexo 1 como recursos auxiliares.

En este marco de servicios del EIISI no se formulan sugerencias ni recomendaciones sobre la capacidad, la aptitud, la madurez o la calidad de ningún tipo de EIISI en particular. Esos temas son importantes por el valor que aporta cualquier EIISI a sus mandantes, pero se han omitido deliberadamente en este documento marco. Además, este marco no examina la puesta en práctica de ningún servicio en particular, ni propone forma específica alguna para ello. Es importante comprender que esos servicios pueden aplicarse de muchas maneras diferentes, sin dejar de garantizar que se cumplan las expectativas razonables de los mandantes e interesados.

2 Introducción y antecedentes

El equipo de intervención en caso de incidentes de seguridad informática (EIISI) es una unidad orgánica (que puede ser virtual) o una capacidad que presta servicios y apoyo a una agrupación concreta para prevenir, detectar, gestionar y reaccionar ante incidentes de seguridad informática, de conformidad con su cometido.

Cuando está debidamente creado, el EIISI tiene un mandato claro, un modelo de gobernanza, un marco de servicios adaptado, tecnologías y procesos para proporcionar, medir y mejorar continuamente los servicios definidos.

Diversas entidades de la comunidad de EIISI han ido elaborando a lo largo de los años su propia lista o marco de servicios. Con la evolución de la tecnología, las herramientas y los procesos, la comunidad reparó en que había temas y actividades que faltaban en las listas existentes. El FIRST, interesado en permitir el desarrollo y consolidación mundial de los EIISI, reconoció que se trataba de aspecto fundamental para elaborar un lenguaje común a todos los EIISI y a otras entidades con las que colaboran. Dada la amplitud geográfica y funcional de la composición del FIRST, se determinó que la comunidad que lo constituye sería una fuente adecuada para la definición y representación definitiva de los servicios prestados por los EIISI. Basándose en esta premisa, se puso en marcha un planteamiento común con el fin de perfeccionar el marco de servicios del EIISI y en 2017 se publicó una versión preliminar.

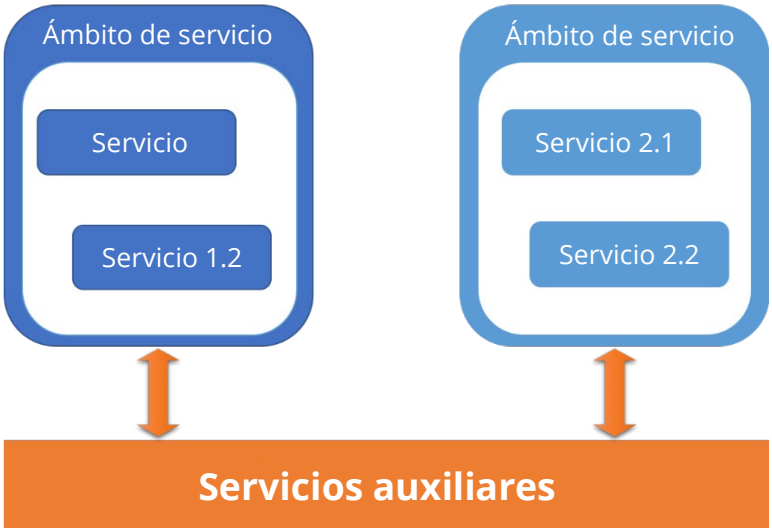
Desde entonces, se ha adoptado un planteamiento similar para elaborar un marco de servicios de los equipos de intervención en caso de incidentes de seguridad en los productos (EIISP), en reconocimiento de muchos aspectos operativos que requieren un conjunto diferente de servicios y actividades correspondientes. Todos los marcos de servicios pueden consultarse en el sitio web del FIRST.[1]

La presente es una versión mejorada de la segunda versión del marco de servicios del EIISI. Basándose en las opiniones recabadas de varios expertos sobre la primera versión, diversas partes han sido reestructuradas y ampliadas para esta edición. En particular, se han eliminado las actividades internas, por cuanto éstas no constituyen ofertas de servicios a los mandantes. Las actividades internas y externas en apoyo al ciclo vital completo de cualquier oferta de servicios pueden organizarse en servicios y funciones, al igual que los servicios designados destinados a los mandantes. Esos servicios y funciones se conocen principalmente como servicios auxiliares. Como ejemplos cabe citar las actividades administrativas, como la gestión del personal y la contratación, el reembolso de los gastos de viaje o la organización de actividades de formación.[2]

Según nuestros conocimientos, hay maneras muy diferentes de prestar tales servicios auxiliares, en su mayoría dependen de la organización que integra el EIISI o de las ofertas de servicios conexos. Por ejemplo, la contratación y la gestión del personal es sin duda necesaria para dar soporte al EIISI, pero se considera una tarea típica de apoyo institucional y no específica de los EIISI.

[1] https://www.first.org/standards/frameworks/csirts/ para materiales relacionados con los EIISI.

[2] Check [Kossakowski 2001] analiza los servicios auxiliares internos y su relación con otros servicios.



Aunque los servicios y funciones internas permiten vertebrar cualquier equipo o unidad organizativa para que puedan desempeñar su cometido, tales servicios auxiliares se consideran fuera de alcance y no se detallan ni analizan en los marcos de servicios de FIRST.

Dado que los EIISI continuarán afrontando los cambiantes retos para proteger a sus integrantes contra las nuevas amenazas, en futuras versiones se revisarán, examinarán y ampliarán o enmendarán, según procede, los servicios contemplados por este marco.[3]

3 Diferencia entre un EIISI y un EIISP

Las principales diferencias entre el EIISI de la organización y otros equipos de seguridad en la misma organización, como los EIISP radican en que en los primeros se hace hincapié en los mandantes y los servicios ofrecidos. Por regla general, el hecho diferenciador fundamental entre el EIISP y cualquier otro equipo de seguridad, en particular los EIISI, dentro de una organización es que el EIISP se concentra en los productos.

Dentro de una organización, el EIISI corporativo se concentra en la seguridad de los sistemas y redes informáticas que constituyen la infraestructura de dicha organización. Si una organización grande dispone de múltiples equipos de seguridad y EIISI, uno de ellos puede ejercer de coordinador y punto de contacto exclusivo con las partes externas. Esos equipos se denominan EIISI coordinadores.

Los EIISI coordinadores se establecen también como entidades independientes que prestan servicios a un conjunto específico de personas y/u organizaciones denominado agrupación. Las organizaciones que pertenecen a una agrupación específica comparten algunas características comunes (como formar parte de una red nacional de investigación o pertenecer a un país

[3] Se ha creado un Grupo de Interés Especial (SIG) de FIRST para dirigir el "Desarrollo del marco EIISI".

concreto). El EIISI coordinador actúa como punto de contacto exclusivo para todo el grupo y se dedica a aspectos de seguridad general de estas organizaciones.

En la actualidad, los EIISI nacionales se han establecido como un tipo distintivo del EIISI coordinador para facilitar y a menudo coordinar las actividades de los EIISI dentro de un determinado país u ofrecer servicios limitados para todos los ciudadanos, sectores específicos de entidades de infraestructura esencial, etc. de dicho país.

Si bien existen importantes diferencias entre los EIISI y EIISP, es importante saber que también existen sinergias entre ambos. Es importante tener presente que los EIISI y EIISP no actúan de manera independiente entre sí, ya que, por ejemplo, muchos EIISI advierten a sus integrantes sobre vulnerabilidades de la seguridad, advertencias que casi siempre se basan en la información proporcionada por los EIISP de los proveedores.

4 Estructura del marco de servicios EIISI

El marco de los servicios EIISI se basa en las relaciones de cuatro elementos fundamentales:

ÁMBITOS DE SERVICIO → SERVICIOS → FUNCIONES → SUBFUNCIONES

Estos elementos se definen así:

ÁMBITOS DE SERVICIO

Los ámbitos de servicio agrupan los servicios relacionados con un aspecto común, lo que ayuda a organizar los servicios en categorías generales para facilitar el entendimiento y la comunicación. La especificación de cada servicio incluye un campo "descripción" que contiene un texto explicativo general en el que se describe el ámbito de servicio y la lista de servicios de cada uno de dichos ámbitos.

SERVICIOS

Por servicio se entiende el conjunto de funciones reconocibles y coherentes orientadas a resultados específicos. Dichos resultados son los previstos o exigidos por los integrantes o por una entidad a través de sus interesados o representantes.

Los servicios se especifican con la siguiente plantilla:

- campo "descripción", que se describe la naturaleza del servicio;
- campo "finalidad", que describe la finalidad del servicio;
- campo "resultado", que describe los resultados cuantificables del servicio.

FUNCIONES

Por función se entiende la actividad o conjunto de actividades destinadas a cumplir la finalidad de un determinado servicio. Se puede compartir y utilizar cualquier función en el contexto de diversos servicios.

Las funciones se describen mediante la siguiente plantilla:

- campo "descripción", que describe la función;
- campo "finalidad", que describe la finalidad de la función;
- campo "resultado" que describe resultados cuantificables de la función;
- lista de subfunciones que pueden realizarse en el marco de la función.

SUBFUNCIONES

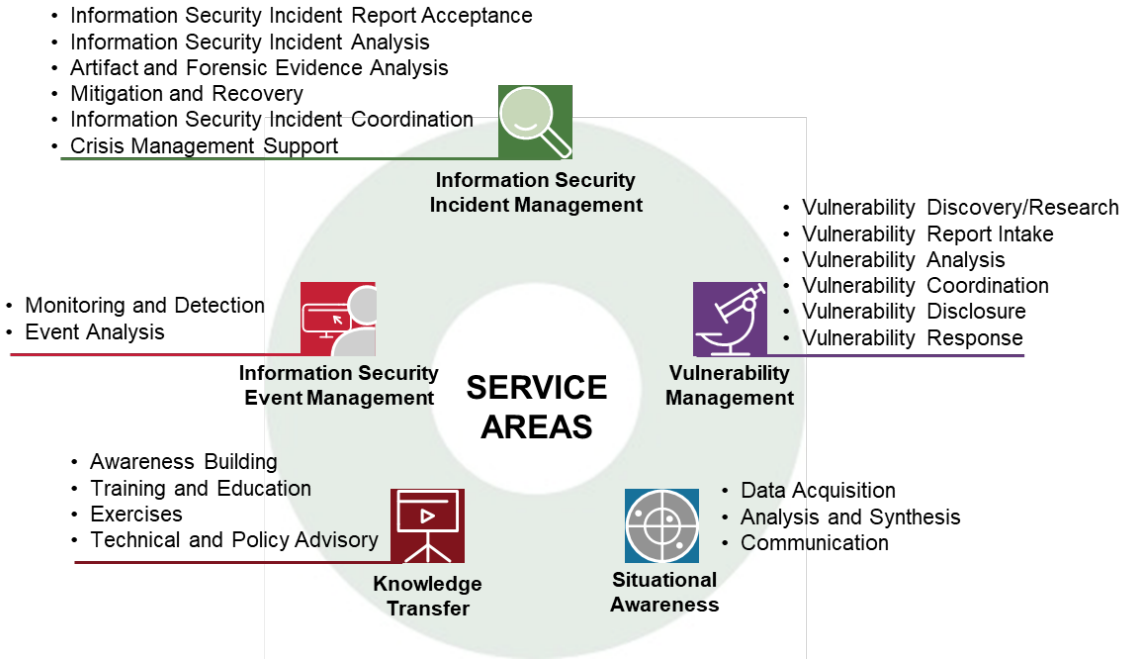
Por subfunción se entiende la actividad o conjunto de actividades destinadas a cumplir la finalidad de una determinada función. Se puede compartir y utilizar cualquier subfunción en el contexto de diversos servicios y/o funciones. Opcionalmente, las subfunciones pueden realizarse o requerirse para cualquiera de esas funciones y/o servicios.

Las subfunciones se describen mediante la siguiente plantilla:

- campo "descripción", que describe la función;
- campo "finalidad", que describe la finalidad de la función;
- campo "resultado" que describe resultados cuantificables de la función.

A los efectos del marco de servicios del EIISI no se han descrito completamente las subfunciones. Sólo se ofrece una breve caracterización de cada una de ellas.

En la figura siguiente se muestran (página siguiente) los servicios y los ámbitos de servicio del marco de servicios del EIISI. En el Apéndice 4 figura un cuadro con todos los ámbitos de servicio, servicios y funciones.



Leyenda de la Figura
ÁMBITOS DE SERVICIO
Gestión de incidentes de seguridad de la información; *Aceptación del informe sobre incidentes de seguridad de la información; Análisis de incidentes de seguridad de la información; Análisis de artefactos y pruebas forenses; Mitigación y recuperación; Coordinación de incidentes de seguridad de la información; Ayuda en la gestión de crisis*
Gestión de eventos de seguridad de la información; *Supervisión y detección; Análisis de eventos*
Transferencia de conocimientos; *Concienciación; Formación y educación; Ejercicios; Asesoría técnica y política*
Gestión de vulnerabilidades; *Detección/investigación de vulnerabilidades; Admisión de informes sobre vulnerabilidades; Análisis de vulnerabilidades; Coordinación de vulnerabilidades; Divulgación de vulnerabilidades; Respuesta a vulnerabilidades*
Consciencia coyuntural; *Adquisición de datos; Análisis y síntesis; Comunicación*

5 Ámbito de servicio: Gestión de eventos de seguridad de la información

La gestión de eventos de seguridad de la información tiene por objeto identificar los incidentes de seguridad de la información a partir de la correlación y el análisis de los eventos de seguridad de muy diversos eventos y fuentes de datos contextuales. En las organizaciones más grandes, este ámbito de servicio a veces se asigna total o parcialmente a un Centro de Operaciones de Seguridad (SOC), que además puede realizar la gestión de incidentes de seguridad de la información de primer o incluso segundo nivel, como el inicio de mitigaciones o ajustes de los controles de seguridad. Dado que cualquier servicio de gestión de incidentes de seguridad de la información depende de datos cualificados y precisos sobre los eventos de seguridad de la información, la interfaz entre el SOC y el EIISI asignado es crucial.[4]

Los siguientes servicios se consideran parte de la oferta de este ámbito de servicios concreto:

- supervisión y detección;
- análisis de eventos.

5.1 Servicio: Supervisión y detección

Finalidad: Poner en marcha un procesamiento automatizado y continuo de muy diversas fuentes de incidentes de seguridad de la información y datos contextuales a fin de identificar posibles incidentes de seguridad de la información, como ataques, intrusiones, filtración de datos o infracciones de la política de seguridad.

Descripción: Basándose en registros, datos de NetFlow, alertas de IDS, redes de sensores, fuentes externas u otros datos de eventos de seguridad de la información disponibles, aplicar una serie de métodos, que van desde la lógica simple o las reglas de concordancia de patrones hasta la aplicación de modelos estadísticos o el aprendizaje automático para identificar posibles incidentes de seguridad de la información. Dicha identificación podría entrañar el procesamiento de grandes volúmenes de datos y por lo general, aunque no necesariamente, se habrá de recurrir a herramientas especializadas como gestión de eventos e información de seguridad (SIEM) o plataformas de macrodatos. Un objetivo importante de la mejora continua es reducir al mínimo el número de falsas alarmas que se han de analizar en el contexto del servicio de análisis.

Resultado: Se identifican los posibles incidentes de seguridad de la información para su análisis en el contexto del servicio de Análisis.

[4] Si bien este marco de servicios no tiene por objeto definir un marco de servicios SOC, cabe esperar que los servicios de los ámbitos de gestión de eventos e incidentes de seguridad de la información resulten útiles y directamente aplicables al definir los servicios SOC.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- gestión de registros y sensores;
- gestión de casos de uso de detección;
- gestión de datos contextuales.

5.1.1 Función: Gestión de registros y sensores

Finalidad: Gestionar fuentes de registro y los sensores.

Descripción: Los sensores y las fuentes de registro necesitan una gestión operativa a lo largo de su ciclo de vida. Se deben desplegar, incorporar y desmantelar. También se deben identificar y resolver las interrupciones, la calidad y el alcance de los datos y los problemas de configuración. Los sensores que tienen algún tipo de configuración, como patrones definidos, deben mantener su configuración para poder ser eficaces. Los sensores también pueden incluir servicios de detección externos o fuentes de inteligencia de código abierto (OSINT), si constituyen la base de los casos de uso de detección.

Resultado: Se dispone de un flujo fiable de eventos de seguridad de la información, que se utilizará para detectar casos de utilización.

5.1.2 Función: Gestión de casos de utilización sobre detección

Finalidad: Gestionar la cartera de casos de utilización sobre detección a lo largo de todo el ciclo de vida.

Descripción: Se elaboran, prueban y mejoran nuevos métodos de detección, que finalmente se incorporan a un caso detección en la producción. Es necesario elaborar instrucciones para la clasificación, la calificación y la correlación de los analistas, por ejemplo, en forma de guías y procedimientos operativos normalizados (PON). Es necesario mejorar, redefinir o abandonar los casos de utilización que no funcionan bien, es decir, que tienen una relación beneficio/esfuerzo desfavorable. La cartera de casos de utilización sobre detección debe ampliarse de manera orientada a los riesgos y de manera coordinada con los controles preventivos.

Resultado: Se ha elaborado una cartera de casos de utilización sobre detección efectiva que son pertinentes para los integrantes.

5.1.3 Función: Gestión de datos contextuales

Finalidad: Gestión de las fuentes de datos contextuales para la detección y acumulación.

Descripción: Las diversas fuentes de datos contextuales que intervienen en la detección y la acumulación se deben gestionar a lo largo de su ciclo de vida. Pueden ser API dinámicas o exportaciones de otros sistemas informáticos, como una base de datos de gestión de la configuración (CMDB), administración de identidades y acceso (IAM) o sistemas Intel de amenazas, o conjuntos de datos completamente separados que deben administrarse manualmente. Este último sería el caso de listas de indicadores, listas de vigilancia y listas blancas para eliminar falsos positivos.

Resultado: Se dispone de datos contextuales actualizados para la detección y acumulación.

5.2 Servicio: Análisis de eventos

Finalidad: La selección de posibles incidentes de seguridad de la información detectados y su clasificación como incidentes de seguridad de la información para su tramitación por el ámbito de servicio de gestión de incidentes de seguridad de la información o para descartarlos como falsa alarma.

Descripción: Cada flujo de posibles incidentes de seguridad de la información detectados se debe examinar y clasificar como incidente de seguridad de la información (verdadero positivo) o bien como falsa alarma (falso positivo) mediante análisis manual y/o automatizado. A tal efecto podría ser necesario recopilar manual o automáticamente información adicional, dependiendo del caso de utilización sobre detección. Debe darse prioridad al análisis de incidentes de seguridad de la información potencialmente más críticos para poder reaccionar de manera oportuna a lo más importante. La clasificación estructurada de los posibles incidentes de seguridad de la información detectados permite una mejora continua y efectiva de manera directa mediante la identificación de los casos de utilización sobre la detección, las fuentes de datos o los procesos con problemas de calidad.

Resultado: Los incidentes de seguridad de la información clasificados y correlacionados están disponibles como parámetros del ámbito de servicio de gestión de incidentes de seguridad de la información y los falsos positivos están clasificados para mejorar constantemente.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- correlación;
- clasificación.

5.2.1 Función: Correlación

Finalidad: Identificar eventos directamente relacionados con incidentes de seguridad posibles o en curso.

Descripción: Los posibles incidentes de seguridad de la información relacionados con los mismos activos (por ejemplo, sistemas, servicios, clientes) o identidades (por ejemplo, usuarios), o que, en cambio, están directamente relacionados con otros posibles incidentes de seguridad de la información, se agrupan y se tramitan como un único incidente de seguridad de la información a fin de evitar la duplicación de tareas. Los posibles nuevos incidentes de seguridad de la información directamente relacionados con incidentes de seguridad de la información en curso se asignan a ese incidente de seguridad de la información en lugar de abrir un nuevo incidente de seguridad de la información separado.

Resultado: Se agrupan los posibles incidentes de seguridad de la información relacionados para la clasificación combinada o se actualiza un incidente de seguridad de la información existente ya tramitado por el ámbito de servicio de gestión de incidentes de seguridad de la información.

5.2.2 Función: Clasificación

Finalidad: Selección y clasificación de posibles incidentes de seguridad detectados para identificar, clasificar y priorizar verdaderos positivos.

Descripción: Los posibles incidentes de seguridad de la información se deben seleccionar y clasificar como incidente de seguridad de la información (verdadero positivo) o falsa alarma (falso positivo). Como los analistas sólo pueden analizar un número limitado de posibles incidentes de seguridad de la información, y para evitar el cansancio causado por las alertas, la automatización resulta fundamental. Constar con herramientas consolidadas facilita la selección eficaz al nutrirse de información contextual, asignar puntuaciones de riesgo basadas en la importancia de los activos e identidades afectados y/o identificar automáticamente los eventos de seguridad de la información. Se deben determinar y automatizar los casos recurrentes que pueden automatizarse. Los posibles incidentes de seguridad de la información de mayor gravedad deberían analizarse antes que los menos graves. Además de clasificarlos como verdaderos o falsos positivos, es importante una clasificación más detallada para mejorar continuamente los casos de utilización sobre detección, así como la gestión de fuentes de registro, sensores y fuentes de datos contextuales. La clasificación más detallada también contribuye a definir los IFR con mayor calidad para medir el éxito de este ámbito de servicio.

Resultado: Se pueden tramitar posibles incidentes de seguridad de la información en el marco del ámbito de servicio de la gestión de incidentes de seguridad de la información.

6 Ámbito de servicio: Gestión de incidentes de seguridad de la información

Este ámbito de servicio constituye el núcleo de todo EIISI y consiste en servicios que son esenciales para ayudar a los mandantes durante un ataque o incidente. Los EIISI deben estar preparados para ayudar y apoyar. Gracias a esta posición y experiencia únicas, son capaces no sólo de recopilar y evaluar informes de incidentes de seguridad de la información, sino también de analizar los datos relevantes y realizar un análisis técnico detallado del propio incidente y de cualquier dispositivo utilizado.

A partir de este análisis, se pueden recomendar medidas de mitigación y de recuperación del incidente, y se ayudará a los mandantes a aplicar las recomendaciones. Para ello también se requiere la coordinación con entidades externas como los EIISI o expertos en seguridad, proveedores o EIISP para resolver todos los aspectos y reducir el número de ataques exitosos en el futuro.

Los conocimientos especializados que aportan los EIISI son también decisivos para hacer frente a las crisis (de seguridad de la información). Si bien en muchos casos el EIISI no se encargará de gestionar la crisis, puede ayudar en cualquier actividad de ese tipo. El hecho de que sus contactos estén disponibles, por ejemplo, puede mejorar en gran medida la aplicación de las medidas de mitigación necesarias o los mecanismos de protección.

La aplicación de los conocimientos y la infraestructura disponible para ayudar a sus mandantes resulta esencial para mejorar la gestión general de los incidentes de seguridad de la información.

Se considera que los siguientes servicios forman parte de la oferta de este ámbito de servicio:

- aceptación del informe de incidentes de seguridad de la información;
- análisis de incidentes de seguridad de la información;
- análisis de dispositivos y pruebas forenses;
- mitigación y recuperación;
- coordinación de incidentes de seguridad de la información;
- ayuda en la gestión de crisis.

6.1 Servicio: Aceptación del informe de incidentes de seguridad de la información

Finalidad: Recibir y procesar informes de posibles incidentes de seguridad de la información remitidos por los mandantes, los servicios de gestión de eventos de seguridad de la información o por terceros.

Descripción: Para el EIISI, la tarea más importante es la aceptación de los informes sobre los eventos de seguridad de la información y los posibles incidentes de seguridad de la

información que afecten a las redes, dispositivos, componentes, usuarios, organizaciones o la infraestructura –a los que se hace referencia como "víctimas"– en el conjunto de mandantes. El EIISI debe prever que los posibles incidentes de seguridad de la información puedan proceder de diversas fuentes en diversos formatos, tanto manuales como automáticos.

Para que los mandantes puedan notificar los incidentes de seguridad de la información con mayor eficacia, el EIISI debería proporcionar uno o varios mecanismos, así como una guía o instrucciones sobre qué se debe notificar, y cómo hacerlo con toda seguridad, en caso de incidente de seguridad de la información. Los mecanismos de denuncia pueden ser el correo electrónico, un sitio web, un formulario o portal dedicado a la denuncia de incidentes de seguridad de la información u otros métodos adecuados para presentar informes de manera segura. La guía para la presentación de informes, si no se incluyen en el propio formulario de presentación de informes sobre incidentes de seguridad de la información, deben proporcionarse en un documento separado o en una página web, y deben enumerar la información específica que es conveniente incluir en el informe.

Debido al número potencialmente elevado de posibles incidentes de seguridad de la información tramitados automáticamente que se detectan a través del servicio de gestión de eventos de seguridad de la información, debe preverse dicho número antes de adoptar esas interfaces o de autorizar los mandantes a utilizarlas.[5]

Resultado: Se reciben informes de incidentes de seguridad de la información en un formato profesional y coherente a partir de cada informe, así como su validación y clasificación inicial.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- recepción del informe de incidentes de seguridad de la información;
- selección y tramitación de incidentes de seguridad de la información.

6.1.1 Función: Admisión de informes sobre incidentes de seguridad de la información

Finalidad: Aceptar o recibir información sobre un incidente de seguridad de la información, notificado por mandantes o terceros.

Descripción: La admisión efectiva de los informes sobre incidentes de seguridad de la información requiere mecanismos y procesos para recibir los informes de los mandantes, los interesados y de terceros (por ejemplo, detectores, investigadores, ISAC y otros EIISI). Los informes de incidentes de seguridad de la información pueden incluir dispositivos/redes/usuarios/organizaciones afectados, las condiciones ya identificadas como vulnerabilidades explotadas, el impacto tanto a nivel técnico como empresarial, y las acciones

[5] Como es de esperar, todos los servicios relacionados con la adquisición de información y datos presentan muchas similitudes. Por consiguiente, es frecuente combinar esos servicios ofrecidos de varios ámbitos de servicio en un solo servicio/función. Aunque no es obligatorio y no hay una combinación establecida de ámbitos de servicios, hemos optado por mantener esos servicios por separado dentro del marco de servicios del EIISI, aunque cada equipo es libre de elegir el mejor modelo de organización que más se adapte a su configuración.

que se han tomado para iniciar medidas de reparación y/o mitigación y su posible resolución. En ocasiones, la información sobre incidentes de seguridad de la información puede recibirse junto con información de otros servicios, concretamente junto con la admisión de informes sobre vulnerabilidades (por ejemplo, si se notifica un incidente de seguridad de la información que se ha identificado al analizar un informe de vulnerabilidades). Se puede o no acusar recibo de los informes presentados automáticamente, en espera de otras decisiones de las interfaces y protocolos implementados.

Resultado: Se tramitan adecuadamente los informes de incidentes de seguridad de la información presentados por los mandantes o terceros, en particular el inicio de la documentación o el seguimiento de los informes.

Se considera que las siguientes subfunciones forman parte de esta función:

- supervisar periódicamente los canales de comunicación y comprobar si los medios anunciados para ponerse en contacto con el EIISI están operativos y se pueden presentar informes;
- realizar un acuse de recibo inicial al remitente del informe de incidentes de seguridad de la información, solicitar información adicional, si procede, y establecer expectativas con el remitente.

6.1.2 Función: Clasificación y tramitación de incidentes de seguridad de la información

Finalidad: Examen preliminar, catalogar, priorizar y tramitar el incidente de seguridad de la información notificado.

Descripción: Los informes sobre incidentes de seguridad de la información se examinan y se clasifican para hacerse una idea inicial del incidente de seguridad de la información del caso. Reviste especial importancia determinar si puede tener repercusiones reales sobre la seguridad de la información y puede causar (o ya ha causado) daños a la confidencialidad, disponibilidad, integridad y/o autenticidad de los bienes de información u otros activos. Dependiendo de la calidad y grado de detalle de la información proporcionada en el informe inicial, puede o no ser evidente si se ha producido un verdadero incidente de seguridad de la información o si existe una causa diferente, por ejemplo, un error de configuración o un fallo del *hardware*. El siguiente paso se determinará mediante evaluación preliminar (por ejemplo, procesar el informe para su análisis ulterior; solicitar información adicional al remitente o de otras fuentes; decidir que no es necesario actuar o que es una falsa alarma).

Es posible que los ataques se originen en los mandantes del EIISI, que se dirijan contra ellos o que los mandantes se vean afectados únicamente por efectos colaterales. Si el EIISI no presta servicios de gestión de la seguridad de la información para las víctimas identificadas, entonces el informe deberá remitirse de manera segura a un grupo externo para su gestión, como las organizaciones afectadas o los EIISI.

A menos que haya una razón para rechazar el informe de incidentes de seguridad de la información o que el informe se haya remitido a otra entidad responsable de su tramitación, el

informe deberá transmitirse al servicio de análisis de vulnerabilidades para su ulterior examen, análisis y tramitación.

Resultado: Puede determinarse si el incidente notificado es efectivamente un incidente de seguridad de la información que debe ser tramitado por el EIISI o transmitido a otra entidad pertinente.

Se considera que las siguientes subfunciones forman parte de la implementación de este servicio:

- tramitar los informes y datos presentados, incluidos los dispositivos o artefactos de forma aislada, para proteger la integridad del entorno laboral y evitar ataques exitosos contra el EIISI por esos medios;
- actualizar el acuse de recibo de los informes proporcionando alguna retroalimentación sobre las medidas ulteriores basadas en los resultados disponibles de la categorización o el establecimiento de prioridades;
- fusionar la nueva información sobre los incidentes de seguridad de la información ya tramitados con los datos disponibles para permitir un análisis y un procesamiento coherentes.

6.2 Servicio: Análisis de incidentes de seguridad de la información

Finalidad: Analizar y comprender mejor los incidentes de seguridad de la información confirmados.

Descripción: Este servicio consiste en funciones para comprender los incidentes de seguridad de la información y sus repercusiones reales y potenciales, a fin de detectar los problemas o vulnerabilidades o deficiencias subyacentes (causas fundamentales) que hicieron posible el éxito del ataque, la transgresión o la explotación.

El análisis detallado suele ser complejo y requiere mucho tiempo. El objetivo es identificar y caracterizar el incidente de seguridad de la información con un grado de detalle que permita la comprensión actual de su impacto. Los incidentes de seguridad de la información pueden caracterizarse por su alcance, las entidades afectadas, los instrumentos o los ataques desplegados, los plazos, etc. Este servicio puede continuar en paralelo mientras se ofrece el servicio y las funciones de coordinación de los incidentes de seguridad de la información o se adoptan medidas de mitigación/recuperación.

El EIISI puede utilizar otra información y su propio análisis (más adelante se describen algunas opciones) o los conocimientos disponibles de los proveedores y los equipos de seguridad de los productos o los investigadores de seguridad para comprender mejor lo que ha ocurrido y qué medidas adoptar para remediar las pérdidas o los daños.

Resultado: Se conocen mejor los detalles clave del incidente de seguridad de la información (por ejemplo, la descripción, el impacto, el alcance, los ataques/explotaciones y las soluciones).

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- clasificación de incidentes de seguridad de la información (prioridades y clasificación);
- recopilación de información;
- coordinación de análisis detallados;
- análisis de causas fundamentales del incidente de seguridad de la información;
- correlación entre incidentes.

6.2.1 Función: Clasificación de incidentes de seguridad de la información (prioridades y clasificación)

Finalidad: Clasificar, priorizar y crear una evaluación inicial del incidente de seguridad de la información.

Descripción: El servicio de análisis de incidentes de seguridad de la información comienza con un examen de la información disponible para clasificar, priorizar y evaluar el impacto que los incidentes de seguridad de la información tiene en los sistemas implicados sujetos al mandato del EIISI. Parte de esta información puede haberse documentado durante la función de clasificación y procesamiento de informes de incidentes de seguridad de la información (del servicio de admisión de informes de incidentes de seguridad de la información) si el incidente de seguridad de la información fue comunicado al EIISI por un mandante o un tercero.

Si aún no se ha completado la clasificación previa, el incidente de seguridad de la información puede asignarse a un experto en la materia para que realice una confirmación técnica de que el incidente tiene alguna incidencia en los sistemas implicados y es relevante para el mandato del EIISI (es decir, un posible impacto de seguridad en las redes o sistemas que puede resultar en un daño a la confidencialidad, disponibilidad o integridad de los activos de información en un área del EIISI de acuerdo con su mandato).

Resultado: Se clasifica, prioriza y actualiza el registro de información de un incidente de seguridad de la información.

6.2.2 Función: Recopilación de información

Finalidad: Admitir, catalogar, almacenar y rastrear información relativa al incidente de seguridad de la información y a todos los eventos de seguridad de la información que se consideren parte del mismo.

Descripción: Permitir la recopilación de toda la información útil para comprender mejor el contexto, de modo que el origen y el contenido de la información se puedan evaluar y etiquetar adecuadamente para cualquier procesamiento posterior.

Al recabar la información, se deben aceptar y respetar las políticas de compartición acordadas y las limitaciones sobre qué datos pueden utilizarse en cada contexto o para qué tipo de procesamiento. Asimismo, los mecanismos y procedimientos de recopilación deben garantizar el adecuado etiquetado y la atribución de las fuentes a fin de validar posteriormente los orígenes, la idoneidad y la autenticidad.

Resultado: Se dispone de información estructurada sobre metadatos o datos digitales y no digitales recopilados, con información de rastreo y puntos de control de la integridad tanto en lo relativo a la tramitación como al almacenamiento. Dependiendo de si los resultados se utilizarán para futuros análisis (informales) o para actividades de fiscalización, existen diferentes requisitos con respecto al establecimiento de una cadena de custodia oficial que pueda defenderse en los tribunales en alguna etapa posterior.

Se considera que las siguientes subfunciones forman parte de la implementación de esta función:

- evaluación y validación de las fuentes de información que proporcionan datos e información;
- recopilación de informes sobre eventos maliciosos o sospechosos, eventos de seguridad de la información, posibles incidentes de seguridad de la información en trámite y/o informes de incidentes de seguridad de la información de mandantes y terceros (como otros equipos de seguridad o fuentes de inteligencia comercial), ya sea de manera manual, automatizada o legible por máquina;
- recopilación y catalogación de datos digitales que pueden ser, pero no se garantiza que lo sean, útiles para comprender la actividad del incidente (por ejemplo, imágenes de disco y memoria, archivos con metadatos o sumas de verificación, características de la arquitectura de la red, registros); estos datos son, entre otros, los artefactos considerados como restos de la actividad agresora;
- recopilación y catalogación de datos no digitales (por ejemplo, hojas de registro físico, diagramas de arquitectura, modelos empresariales, datos de evaluación de sitios, políticas, marcos de riesgo empresarial);
- recopilación y catalogación de metadatos relativos a la fuente, el método de recopilación, las personas que han manipulado datos u objetos, el propietario y la información de custodia, especialmente porque pueden considerarse como pruebas para el análisis forense o las actividades de fiscalización ulteriores.

6.2.3 Función: Coordinación de análisis detallado

Finalidad: Iniciar y rastrear cualquier otro análisis técnico sobre el incidente de seguridad de la información.

Descripción: Como podría ser necesario realizar un análisis técnico más detallado, ese análisis puede ser efectuado por otros expertos (dentro o fuera de la organización anfitriona o del EIISI) o por otros terceros (como un proveedor de servicios especializado en ese análisis). Para ello es necesario iniciar y rastrear esas actividades hasta haber llevado a buen término el análisis deseado.

Resultado: Se dispone de una lista de análisis pendientes y subcontratados – desde el punto de vista del encargado del incidente que coordina la respuesta a los incidentes de seguridad de la información.

6.2.4 Función: Análisis de la causa fundamental del incidente de seguridad de la información

Finalidad: Identificar la causa fundamental del incidente de seguridad de la información, de las circunstancias que permitieron que las vulnerabilidades explotadas o que permitieron que la explotación tuviera éxito (por ejemplo, el comportamiento del usuario).

Descripción: Esta función implica el proceso y las acciones necesarias para comprender la arquitectura, el uso o los fallos de implementación que causaron o expusieron los sistemas, las redes, los usuarios, las organizaciones, etc., al tipo de ataque o explotación o vulneración que se ejerció contra la víctima del incidente de seguridad de la información. También se ocupa de las circunstancias en que, una vez logrado el acceso inicial, el atacante podría comprometer más sistemas para obtener más acceso.

En función de la naturaleza del incidente de seguridad de la información, puede resultar difícil para un EIISI desempeñar cabalmente esta función. En muchas situaciones, lo mejor es que sea el propio afectado el que desempeñe esta función, ya que, especialmente en el contexto de los EIISI de coordinación, no se dispone de conocimientos técnicos detallados sobre los sistemas o redes que se han visto comprometidos.

Resultado: Se conoce el incidente de seguridad de la información y la forma en que los agresores obtuvieron inicialmente acceso y lo utilizaron después, a fin de poder determinar métodos de solución o mitigación para reducir al mínimo el riesgo de exposición o explotación futuras eliminando las causas fundamentales.

6.2.5 Función: Correlación entre incidentes

Finalidad: Permitir el uso de toda la información disponible para comprender mejor el contexto y detectar interrelaciones que de otro modo no se habrían reconocido ni habrían permitido actuar.

Descripción: Esta función implica la correlación de la información disponible sobre múltiples incidentes de seguridad de la información para determinar las interrelaciones, tendencias o mitigaciones aplicables a partir de incidentes de seguridad de la información ya cerrados para mejorar la respuesta a los incidentes de seguridad de la información en trámite.

Resultado: Comprender el panorama general, en cuanto a consciencia coyuntural, a partir del conocimiento detallado de las similitudes y las interrelaciones confirmadas o sospechadas de incidentes de seguridad de la información que de otra manera parecerían independientes.

6.3 Servicio: Análisis de los artefactos y de pruebas forenses

Finalidad: Analizar y comprender los artefactos relacionados con un incidente confirmado de seguridad de la información, habida cuenta de la necesidad de preservar las pruebas forenses.

Descripción: Los servicios relacionados con la comprensión de las capacidades y la intención de los artefactos (por ejemplo, *malware*, ataques, volcados de memoria volátil o copias de disco, códigos de aplicaciones, registros, documentos), los mecanismos utilizados, su propagación, detección, mitigación y su desarme o neutralización. Esto se aplica a todos los formatos y

fuentes: *hardware*, *firmware*, memoria, *software*, etc. Todo artefacto o prueba debe ser preservado y recopilado sin alteración alguna, y mantenerse aislado. Dado que ciertos artefactos y datos pueden acabar convirtiéndose en pruebas en el contexto de las actividades de fiscalización, quizá tengan que aplicarse reglamentos o requisitos específicos.

Aun cuando no se preserve una cadena de custodia, este servicio suele implicar tareas complejas que requieren mucho tiempo y conocimientos especializados, la creación de entornos de análisis dedicados y supervisados, con o sin accesos externos desde redes estándar alámbricas o inalámbricas (como la realización de las actividades forenses en una sala sellada o de Faraday), el registro de actividad y el cumplimiento de procedimientos.

Como parte del tratamiento de los incidentes de seguridad de la información, pueden encontrarse artefactos digitales en los sistemas afectados o en los sitios de distribución de *malware*. Los artefactos también pueden consistir en los restos de un ataque de intrusos, como ejecutables, *scripts*, archivos, imágenes, archivos de configuración, herramientas, salidas de herramientas, registros, piezas de código activas o inactivas, etc.

El análisis se lleva a cabo con el fin de averiguar parte o la totalidad de la información que figura a continuación, aunque la lista no es exhaustiva:

- el contexto que requieren los artefactos para su funcionamiento y llevar a cabo las tareas previstas, ya sean maliciosas o no;
- cómo pueden haber sido utilizados los artefactos para el ataque: cargado, descargado, copiado, ejecutado o creado dentro de los entornos o componentes de una organización;
- qué sistemas han participado a nivel local y remoto para dar soporte a la distribución y las acciones;
- qué hizo el intruso una vez dentro del sistema, red, organización o infraestructura: desde la recopilación pasiva de datos, hasta la investigación activa y la transmisión de datos con fines de filtración, o la recopilación de nuevas solicitudes de acción, actualizándose o haciendo un movimiento lateral dentro de una red comprometida (local);
- qué hizo alguna vez un usuario, proceso de usuario o sistema de usuario para que la cuenta de usuario o el dispositivo de usuario quedara comprometido;
- qué comportamiento caracteriza a los artefactos o sistemas comprometidos, ya sea de manera autónoma, en conjunto con otros artefactos o componentes, conectados a una red local o a Internet, o en cualquier combinación;
- la forma en que los artefactos o sistemas comprometidos establecen la conectividad con el objetivo (por ejemplo, la trayectoria de la intrusión, el objetivo inicial o las técnicas de evasión de la detección);
- qué arquitectura de comunicación (punto a punto, instrucción y control, o ambas) se ha utilizado;
- cuáles fueron las acciones de los actores de la amenaza, cuál es su red y la huella de los sistemas;
- cómo evadieron los intrusos o los artefactos la detección (incluso durante largos periodos de tiempo que pueden incluir el reinicio o la reinicialización).

Esto puede lograrse mediante diversos tipos de actividades, en particular:

- análisis de medios o de superficie;
- ingeniería inversa;
- análisis dinámico o en tiempo de ejecución;
- análisis comparativo.

Cada actividad aporta información adicional sobre los artefactos. Los métodos de análisis incluyen, entre otros, la identificación del tipo y las características de los artefactos, la comparación con los artefactos conocidos, la observación de la ejecución de los artefactos en tiempo de ejecución o en tiempo real, y el desensamblado e interpretación de artefacto binario.

Al llevar a cabo un análisis de los artefactos, el analista trata de reconstruir y determinar qué es lo que hizo el intruso, a fin de detectar la vulnerabilidad explotada, evaluar los daños, preparar soluciones para mitigar los efectos de los artefactos y proporcionar información a los componentes y otros investigadores.

Resultado: Comprender la naturaleza de los artefactos digitales recuperados y las pruebas forenses analizadas, así como la relación con otros artefactos, objetos o componentes internos o externos, ataques a estructuras, herramientas y vulnerabilidades explotadas. Crear hipótesis o pruebas de lo que hizo el perpetrador de la amenaza y cómo se comportaron los artefactos. Este conocimiento es fundamental para evaluar las pérdidas, los daños, los impactos comerciales, etc. y para elaborar estrategias de contención y mitigación o recuperación. Se comprenden las tácticas, técnicas y procedimientos utilizados por los atacantes o intrusos para comprometer los sistemas, usuarios, redes, organizaciones y/o infraestructuras. Esto incluye las tácticas, técnicas y procedimientos utilizados para propagar, filtrar datos, actualizar, modificar o falsificar su comportamiento, datos, borrar automáticamente rastros de sus propias actividades o llevar a cabo otras actividades maliciosas.

Se considera que la siguiente lista de funciones forma parte de la implementación de este servicio:

- análisis de medios o superficies;
- ingeniería inversa;
- análisis dinámico y/o en tiempo de ejecución;
- análisis comparativo.

6.3.1 Función: Análisis de medios o de superficie

Finalidad: Comparar la información recabada a partir de los artefactos con otros públicos y privados y/o repositorios autorizados.

Descripción: Esta función implica identificar y caracterizar la información básica y los metadatos sobre los artefactos, incluidos, entre otras cosas, los tipos de ficheros, las cadenas de salida, los valores generadores criptográficos, los certificados, el tamaño de los archivos y los nombres de archivos y directorios. A medida que se reúna y se analice más a fondo toda la información

disponible, ésta podrá utilizarse para examinar cualquier repositorio de información de fuente pública/abierta o privada/cerrada para conocer mejor el artefacto o su comportamiento, por cuanto dicha información puede utilizarse para determinar los siguientes pasos.

Resultado: Se han identificado las características y/o la signatura del artefacto digital y toda la información ya conocida sobre el artefacto, incluidos el carácter malicioso, el impacto y la mitigación.

6.3.2 Función: Ingeniería inversa

Finalidad: Realizar un análisis estático minucioso del artefacto para determinar su completa funcionalidad, independientemente del entorno en el que se pueda ejecutar.

Descripción: Realizar un análisis más detallado de los artefactos de *malware* para incluir la identificación de acciones ocultas y el lanzamiento de instrucciones. La ingeniería inversa permite al analista descubrir cualquier ofuscación y compilación (para binarios) e identificar el programa, guion o código que integra el *malware*, ya sea desvelando el código fuente o mediante el desensamblado del código binario en lenguaje ensamblador e interpretándolo. El analista descubre todas las funciones y acciones incluidas en el lenguaje máquina que el *malware* puede realizar. La ingeniería inversa es un análisis más detallado que se lleva a cabo cuando los análisis de superficie y en tiempo de ejecución no proporcionan toda la información necesaria.

Resultado: Se desvela la funcionalidad íntegra del artefacto digital para comprender cómo funciona, cómo se activa, las debilidades del sistema que se pueden explotar, su impacto total y los daños potenciales, con el fin de desarrollar soluciones que permitan mitigar los efectos del artefacto y, si procede, crear una nueva signatura para compararla con otras muestras.

Se considera que las siguientes subfunciones forman parte de la implementación de esta función:

- análisis estático;
- ingeniería inversa del código;
- análisis y descripción del comportamiento potencial;
- posible diseño de la signatura.

6.3.3 Función: Análisis dinámico o en tiempo de ejecución

Finalidad: Descubrir cómo funciona el artefacto.

Descripción: Esta función consiste en comprender las capacidades de un artefacto observando su funcionamiento mientras se ejecuta la muestra en un entorno real o emulado (por ejemplo, en un espacio acotado (sandbox), en un entorno virtual y en emuladores de *hardware* o *software*).

Al utilizar un entorno simulado se detectan los cambios en el anfitrión, el tráfico de red y el resultado de la ejecución. La premisa básica es intentar ver el artefacto en funcionamiento en un entorno lo más real posible.

Resultado: Se obtiene una visión adicional del funcionamiento del artefacto digital observando su comportamiento durante su ejecución para determinar los cambios en el sistema anfitrión afectado, otras interacciones de sistema y el tráfico de red resultante, a fin de comprender mejor los daños y los efectos para el sistema, crear nuevas signaturas de artefactos y determinar las medidas de mitigación.

Nota: No puede observarse toda la funcionalidad mediante el análisis en tiempo de ejecución ya que no es posible activar todas las secciones de código de artefacto. El análisis en tiempo de ejecución sólo permite al analista ver lo que el *malware* hace en la situación de prueba, no todo lo que es capaz de hacer.

Las siguientes subfunciones se consideran parte de la implementación de esta función:

- preparación del entorno de análisis (en tiempo real/restringido/cerrado, emulado/simulado);
- preparando colectores, sensores y/o sondas;
- recoger los datos y metadatos iniciales de comportamiento;
- sondear el artefacto en múltiples ocasiones en varios contextos;
- llevar a cabo un análisis del comportamiento de los sistemas y/o redes, tanto a corto como a largo plazo;
- sacar conclusiones evaluando todos los resultados y datos recabados, comparando los diversos resultados e investigando las bases de conocimientos disponibles para los resultados técnicos existentes que coincidan con los hallazgos.

6.3.4 Función: Análisis comparativo

Finalidad: Realizar un análisis centrado en la identificación de la funcionalidad o intención común, en particular el análisis de la semejanza con los artefactos catalogados.

Descripción: Esta función implica investigar la relación del artefacto con otros artefactos. Las similitudes pueden estar en el código o el *modus operandi*, los objetivos, la finalidad y los autores. Tales similitudes pueden utilizarse para deducir el alcance de un ataque (por ejemplo, si hay un objetivo más grande, si se ha utilizado antes un código similar).

Entre las técnicas de análisis comparativo figura la comparación de coincidencias exactas o de similitudes en el código. El análisis comparativo ofrece una visión más amplia del modo en que se utilizó y modificó con el tiempo el artefacto, o versiones similares del mismo, y ayuda a comprender la evaluación del *malware* o de otros tipos de artefactos maliciosos.

Resultado: Se derivan los puntos comunes o las relaciones con otros artefactos a fin de identificar las tendencias o similitudes que pueden proporcionar una visión o comprensión adicional de la funcionalidad, el impacto y la mitigación de un artefacto digital.

Se considera que las siguientes subfunciones forman parte de la implementación de esta función:

- definir una referencia para las características y comportamientos observados;

- buscar características idénticas o similares en los repositorios/bases de conocimientos disponibles;
- actualizando los repositorios/bases de conocimiento disponibles con respecto a indicios, comportamientos y/o signaturas recién observados o previamente desconocidos que pueden emplearse para clasificar más detalladamente el artefacto investigado.

6.4 Servicio: Mitigación y recuperación

Finalidad: Contener el incidente de seguridad de la información en la medida de lo posible para limitar el número de víctimas, reducir las pérdidas y recuperarse de los daños, evitar nuevos ataques y nuevas pérdidas mediante la eliminación de las vulnerabilidades o puntos débiles explotados y mejorar la seguridad cibernética en general.

Descripción: Una vez que se ha confirmado mediante análisis un posible incidente de seguridad de la información y se ha preparado una estrategia de respuesta, ésta debe convertirse en el plan de respuesta. Antes incluso de ultimar el plan de respuesta, se pueden tomar medidas *ad hoc*. Este servicio incluye también el inicio y rastreo de todas las actividades que se realicen hasta que el incidente de seguridad de la información pueda considerarse cerrado o se disponga de nueva información que requiera un análisis más profundo y que, en adelante, pueda también modificar la estrategia y el plan de respuesta.

Resultado: Se mitiga el incidente de seguridad de la información y se mejora la situación de ciberseguridad. Se restablece la integridad de los sistemas afectados por el ataque o las actividades subyacentes del atacante, así como la capacidad de servicio de la red y los sistemas comprometidos. De ser posible, se restauran los datos que se hubiesen perdido.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- establecimiento de un plan de respuesta;
- medidas *ad hoc* y contención;
- restauración de sistemas;
- ayuda a otras entidades de seguridad de la información.

En el caso del EIISI coordinador, no se facilitarán todas las funciones. Si bien el "apoyar a otras entidades de seguridad de la información" es una actividad que realizan esos equipos, a veces también ayudan a "establecer un plan de respuesta".

6.4.1 Función: Establecer un plan de respuesta

Finalidad: Definir y ejecutar un plan para restaurar la integridad de los sistemas afectados y restituir los datos, sistemas y redes afectados al estado operativo no degradado, restableciendo plenamente los servicios afectados sin recrear el contexto en el que se originó el problema de seguridad para que no pueda suceder de nuevo.

Descripción: Si no se comprenden plenamente las repercusiones para la empresa y los requisitos para la mitigación y recuperación, no podrá darse una respuesta significativa. Dado que existe un conflicto de intereses –rastrear el ataque para obtener más inteligencia o bien contener el

ataque para evitar más pérdidas– es necesario tener cabalmente en cuenta los intereses y elaborar un plan de respuesta que resulte plausible para resolver los hechos conocidos y obtener el resultado deseado en el plazo requerido.

Como sucede con todos los planes, al disponer de nuevos resultados de análisis, es necesario revisar los nuevos hallazgos. De hecho, el plan de respuesta normalmente tendrá que modificarse para dar orientaciones y asesoramiento continuos. Pero sin un plan de este tipo -–a menos que la respuesta esté a cargo de un pequeño grupo de la organización con pocos requisitos de interfaces externas u otras entidades– será imposible llevar a cabo las actividades de manera eficiente y con eficacia debido a la falta de coordinación.

Resultado: Definir el plan de respuesta convenido que satisfaga las necesidades de la empresa, con la ayuda de los recursos y el apoyo disponibles, y su ulterior ejecución. El servicio de "coordinación" se encargará del rastreo y la coordinación por el EIISI.

Se considera que las siguientes subfunciones forman parte de la implementación de esta función:

- determinar las repercusiones para la empresa del incidente de seguridad de la información;
- determinar los requisitos de la empresa y el plazo para una recuperación exitosa;
- definir los procesos y criterios de decisión (si no están ya definidos por las políticas);
- identificar los objetos a recuperar: entornos, sistemas, aplicaciones, funciones transversales, etc.;
- identificar el apoyo y las acciones necesarias por las entidades internas y externas;
- determinar el plan de respuesta que permita dar una respuesta significativa dentro de los requisitos de la empresa y el marco temporal deseados, sobre la base de los recursos disponibles y el alcance técnico de las medidas requeridas.

6.4.2 Función: Medidas *ad hoc* y contención

Finalidad: Aplicar medidas que garanticen que los incidentes de seguridad de la información no se propaguen más, es decir, que permanezca confinado en el sistema, los usuarios y/o los dominios actualmente afectados para garantizar que no se produzcan más pérdidas (como la filtración de documentos, cambios en las bases de datos o los datos, etc.).

Descripción: El reto inmediato en caso de un incidente de seguridad de la información es impedir que se propague. Mientras los sistemas están comprometidos o el *malware* permanezca activo en los sistemas de los usuarios finales, se producirán más pérdidas de datos y quedarán más comprometidos. El objetivo principal de los ataques suele ser acceder a datos y sistemas específicos, incluidos los ataques (que incluyen, entre otros, los movimientos laterales) a otras organizaciones tanto internas como externas a la organización víctima del incidente de seguridad de la información. Para poder detener o al menos limitar el alcance de cualquier actividad maliciosa o de nuevas pérdidas es preciso tomar acciones a corto plazo, como bloquear o filtrar el tráfico y eliminar el acceso a servicios o sistemas específicos, llegando incluso a desconectar los sistemas esenciales.

Denegar un mayor acceso a datos que potencialmente contienen pruebas esenciales permitirá realizar un análisis completo de esas pruebas. Impedir el mayor acceso a otros sistemas y redes también limitará la responsabilidad que conlleva los daños causados a otras organizaciones.

Detener los daños inmediatos y limitar el alcance de las actividades maliciosas mediante acciones tácticas a corto plazo (por ejemplo, el bloqueo o el filtrado del tráfico) implica también recuperar el control de los sistemas. Mientras los agresores o el *malware* activo tengan fácil acceso a otros sistemas o redes, no será posible volver al funcionamiento normal.

Resultado: Se recupera el control de los sistemas y redes implicados. Se impide el acceso de los atacantes y el *malware* a los datos, sistemas y redes para evitar otros ataques y/o que queden comprometidos otros sistemas y datos.

Las siguientes subfunciones podrían formar parte de la implementación de esta función:

- eliminar temporalmente el acceso de los usuarios/sistemas/servicios/redes;
- desconectar temporalmente los sistemas o redes de las redes o troncales;
- desactivar temporalmente los servicios;
- exigir a los usuarios que cambien sus contraseñas o credenciales de cifrado;
- vigilar los signos de intrusión e indicadores de compromiso;
- verificar que todos los usuarios/sistemas/servicios/redes no estén afectados.

6.4.3 Función: Restauración del sistema

Finalidad: Aplicar cambios en el dominio, la infraestructura o la red afectados que sean necesarios para solucionar y evitar que este tipo de actividad vuelva a producirse.

Descripción: Restaurar la integridad de los sistemas afectados y restituir los datos, sistemas y redes afectados a un estado operativo no degradado, restaurando los servicios afectados a su plena funcionalidad. Dado que la realidad empresarial suele exigir que los sistemas vuelvan a funcionar normalmente lo antes posible, existe el riesgo de que no se hayan eliminado totalmente los medios de acceso no autorizado. Por consiguiente, a menos que se disponga de resultados del análisis, incluso los sistemas restituidos se deben supervisar y gestionar meticulosamente. Especialmente si (aún) no pueden eliminarse las vulnerabilidades y puntos débiles identificados, es necesario aplicar mecanismos de protección y detección mejorados para evitar incidentes de seguridad de la información de este u otros tipos.

Resultado: Se aplican medidas para restablecer la plena funcionalidad y capacidad de los sistemas y servicios. Se aplican medidas para cerrar cualquier vulnerabilidad o punto débil detectado que haya sido el origen o contribuido al incidente de seguridad de la información. Se mejoran las medidas de detección y reacción conforme a lo recomendado por el plan de análisis y respuesta.

Se considera que las siguientes subfunciones forman parte de la implementación de esta función:

- restaurar los datos del usuario/sistema a partir de copias de seguridad fiables;
- restaurar configuraciones de copias de seguridad fiables o contenido recreado;
- propiciar servicios para discapacitados y restablecer el acceso para usuarios/sistemas/redes;
- realizar pruebas funcionales para validar la capacidad y la idoneidad de los sistemas/servicios/redes tanto a nivel de infraestructura como de aplicación.

6.4.4 Función: Ayuda a otras entidades de seguridad de la información

Finalidad: Permitir que los mandantes realicen las actividades de gestión y técnicas necesarias para mitigar satisfactoriamente un incidente de seguridad de la información y recuperarse de dicho incidente.

Descripción: El EIISI puede proporcionar asistencia directa (*in situ*) para ayudar a los mandantes a recuperarse de las pérdidas y eliminar las vulnerabilidades. Podría ser una extensión directa de la oferta de servicios de análisis *in situ* (véase más arriba). Por otra parte, el EIISI podría optar por prestar ayuda al personal de los mandantes que respondan al incidente de seguridad de la información con explicaciones más detalladas, recomendaciones, etc.

Resultado: Se mejora la respuesta de los mandantes y la recuperación es más rápida. Incrementando el conjunto de conocimientos disponibles se puede reforzar la eficacia y la eficiencia futuras de las actividades conexas. Además, se contribuye a ayudar a las entidades dentro de la organización que carecen de conocimientos técnicos detallados para tomar las medidas de respuesta necesarias.

6.5 Servicio: Coordinación de incidentes de seguridad de la información

Finalidad: Garantizar notificación oportuna y la distribución de información exacta; mantener el flujo de información y rastrear la situación de las actividades de las entidades encargadas o a las que se les encomiende participar en la respuesta al incidente de seguridad de la información; y asegurarse de que el plan de respuesta se ejecuta y que las divergencias causadas tanto por las demoras como por la nueva información se gestionan en consecuencia.

Descripción: Es fundamental para todos los interesados y las organizaciones afectadas que se les notifique y mantenga informados sobre los pormenores y las actividades en curso en relación con un incidente de seguridad de la información. Dado que algunas actividades imprescindibles para la mitigación y recuperación satisfactorias pueden requerir la aprobación de la administración, es indispensable establecer funciones adecuadas de tramitación y notificación antes de poder gestionar eficaz y eficientemente cualquier incidente de seguridad de la información. A medida que el EIISI analiza toda la información que vaya surgiendo, es necesaria la coordinación para garantizar que las notificaciones y la información llegan a los puntos de contacto correctos, se rastrean sus respuestas y se vela por que todas las partes implicadas informen de sus actividades para conocer con exactitud la situación hasta que el incidente de seguridad de la información se considere cerrado y no requiera más coordinación.

Los interesados deben disponer de canales para formular preguntas, verificar el estado de los incidentes de seguridad de la información e informar de los problemas al EIISI. Para hacer participar a los interesados internos, el EIISI debe proporcionar canales de comunicación para anunciar el estado de la reparación de los incidentes de seguridad de la información. Para permitir la participación de interesados externos, el EIISI debe mantener canales de comunicación con otros EIISI y comunidades de EIISI que pudieran proporcionar recomendaciones o apoyo técnico.

Resultado: Se coordina satisfactoriamente la respuesta de todas las entidades bien informadas que contribuyen a reaccionar ante un incidente de seguridad de la información.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- comunicación;
- distribución de notificaciones;
- distribución de información pertinente;
- coordinación de actividades;
- notificación;
- comunicación a los medios.

6.5.1 Función: Comunicación

Finalidad: Colaborar eficazmente con los interesados y establecer múltiples canales de comunicación adecuados con la confidencialidad necesaria.

Descripción: El EIISI debe elaborar y publicar sus comunicaciones con exactitud para su audiencia. A cambio, el EIISI también debe estar dotado para recibir opiniones, informes, comentarios y preguntas de muy diversas fuentes basadas en su propia comunicación.

La política de seguridad y la política de intercambio de información pueden exigir que la información se gestione escrupulosamente. El EIISI debe poder compartir información con los interesados de manera fiable, segura y privada, tanto externos como internos.

Deben establecerse cuanto antes acuerdos de confidencialidad y los recursos de comunicación deben configurarse en consecuencia. Como complemento, también se puede recurrir al concepto de "información sujeta a embargo". Asimismo, también debe establecerse una política de retención para garantizar que tanto los datos utilizados para elaborar la información como la información propiamente dicha se gestionen, compartan y conserven adecuadamente en función de las limitaciones, como la duración, hasta que se anulen esas limitaciones o la información se divulgue públicamente.

Los canales de comunicación pueden adoptar múltiples formas en función de las necesidades de los interesados y los mandantes. Toda la información comunicada debe ser etiquetada de acuerdo con la política de intercambio de información. Se puede utilizar el protocolo semáforo.

Resultado: Todos los canales de comunicación están disponibles con arreglo a los requisitos de seguridad de todas las partes receptoras y emisoras.

Se considera que las siguientes subfunciones forman parte de la aplicación de esta función:

- proporcionar canales de comunicación internos;
- proporcionar canales de comunicación externos.

6.5.2 Función: Distribución de notificaciones

Finalidad: Alertar a las entidades afectadas por el incidente de seguridad de la información o a las que puedan contribuir a la respuesta al mismo y proporcionarles la información necesaria para que comprendan su función y las posibles expectativas de su cooperación y apoyo.

Descripción: Los incidentes de seguridad afectan a muchas entidades internas y potencialmente externas, así como a sistemas y redes. Dado que los EIISI son el centro neurálgico en el que se reciben informes de posibles incidentes de seguridad de la información, también sirven como centro para notificar a los puntos de contacto autorizados. En la notificación se suelen facilitar no sólo los detalles técnicos adecuados, sino también información sobre la respuesta prevista y el punto de contacto para darle seguimiento.

Resultado: Se pone a la disposición de las entidades que deben participar en la respuesta, o ser informadas de ello, la información sobre el incidente de seguridad de la información.

6.5.3 Función: Distribución de información pertinente

Finalidad: Mantener la comunicación con las entidades identificadas y proporcionar un adecuado flujo de la información disponible a fin de que esas entidades puedan beneficiarse de los conocimientos disponibles y de las lecciones extraídas, aplicar respuestas mejoradas o adoptar nuevas medidas *ad hoc*.

Descripción: A medida que avanza la respuesta a un incidente de seguridad de la información, se dispone de más resultados de análisis e informes de otros posibles expertos en seguridad, EIISI o víctimas.

Puede ser útil transmitir parte de la información y las lecciones extraídas al ámbito de servicio de transferencia de conocimientos (de existir) para mejorar la formación y la documentación técnica, así como para ayudar a crear una conciencia adecuada, especialmente si se identifican nuevas tendencias de ataques o incidentes.

Resultado: Se distribuye la información disponible a las personas responsables de participar en la respuesta o a las que se les ha de mantener informadas sobre los progresos y la situación actual.

6.5.4 Función: Coordinación de actividades

Finalidad: Hacer un seguimiento de la situación de todas las comunicaciones y actividades.

Descripción: Dado que son muchas las entidades que pueden participar en la respuesta a un incidente de seguridad de la información, es necesario hacer un seguimiento de la situación de todas las comunicaciones y actividades. Esto implicar las medidas solicitadas por el EIISI o las solicitudes de compartición de información adicional, además de las solicitudes de análisis técnico de los artefactos o el intercambio de indicadores de compromiso, información sobre otras víctimas, etc. Esto se produce principalmente cuando el EIISI depende de información y recursos ajenos a su control directo para tomar las acciones necesarias en la mitigación de un incidente. Pero también ocurre dentro de organizaciones más grandes para las que el EIISI interno coordina las actividades de mitigación y recuperación.

Al ofrecer coordinación bilateral o multilateral, el EIISI participa en el intercambio de información para habilitar aquellos recursos con los que actuar o para ayudar a otros a detectar, proteger o resolver las actividades en curso de los atacantes y ayudar a cerrar el incidente de seguridad de la información.

Resultado: Se genera consciencia coyuntural del estado de todas las actividades y de las entidades que participan en la respuesta.

6.5.5 Función: Notificación

Finalidad: Garantizar que todas las entidades implicadas en la empresa dispongan de información sobre el estado de las actividades en curso, de modo que al decidir sobre la forma de proceder conozcan lo mejor posible la situación.

Descripción: Proporcionar información concisa y objetiva sobre el estado actual de las actividades solicitadas o realizadas en respuesta a un incidente de seguridad de la información. En lugar de esperar a que se extraiga dicha información mediante una acción coordinada en curso, como se requiere para cualquier respuesta satisfactoria, disponer de informes oportunos es fundamental para lograr una coordinación eficaz.

Resultado: Se informe a los interesados internos del alcance de las actividades en curso, las acciones ya realizadas y las pendientes. También se comunica la incidencia estimada de las demoras, las recomendaciones y las medidas solicitadas, lo que permite comprender la repercusión general para la estrategia de respuesta seleccionada y el plan desarrollado.

6.5.6 Función: Comunicación con los medios

Finalidad: Colaborar con los medios de comunicación (públicos) para poder proporcionar información empírica precisa y fácil de entender sobre los eventos en curso, a fin de evitar la propagación de rumores e información engañosa.

Descripción: La comunicación con los medios de comunicación no es posible en muchos casos. Si bien los EIISI suelen tratar de evitar ese contacto, es importante tener en cuenta que los medios de comunicación pueden ayudar a mitigar determinados tipos de ataques continuos y a gran escala que causan incidentes de seguridad de la información. Para ello es necesario explicar qué es lo que está causando los incidentes de seguridad de la información y explicar la incidencia en los usuarios y/o las organizaciones. En algunos casos, el EIISI puede optar por proporcionar esta información de una manera adecuada para su divulgación al público, pero para ello se requiere

conocimientos específicos dentro del EIISI que no siempre tienen. En cualquier caso, si el EIISI se comunica con los medios de comunicación, debe simplificar en la medida de lo posible las cuestiones técnicas y eliminar además toda la información confidencial.

Resultado: Se elabora información empírica que ofrece un resumen claro del incidente de seguridad de la información en curso, comprendidas las medidas que deben adoptar las posibles víctimas o se describe la estrategia de respuesta elegida para recuperarse del incidente de seguridad de la información.

6.6 Servicio: Ayuda en la gestión de la crisis

Finalidad: Proporcionar conocimientos y contactos a otros expertos en seguridad, EIISI y comunidades de EIISI para ayudar a mitigar la crisis.

Descripción: Si bien los incidentes de seguridad de la información de hoy en día raramente constituyen una crisis organizacional o nacional, en realidad tienen el potencial para ello. Pero la respuesta a una crisis suele asociarse a una emergencia que amenaza el bienestar de las personas y de la sociedad en general, o al menos la existencia de una organización. Conforme a lo dispuesto en la gestión de crisis, un alto cargo asumirá la responsabilidad de una crisis, alterando así la jerarquía habitual durante la emergencia.

Dado que los sistemas y redes pueden contribuir a las emergencias o deben estar disponibles para responder a una situación de crisis, el EIISI será por lo general un recurso fundamental para la gestión de esas situaciones y aportará su valiosa experiencia, pero también se ha de contar con los servicios y redes de puntos de contacto establecidos.

Resultado: El equipo de gestión de crisis utiliza los recursos del EIISI para resolver los problemas de ciberseguridad de la crisis actual. Asimismo, se recurre a los recursos de comunicación del EIISI para solicitar a los mandantes y a las partes externas medidas de apoyo o ayuda específicas. También puede utilizarse para comunicarse de manera fiable con los mandantes, utilizando los medios de comunicación establecidos y redes fiables.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- distribución de información a los mandantes;
- informe sobre el estado de la seguridad de la información;
- comunicación de decisiones estratégicas.

6.6.1 Función: Distribución de información a los mandantes

Finalidad: Proporcionar recursos de comunicación para ayudar a responder a la crisis.

Descripción: A medida que avanza la respuesta a la crisis, se debe distribuir y divulgar información. Como el EIISI ha establecido tales recursos para sus propios fines, el equipo que gestiona la crisis puede considerar adecuado o necesario utilizar dichos recursos.

Resultado: Se distribuye la información disponible a los mandantes, gracias a las relaciones de confianza establecidas que ayudan a tranquilizar a los destinatarios acerca de la exactitud de la información divulgada.

6.6.2 Función: Notificación del estado de seguridad de la información

Finalidad: Garantizar que el equipo de gestión de crisis tenga una visión general de los actuales incidentes de seguridad de la información y de las vulnerabilidades conocidas para tenerlos presentes en sus prioridades y estrategias generales.

Descripción: La función consiste en proporcionar información concisa y objetiva sobre la situación actual de la ciberseguridad cibernética para el grupo de mandantes. Dado que puede aprovecharse una crisis para iniciar otros ataques o éstos pueden formar parte de otras actividades que culminan en esta crisis, es muy importante que el equipo de gestión de crisis conozca cabalmente la situación.

El EIISI puede proporcionar conocimientos de la situación para sus servicios y sus mandantes, ya sea previa solicitud o en el marco de las políticas vigentes en caso de crisis. En cualquier caso, como la gestión de crisis sólo puede tener éxito si se establece un adecuado flujo de información, por cuanto depende de la coordinación de los recursos para abordar los aspectos más graves de la crisis, la información se debe proporcionar de manera oportuna y con exactitud.

Habida cuenta de que para gestionar los incidentes de seguridad de la información en curso se necesitarán recursos, es preciso decidir si se interrumpe la respuesta mientras dure el incidente (y asignar los recursos ahora disponibles a otras esferas) o proseguir. Cuanto mejor se conozca la situación, más razonables serán las decisiones que se tomen.

Resultado: Se informa al equipo de gestión de crisis del alcance de las actividades en curso, de las medidas ya completadas y de las pendientes. También se le comunicarán las posibles repercusiones de las demoras, las recomendaciones y las medidas solicitadas, lo que permitirá comprender la incidencia general de la estrategia seleccionada para abordar la crisis actual.

6.6.3 Función: Comunicación de decisiones estratégicas

Finalidad: Informar oportunamente a otras entidades sobre el impacto causado por la crisis en los incidentes de seguridad de la información actualmente abiertos.

Descripción: Informar a otras entidades de manera oportuna sobre el impacto causado por la crisis en los incidentes de seguridad de la información actualmente abiertos ayuda a comprender claramente el apoyo que también puede proporcionar el EIISI durante la crisis, y garantiza que las entidades entienden lo que cabe esperar. También garantiza que otras partes dejen de prestar apoyo o de interactuar con el EIISI, ya que podrían creer que la crisis está tomando el relevo.

Dado que el equipo de gestión de crisis puede decidir aplazar la respuesta a un incidente real de seguridad de la información debido a una crisis, esas decisiones deben comunicarse a todas las

entidades participantes. De esta manera se evitan malentendidos y otros problemas que también pueden dar lugar a una pérdida de confianza en el EIISI y/o la organización anfitriona.

Resultado: Se distribuye la información sobre el impacto de la crisis en la operación del EIISI a los mandantes y otras entidades que participan en la respuesta a los incidentes abiertos de seguridad de la información. Se describen claramente las expectativas del EIISI respecto de esas entidades y se garantiza la comunicación clara de las necesidades de información del EIISI.

7 Ámbito de servicio: Gestión de vulnerabilidades

El ámbito de servicios de gestión de vulnerabilidades comprende servicios relacionados con el descubrimiento, el análisis y el tratamiento de vulnerabilidades de seguridad nuevas o notificadas en los sistemas de información. El ámbito de servicios de gestión de vulnerabilidades también incluye servicios relacionados con la detección de vulnerabilidades conocidas y la respuesta a las mismas a fin de evitar que sean explotadas. Por consiguiente, este ámbito de servicios abarca los servicios relacionados con las vulnerabilidades nuevas y conocidas.

Si bien se utiliza a veces el término "gestión de vulnerabilidades" para referirse al proceso de evitar simplemente que se exploten las vulnerabilidades conocidas (por ejemplo, "explorar y parchear"), en el presente marco de servicios del EIISI, esas actividades se consideran funciones y subfunciones del servicio denominado respuesta a vulnerabilidades, que es sólo un posible servicio que podría prestar el EIISI. Para muchos EIISI, esas funciones de respuesta a vulnerabilidades son responsabilidad de otras funciones que exploran y solucionan vulnerabilidades de seguridad.

Se considera que los siguientes servicios se ofrecen en este ámbito de servicios:

- descubrimiento/investigación de vulnerabilidades;
- admisión de informes de vulnerabilidades;
- análisis de vulnerabilidades;
- coordinación de vulnerabilidades;
- divulgación de vulnerabilidades;
- respuesta a vulnerabilidades.

Son pocos los EIISI que proporcionan todos estos servicios, dado que sólo ofrecen aquellos comprendidos en su ámbito de responsabilidad. Por ejemplo, el EIISI puede limitar sus servicios a conocer nuevas vulnerabilidades a partir de fuentes públicas (descubrimiento/investigación de vulnerabilidades) o de terceros (admisión de informes de vulnerabilidades) y luego emitir un aviso de seguridad a sus mandantes (divulgación de vulnerabilidades) cuando sea necesario, sin participar necesariamente en ninguna actividad de coordinación con los proveedores de productos o los que elaboren una solución (coordinación de vulnerabilidades), o implicarse en el despliegue directo de una solución (respuesta a vulnerabilidades).

7.1 Servicio: Descubrimiento/investigación de vulnerabilidades

Finalidad: Encontrar, conocer o buscar nuevas vulnerabilidades (previamente desconocidas); las vulnerabilidades pueden ser descubiertas por los miembros del ámbito de servicios de gestión de vulnerabilidades o a través de otras actividades relacionadas del EIISI

Descripción: El descubrimiento de una nueva vulnerabilidad es el primer paso necesario para iniciar el ciclo de vida de la gestión general de vulnerabilidades. Este servicio incluye aquellas funciones y actividades que el EIISI puede realizar activamente a través de su propia investigación u otros servicios para descubrir una nueva vulnerabilidad. Las funciones y actividades relacionadas con la recepción pasiva de información sobre nuevas vulnerabilidades por otra persona se describen más adelante en el servicio de admisión de informes sobre vulnerabilidades. En ocasiones, el EIISI puede descubrir una nueva vulnerabilidad mientras realiza otras actividades, como por ejemplo al analizar o investigar un informe de incidentes. Otra forma de conocer la nueva vulnerabilidad es a través de la lectura de fuentes públicas (por ejemplo, sitios web, listas de correo[6]), otras fuentes externas (por ejemplo, servicios de primera calidad, suscripciones), o buscando activamente las vulnerabilidades a través de una investigación deliberada (por ejemplo, a través de pruebas aleatorias o ingeniería inversa). Esos descubrimientos se deben documentar e incorporar a los procesos de gestión de vulnerabilidades de la organización, con independencia de la forma en que el EIISI haya descubierto o reparado en la vulnerabilidad.

Resultado: Se aumenta el descubrimiento de posibles vulnerabilidades que no se comunicaron directamente al EIISI.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- descubrimiento de vulnerabilidades en respuesta a incidentes;
- descubrimiento de vulnerabilidades a partir de fuentes públicas;
- investigación de vulnerabilidades.

Estas funciones pueden consistir en servicios (o funciones) realizadas por otros (por ejemplo, investigadores, proveedores, EIISP, o especialistas de terceros) en lugar del EIISI.

7.1.1 Función: Descubrimiento de vulnerabilidades en respuesta a incidentes

Finalidad: Identificar vulnerabilidades que se explotaron en el contexto de un incidente de seguridad.

Descripción: En el curso del análisis de un incidente de seguridad, es posible que se descubra información acerca de una vulnerabilidad que fue explotada por el atacante. El incidente puede

[6] La nueva información sobre vulnerabilidades recibida por correo electrónico puede considerarse como una actividad del servicio de Descubrimiento de Vulnerabilidades, de la función de descubrimiento de vulnerabilidades a partir de fuentes públicas, del servicio de admisión de informes sobre vulnerabilidades o de la función de recepción de informes sobre vulnerabilidades, dependiendo de los procesos internos del EIISI o de la amplitud con que se haya distribuido la información sobre vulnerabilidades.

haberse producido gracias a la explotación de una vulnerabilidad conocida que no ha sido corregida o acotada previamente; o de una nueva vulnerabilidad (incipiente).

Parte de esta información sobre la vulnerabilidad podría recibirse como resultado de uno de los servicios del ámbito de servicios de gestión de incidentes de seguridad de la información si la vulnerabilidad se explotó en un incidente. La información puede entonces transmitirse a la función de clasificación de vulnerabilidades o al servicio de análisis de vulnerabilidades, según proceda.

Resultado: La información sobre la vulnerabilidad que se sospecha ha sido explotada en un incidente de seguridad se transmite al ámbito de servicios de gestión de vulnerabilidades.

7.1.2 Función: Descubrimiento de vulnerabilidades a partir de fuentes públicas

Finalidad: Conocer nuevas vulnerabilidades leyendo fuentes públicas u otras fuentes de terceros.

Descripción: El EIISI puede enterarse inicialmente de una nueva vulnerabilidad a partir de diversas fuentes públicas que anuncian dicha información. Estas fuentes pueden ser anuncios de proveedores, sitios web de seguridad, listas de correo, bases de datos sobre vulnerabilidades, conferencias de seguridad, medios sociales, etc. También puede enterarse de nuevas vulnerabilidades a través de otras fuentes de terceros que quizá no estén completamente abiertas al público, por ejemplo, a través de suscripciones de pago o servicios exclusivos en los que la información se comparte sólo con un grupo limitado. Se puede asignar personal para desempeñar esta función y reunir información con el fin de organizarla para su ulterior examen y compartición. También es posible recibir información similar sobre vulnerabilidades de los servicios del ámbito de servicios de consciencia coyuntural.

Resultado: Se identifican nuevas vulnerabilidades detectadas por fuentes externas públicas o de otro tipo.

7.1.3 Función: Investigación de vulnerabilidades

Finalidad: Descubrir o investigar nuevas vulnerabilidades mediante la investigación o realización de actividades destinadas a tal efecto.

Descripción: Esta función incluye el descubrimiento de nuevas vulnerabilidades como resultado de actividades específicas del EIISI, como al probar sistemas o *software* mediante pruebas "aleatorias" (*fuzzy*) o mediante la ingeniería inversa del *malware*.

Esta función también puede obtener información de los servicios del ámbito de servicios de gestión de incidentes de seguridad de la información o del ámbito de servicio de consciencia coyuntural que iniciaría esta función para buscar presuntas vulnerabilidades.

El descubrimiento de una nueva vulnerabilidad mediante esta función de investigación de vulnerabilidades puede convertirse en un parámetro de entrada para el servicio de respuesta a incidentes o la función de detección de vulnerabilidades (ver las subfunciones de exploración de vulnerabilidades y prueba de penetración de vulnerabilidades).

Resultado: Se identifican nuevas vulnerabilidades mediante la investigación.

7.2 Servicio: Admisión de informes sobre vulnerabilidades

Finalidad: Recibir y tramitar información sobre vulnerabilidades notificada por los mandantes o terceros.

Descripción: Una de las principales fuentes de información sobre vulnerabilidades son los informes o preguntas formuladas por los mandantes del EIISI o por terceros. El EIISI debe prever que las vulnerabilidades se puedan recibir de diversas fuentes y proporcionar mecanismos, procesos y orientaciones para informar sobre vulnerabilidades. Las infraestructuras de notificación pueden ser el correo electrónico o un formulario de notificación de vulnerabilidad por la web. No todas las vulnerabilidades se comunican directamente al EIISI por sus mandantes o por terceros a través de los canales establecidos. Las guías deben incluir directrices para la presentación de informes, información de contacto y cualquier política de divulgación.

Para que los mandantes puedan informar sobre las vulnerabilidades de manera más eficaz, el EIISI debe proporcionar uno o varios mecanismos, así como orientaciones o instrucciones sobre qué y cómo informar acerca de las vulnerabilidades de manera segura. Los mecanismos de presentación de informes pueden ser el correo electrónico, sitios web, formularios o portales dedicados a la notificación sobre vulnerabilidades u otros métodos adecuados para que los informes puedan presentarse de manera segura. La guía sobre cómo presentar informes, si no se incluye en el propio formulario de notificación sobre vulnerabilidades, debe figurar en documentación separada o en una página web, donde figure la información específica que conviene incluir en el informe.

Resultado: El informe sobre la vulnerabilidad se recibe en un formato profesional y coherente, así como su validación y clasificación iniciales.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- recepción de informes de vulnerabilidades;
- clasificación y tramitación de informes sobre vulnerabilidades.

7.2.1 Función: Recepción de informe sobre vulnerabilidades

Finalidad: Aceptar o recibir información sobre vulnerabilidades, notificada por los mandantes o por terceros.

Descripción: Para que la recepción de los informes sobre vulnerabilidades sea eficaz se requieren mecanismos y procesos para recibir informes remitidos por los mandantes, los interesados y por terceros (inspectores, investigadores, proveedores, EIISP, otros EIISI o coordinadores de vulnerabilidades, etc.). La información sobre vulnerabilidades puede incluir los dispositivos afectados, las condiciones necesarias para explotar la vulnerabilidad, el impacto (por ejemplo, aumento de privilegios, acceso a los datos, etc.), así como las medidas adoptadas para resolver la vulnerabilidad, las medidas de reparación y/o mitigación, y la resolución. En ocasiones, la información sobre vulnerabilidades se recibe junto con información para otros servicios, en particular la admisión de informes sobre incidentes de seguridad de la información

(por ejemplo, si se informa que se ha explotado una vulnerabilidad en un informe sobre un incidentes).

Resultado: Se gestionan adecuadamente los informes sobre vulnerabilidades presentados por mandantes o por terceros, en particular el inicio de la documentación o rastreo de informes.

Se considera que las siguientes subfunciones forman parte de esta función:

- supervisar regularmente los canales de comunicación y comprobar si los canales anunciados para ponerse en contacto con el EIISI están operativos y se pueden presentar informes;
- realizar un acuse de recibo preliminar al remitente del informe sobre vulnerabilidades, solicitar información adicional si es necesario y establecer expectativas con el informante.

7.2.2 Función: Clasificación y tramitación de informes de vulnerabilidades

Finalidad: Examinar, categorizar, priorizar y tramitar inicialmente informes sobre vulnerabilidades.

Descripción: Los informes sobre la vulnerabilidad se examinan y se clasifican para obtener una comprensión inicial de la vulnerabilidad en cuestión y determinar cómo proceder (por ejemplo, tramitar la vulnerabilidad para realizar análisis más detallado, buscar información adicional del informante o de otras fuentes, decidir que no es necesario tomar medidas respecto a esta vulnerabilidad). Dependiendo de la calidad de la información suministrada y de lo detallada que sea en el informe sobre vulnerabilidades, puede resultar o no evidente que exista una nueva vulnerabilidad.

A menos que haya una razón para rechazar un informe sobre vulnerabilidades, éste debe transmitirse al servicio de análisis de vulnerabilidades para su examen, análisis y tratamiento ulteriores. Si el EIISI no proporciona el servicio de análisis de vulnerabilidades, se deberá transmitir el informe de manera segura a un grupo externo para su tramitación, ya sea a los proveedores afectados, los EIISP o al coordinador de vulnerabilidad.

Resultado: Se identifica la información disponible para determinar cómo proceder a continuación.

Se considera que las siguientes subfunciones forman parte de la implementación de este servicio:

- tramitar informes y datos presentados, incluidos los artefactos o materiales en forma aislada, para proteger la integridad del entorno laboral y evitar que se produzcan ataques exitosos contra el EIISI por esos medios;
- actualizar el acuse de recibo de informes, proporcionando información sobre las medidas ulteriores a partir de los resultados de la categorización o el establecimiento de prioridades;
- fusionar la nueva información sobre la vulnerabilidad que se esté gestionando con los datos disponibles para poder realizar un análisis y un procesamiento coherentes.

7.3 Servicio: Análisis de vulnerabilidades

Finalidad: Analizar y comprender las vulnerabilidades confirmadas.

Descripción: El servicio de análisis de vulnerabilidades consiste en funciones destinadas a comprender la vulnerabilidad y sus posibles repercusiones, identificar el problema o fallo subyacente (causa raíz) que permite explotar la vulnerabilidad, y determinar una o más estrategias de reparación o mitigación para evitar o reducir al mínimo la explotación de la vulnerabilidad.

El servicio y las funciones de análisis de la vulnerabilidad pueden continuar en paralelo mientras que el servicio y las funciones de coordinación de la vulnerabilidad se producen con otros participantes en un proceso coordinado de divulgación de la vulnerabilidad (CVD)[7].

Resultado: Se aumenta el conocimiento de los detalles clave de una vulnerabilidad (por ejemplo, la descripción, el impacto, la resolución).

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- clasificación de vulnerabilidades (validación y categorización);
- análisis de la causa raíz de la vulnerabilidad;
- desarrollo de reparaciones de la vulnerabilidad.

7.3.1 Función: Clasificación de vulnerabilidades (validación y categorización)

Finalidad: Categorizar, priorizar y realizar una evaluación preliminar de la vulnerabilidad.

Descripción: El servicio de análisis de vulnerabilidades comienza con un examen de la información disponible para categorizar, priorizar y evaluar los posibles efectos de la vulnerabilidad en los sistemas involucrados, servicio que forma parte del mandato del EIISI. Parte de esta información puede haberse documentado en ejecutar la función de clasificación y procesamiento de informes sobre vulnerabilidades (del servicio de admisión de informes de vulnerabilidad) si la vulnerabilidad fue comunicada al EIISI por un mandante o un tercero.

Si aún no se ha efectuado la clasificación preliminar, se puede asignar la vulnerabilidad a un experto en la materia para que realice una confirmación técnica de que tiene repercusiones para los sistemas implicados y se corresponde con el mandato del EIISI (es decir, las posibles repercusiones en la seguridad en las redes o sistemas pueden dañar la confidencialidad, disponibilidad o integridad de los activos de información en un ámbito de responsabilidad del EIISI).

Resultado: Se clasifica, prioriza y actualiza el registro de información de la vulnerabilidad.

[7] Para más información relacionada con la divulgación coordinada de la vulnerabilidad (CVD), véase en el ámbito de servicio coordinación y divulgación de vulnerabilidades.

7.3.2 Función: Análisis de la causa raíz de la vulnerabilidad

Finalidad: Comprender las deficiencias de diseño o implementación que causa o exhibe la vulnerabilidad.

Descripción: El objetivo de este análisis es identificar la causa raíz de la vulnerabilidad, en particular las circunstancias que permiten que exista dicha vulnerabilidad y, por ende, en qué circunstancias se puede explotar la vulnerabilidad. Mediante este análisis también se puede tratar de comprender las deficiencias explotadas para causar el incidente y la táctica utilizada para aprovechar ese punto débil. Según la naturaleza de la vulnerabilidad, puede resultar difícil para el EIISI desempeñar exhaustivamente esta función. En algunos casos, es posible que el inspector o el informante de la vulnerabilidad ya haya desempeñado esta función. En muchas situaciones, lo ideal es que sea el proveedor del producto, o el desarrollador del *software* o sistema afectado o su respectivo EIISP, el que realice esta función. Es igualmente posible que la vulnerabilidad esté presente en varios productos, en cuyo caso pueden ser necesarios múltiples análisis del *software* o los sistemas afectados, lo que requiere la coordinación con múltiples proveedores, EIISP o interesados.

Resultado: Se comprende la vulnerabilidad y la forma en que los agentes malignos podrán explotarla, y se utiliza esa información para determinar los métodos de reparación o mitigación que permitan minimizar el riesgo de exposición o explotación.

7.3.3 Función: Desarrollo de reparaciones de vulnerabilidades

Finalidad: Desarrollar los pasos necesarios para arreglar (reparar) la vulnerabilidad subyacente o mitigar (reducir) los efectos su explotación.

Descripción: Esta función permitirá, en teoría, encontrar una reparación o remedio para una vulnerabilidad. Si no se dispone oportunamente de un parche o remedio producido por el proveedor, se recomienda una solución temporal o una fórmula alternativa, denominada mitigación, como la desactivación del *software* afectado o la realización de cambios de configuración, para reducir al mínimo los posibles efectos negativos de la vulnerabilidad. Obsérvese que la aplicación o el despliegue efectivo de una reparación (parche) o mitigación (fórmula alternativa) es una función de otro servicio, el denominado respuesta a vulnerabilidades en este marco.

En el contexto del servicio de análisis de vulnerabilidades y desarrollo de reparaciones, esta función puede incluir opcionalmente otras subfunciones o actividades, como la validación del cambio de procedimiento o diseño, la revisión de la reparación por un tercero o la identificación de nuevas vulnerabilidades introducidas en las etapas de reparación. Las vulnerabilidades que no se solucionen o mitiguen deben documentarse como riesgos aceptables.

Para esta función se suele recibir información o datos del proveedor o proveedores del producto afectado, a veces integrados en el informe o anuncio inicial gestionado por otros servicios o funciones.

Resultado: Se establece un plan para cambiar (parchear) el código *software*, implementar una solución alternativa o mejorar los procesos, infraestructuras y/o diseños para cerrar el vector de ataque específico y evitar que se explote la vulnerabilidad.

Se considera que las siguientes subfunciones forman parte de esta función:

- desarrollo de una reparación/parche para la vulnerabilidad;
- desarrollo de una mitigación de la vulnerabilidad.

Por lo general, esta función la realizan otras entidades (por ejemplo, los proveedores de productos, los EIISP).

7.4 Servicio: Coordinación de vulnerabilidades

Finalidad: Intercambiar información y coordinar las actividades con los participantes en el proceso de divulgación coordinada de vulnerabilidades (CVD).

Descripción: La gestión de la mayoría de las vulnerabilidades implica notificar, colaborar y coordinar el intercambio de información relevante con múltiples partes, tales como los inspectores/informadores de vulnerabilidades, los proveedores afectados, los programadores, los EIISP u otros expertos de confianza (por ejemplo, investigadores, EIISI, coordinadores de vulnerabilidad) que pueden trabajar juntos para analizar y solucionar la vulnerabilidad.

Resultado: Se comparte información de manera eficaz y oportuna con los participantes en la CVD que pueden ayudar a proporcionar información para remediar/mitigar la vulnerabilidad.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- notificación/informe de vulnerabilidades;
- coordinación de vulnerabilidades con los interesados.

7.4.1 Función: Notificación/comunicación de vulnerabilidades

Finalidad: Compartir o comunicar información preliminar sobre nuevas vulnerabilidades con aquellos que participarán en el proceso CVD.

Descripción: La gestión de la mayoría de las vulnerabilidades implica notificar, colaborar y coordinar el intercambio de información relevante con múltiples partes, tales como los proveedores afectados, programadores, los EIISP u otros expertos de confianza (por ejemplo, investigadores, EIISI, coordinadores de vulnerabilidades) que pueden trabajar juntos para analizar y arreglar la vulnerabilidad.

Resultado: Se informa a los proveedores (u otros participantes en la CVD) sobre la vulnerabilidad y se procede a desarrollar una reparación o mitigación.

7.4.2 Función: Coordinación de vulnerabilidades con los interesados

Finalidad: Llevar a cabo la coordinación continua y el intercambio de información entre los diversos interesados y participantes en las actividades de divulgación coordinada de vulnerabilidades.

Descripción: Coordinar el intercambio de información entre los inspectores/investigadores, los proveedores, los EIISP y cualquier otro participante en las actividades de divulgación coordinada de vulnerabilidades (CVD) para analizar y arreglar la vulnerabilidad y preparar la divulgación de información al respecto. Esta coordinación comprende también el acuerdo de los participantes sobre el momento y la sincronización de la divulgación.

Resultado: La información sobre vulnerabilidades se comparte de manera más eficaz, oportuna y responsable entre los participantes que pueden elaborar o anunciar una solución de reparación/mitigación.

Se considera que la siguiente subfunción forma parte de esta función:

- preparación de la publicación de la vulnerabilidad.

7.5 Servicio: Divulgación de vulnerabilidades

Finalidad: Divulgar información sobre las vulnerabilidades conocidas a los mandantes para que puedan actuar basándose en dicha información con el fin de prevenir, detectar y remediar/mitigar las vulnerabilidades conocidas.

Descripción: Informar a los mandantes de cualquier vulnerabilidad conocida (puntos de entrada potenciales para los atacantes), de modo que sus sistemas se puedan mantener actualizados y verificar para detectar puntos débiles. Los métodos de divulgación consisten en la publicación de información a través de múltiples canales de comunicación (por ejemplo, sitios web, correo electrónico, redes sociales), bases de datos de vulnerabilidades u otros medios. Este servicio se suele prestar, aunque no siempre, después de la coordinación de vulnerabilidades.

Resultado: Los mandantes informados pueden evitar que se exploten las vulnerabilidades conocidas y pueden detectar y mitigar las vulnerabilidades ya existentes.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- política de divulgación de vulnerabilidades y mantenimiento de la infraestructura;
- anuncio/comunicación/divulgación de vulnerabilidades;
- información recibida tras divulgar vulnerabilidades.

7.5.1 Función: Política de divulgación de vulnerabilidades y mantenimiento de infraestructura

Finalidad: Elaborar y mantener una política que proporcione un marco y establezca expectativas sobre la forma en que el EIISI gestiona y divulga vulnerabilidades y los mecanismos utilizados para divulgar vulnerabilidades.

Descripción: Los EIISI que gestionan informes sobre vulnerabilidades deben definir su política de divulgación de vulnerabilidades y ponerla a disposición de sus mandantes, interesados y participantes en la CVD, preferiblemente publicándola en el sitio web del EIISI. La política de divulgación de vulnerabilidades proporcionará transparencia a los interesados y ayudará a promover políticas de divulgación adecuadas. Las políticas pueden consistir en la no divulgación –es decir, no se revela información sobre vulnerabilidades–, la divulgación limitada –sólo se pone a disposición una parte de la información– y la divulgación completa –en la que se revela toda la información, que puede incluir explotaciones de prueba de concepto. La política de divulgación debe incluir factores como el alcance de la política, referencias a cualesquiera mecanismos y directrices de notificación y los plazos y mecanismos previstos para la divulgación de vulnerabilidades.

Resultado: Se aumenta la confianza, la colaboración y el control de la divulgación y se mejoran las relaciones y la coordinación con los participantes en la CVD.

7.5.2 Función: Anuncio/comunicación/divulgación de vulnerabilidades

Finalidad: Proporcionar información a los mandantes (o al público) acerca de una nueva vulnerabilidad, de manera que puedan detectar, remediar o mitigar, y prevenir la explotación de la vulnerabilidad en el futuro.

Descripción: Divulgar información sobre la vulnerabilidad a los mandantes definidos. La divulgación puede hacerse a través de uno o de todos los mecanismos identificados en la política de divulgación de vulnerabilidades. Los mecanismos de divulgación pueden variar en función de las necesidades o expectativas de los destinatarios. La comunicación puede consistir en un anuncio o aviso de seguridad distribuido por correo electrónico o mensaje de texto, una publicación en un sitio web o en un canal de redes sociales, u otras formas y canales de comunicación, según proceda. El contenido que se incluirá en la divulgación deberá tener un formato predefinido, que en general incluye información general o descripción, un identificador único de la vulnerabilidad, su incidencia, la gravedad o la puntuación CVSS, la solución (reparación o mitigación) y referencias o materiales de apoyo.

Resultado: Se previene, detecta y remedia/mitiga la vulnerabilidad gracias al suministro de información oportuna, de alta calidad y eficaz a los mandantes (o al público en general).

7.5.3 Función: Recibir información después de divulgar la vulnerabilidad

Finalidad: Recibir y responder a cuestiones o informes de los constituyentes acerca de un documento o divulgación de vulnerabilidades.

Descripción: Tras divulgar información sobre una nueva vulnerabilidad, cabe esperar que los EIISI reciban comunicaciones de respuesta en la forma de preguntas de mandantes acerca del documento de vulnerabilidades. En respuesta a esas preguntas puede ser necesario aclarar, revisar o enmendar el mecanismo de divulgación de la vulnerabilidad, previa justificación. La información de los mandantes puede consistir simplemente en un acuse de recibo al documento de vulnerabilidad, o puede informar de un problema o dificultad para aplicar la reparación o mitigación sugerida. Si se determina que la vulnerabilidad ya ha sido explotada, los mandantes pueden informar sobre incidentes recientemente descubiertos como resultado de la divulgación

de la vulnerabilidad. Esos informes deben tenerse en cuenta para las funciones del servicio de notificación de incidentes del EIISI.

Resultado: Se responde oportunamente a cualquier pregunta o solicitud de asistencia después de la divulgación de la vulnerabilidad.

7.6 Servicio: Respuesta a vulnerabilidades[8]

Finalidad: Adquirir activamente información sobre las vulnerabilidades conocidas y actuar teniendo en cuenta esa información para prevenir, detectar y remediar/mitigar esas vulnerabilidades.

Descripción: Las funciones de este servicio tienen por objeto determinar si los sistemas de los mandantes adolecen de las vulnerabilidades señaladas, para lo cual a menudo se investiga deliberadamente la presencia de tales vulnerabilidades. El servicio también puede incluir la supervisión para solucionar o mitigar la vulnerabilidad mediante la aplicación de parches o estrategias alternativas.

Resultado: Se actúa tras recibir información con el fin de detectar la presencia de la vulnerabilidad, remediarla/mitigarla y evitar que sea explotada.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- detección/exploración de vulnerabilidades;
- reparación de vulnerabilidades.

Este servicio de respuesta a vulnerabilidades y sus funciones conexas suelen estar a cargo de otros grupos especializados dentro de la organización, que normalmente no es el EIISI. También es poco probable que este servicio lo preste el EIISI coordinador.

7.6.1 Función: Detección/exploración de vulnerabilidades

Finalidad: Participar activamente en la búsqueda de vulnerabilidades conocidas presentes en los sistemas desplegados.

Descripción: El objetivo de esta función es detectar cualquier vulnerabilidad no parcheada o no mitigada antes de que sea explotada o afecte a la red o los dispositivos. Esta función puede iniciarse en respuesta a un anuncio sobre una nueva vulnerabilidad, o en el contexto de una exploración programada periódicamente para detectar vulnerabilidades conocidas. A fin de detectar eficazmente vulnerabilidades, es útil disponer de un inventario de sistemas, que pueda consultarse para obtener información sobre la versión del *software* a fin de que la organización

[8] Si bien la función y las subfunciones para la detección de vulnerabilidades se denominan a veces "gestión de vulnerabilidades", el presente marco de servicios del EIISI se refiere a ellas como parte de este servicio de respuesta a la vulnerabilidad, que forma parte del ámbito de servicio más amplio denominado gestión de vulnerabilidades en este marco.

pueda evaluar rápidamente la probabilidad de que exista una vulnerabilidad recién notificada en su infraestructura.

Esta función puede recibir información o ser activada por otros servicios y funciones.

Resultado: Se detectan vulnerabilidades mediante procesos o instrumentos oficiales diseñados para identificarlas.

Se considera que las siguientes subfunciones forman parte de esta función:

- exploración/caza de vulnerabilidades;
- evaluaciones de seguridad/pruebas de penetración de vulnerabilidades.

Esta función la realizan típicamente otras entidades (por ejemplo, el servicio informático, el SOC, especialistas de terceros, propietarios de sistemas).

7.6.2 Función: Reparación de vulnerabilidades

Finalidad: Solucionar o mitigar vulnerabilidades para evitar su explotación, normalmente mediante la aplicación oportuna de parches u otras soluciones proporcionadas por los proveedores.

Descripción: La reparación de vulnerabilidades tiene por objeto resolver o eliminar vulnerabilidades. En el caso de vulnerabilidades del *software*, por lo general se recurre al despliegue e instalación de soluciones proporcionadas por los proveedores en la forma de actualizaciones o parches del *software*. Cuando no se dispone de parches aprobados o no se pueden desplegar, se puede aplicar una mitigación o solución alternativa para evitar la explotación de vulnerabilidades. Esta función suele aplicarse después de haber identificado la vulnerabilidad mediante la función de detección/exploración/caza de vulnerabilidades.

Resultado: Se impide o reduce la amenaza de explotación de la vulnerabilidad.

Se considera que las siguientes subfunciones forman parte de esta función:

- reparación de vulnerabilidades (gestión de parches);
- mitigación de vulnerabilidades.

Normalmente, esta función no la realiza el EIISI, sino otras entidades (por ejemplo, TI, SOC, propietarios del sistema).

8 Ámbito de servicio: Consciencia coyuntural

Por consciencia coyuntural se entiende la capacidad de identificar, procesar, comprender y comunicar los aspectos esenciales de lo que está sucediendo en el ámbito de responsabilidad del EIISI y que pueda afectar a las actividades o a la función de sus mandantes. La consciencia coyuntural implica conocer el estado actual e identificar o prever los posibles cambios en ese estado. Este ámbito de servicio incluye determinar la forma de recabar información pertinente de diferentes esferas, cómo integrar esa información y cómo difundirla de manera oportuna para que los mandantes puedan adoptar decisiones adecuadas. Algunas organizaciones establecen un equipo separado para proporcionar el servicio de consciencia coyuntural, mientras que en otras es el equipo del EIISI el que desempeña esta función debido a su visibilidad, comprensión del contexto, capacidades técnicas, acceso a los activos, conexiones externas y función de prevención de incidentes. La consciencia coyuntural no se ciñe exclusivamente en la respuesta a incidentes, es un servicio que garantiza que los datos, el análisis y las acciones estén disponibles para otros servicios como el de gestión de eventos de seguridad, la gestión de incidentes y la transferencia de conocimientos. También garantiza que la información procedente de esos otros ámbitos de servicios se integre adecuadamente en conjunto y se entregue a los componentes apropiados de manera oportuna.

Los siguientes servicios son ofertas de este ámbito de servicio:

- adquisición de datos;
- análisis y síntesis;
- comunicación.

8.1 Servicio: Adquisición de datos

Finalidad: Recopilar datos que ayuden a aumentar la visibilidad de las actividades internas y externas que puedan afectar a la postura de seguridad de los mandantes.

Descripción: Solicitar, recopilar, determinar y satisfacer los requisitos de información de los mandantes para conocer importantes actividades internas y externas pertinentes. Este servicio comprende la logística de la recopilación de información relevante, incluidas noticias de eventos actuales, la programación de eventos futuros, informes y fuentes, el filtrado de la información recabada, la organización de la información para utilizarla en el análisis de incidentes, la prevención, detección u otras actividades (como la planificación o el análisis de tendencia), el almacenamiento para su utilización posterior, la mejora de su "capacidad de búsqueda", y más. Los datos recopilados se utilizarán para determinar las medidas preventivas necesarias y para ayudar a tomar decisiones informadas en relación con la gestión de incidentes y las actividades relacionadas con garantías de la información. Sin una adecuada percepción de los elementos contextuales importantes, aumenta el riesgo de que otros servicios se formen una imagen incorrecta. Los EIISI tendrán que establecer políticas y procedimientos, y podrán emplear tecnología para reunir y examinar la información.

Resultado: Este servicio produce los siguientes artefactos:

- un conjunto de requisitos para la recopilación de datos que identifica las necesidades de consciencia coyuntural y luego asigna esos requisitos a los tipos de información que se han de recabar para cumplir esos objetivos;
- información sobre la situación presente y futura prevista de los activos y actividades de los mandantes;
- información sobre eventos o tendencias externas que permita conocer el entorno de los mandantes y el contexto actual, incluidas las nuevas tecnologías, métodos, prácticas, riesgos y amenazas;
- información con formato adecuado para actividades de análisis y detección.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- agregación, extracción y orientación de políticas;
- correspondencia entre activos a funciones, roles, acciones y principales riesgos;
- recopilación;
- procesamiento y preparación de datos.

8.1.1 Función: Agregación, extracción y orientación de políticas

Finalidad: Establecer el contexto con el que los mandantes y sus activos deben cumplir para saber lo que debe ocurrir en la infraestructura.

Descripción: La recopilación, agregación y extracción de política sienta las bases de la actividad normal aceptable. El resultado final es un contexto que establece cómo se supone que los mandantes y su infraestructura deben funcionar en condiciones aceptables. En el caso de los EIISI de la organización, el contexto incluye comprender las políticas, los planes, las condiciones normales de funcionamiento, los riesgos aceptados y los equilibrios que resultan aceptables de la organización. La comprensión y el contexto sientan las bases con las que se pueden evaluar las observaciones.

Resultado: Se comprenden las observaciones aceptables que están realizando los mandantes. Esta comprensión se basa en los cambios o repercusiones en la infraestructura y los activos.

8.1.2 Función: Relación de correspondencia de los activos con funciones, papeles, acciones y principales riesgos

Finalidad: El conocimiento de los activos existentes, la titularidad, las referencias y la actividad prevista son importantes para las funciones de análisis que identifican la observaciones coyunturales anómalas.

Descripción: Los EIISI necesitan comprender el estado actual de la ciberseguridad cibernética de sus mandantes, y tener que comprender bien cuál es la seguridad aceptable. Quizás necesiten saber:

- los usuarios legítimos de los sistemas y dispositivos internos y de cara al público;
- los dispositivos autorizados y para qué se utilizan;

- los procesos y aplicaciones aprobados, dónde están permitidos y cómo sirven a los mandantes.

Esta información ayuda a establecer prioridades en los bienes que pueden estar en peligro, lo que sirve de contexto para las actividades de gestión de incidentes. Cuanto más precisa sea la información de que disponga el EIISI, más fácil será prever problemas de seguridad y actuar en consecuencia. Disponer de información precisa significa que el EIISI tiene acceso a las políticas de seguridad establecidas, los controles de acceso vigentes, los inventarios actualizados de equipos y *software* y a los diagramas de red detallados.

Resultado: Las siguientes listas son el resultado de esta función:

- lista de las principales funciones y los activos que las respaldan; algunos activos pueden respaldar múltiples funciones;
- lista de los papeles que desempeña cada función y su papel digital equivalente en el activo;
- lista de acciones generalmente permitidas por cada papel;
- lista de los principales riesgos que corren los activos y las funciones.

Estas listas evolucionan con arreglo a los cambios coyunturales.

8.1.3 Función: Recopilación

Finalidad: Recopilar información para el servicio de análisis e interpretación y/u otros servicios del EIISI.

Descripción: Las actividades de recopilación de información y datos no se ciñen a las fuentes que proporcionan información de manera automática. La recopilación incluye la identificación de fuentes útiles como actividades externas relevantes para la información, en particular noticias de otros mandantes, medios de comunicación y otros EIISI u organizaciones de seguridad, actividades internas (por ejemplo, cambios orgánicos), desarrollos tecnológicos, eventos externos, eventos políticos, tendencias de ataque y defensivas, conferencias, formación disponible, etc.

La función de recopilación de datos da soporte a otros servicios como la gestión de eventos de seguridad, la gestión de incidentes y la transferencia de conocimientos. También da soporte a funciones y actividades dentro de estos servicios como el análisis, la predicción, la respuesta y la mitigación de riesgos. La información recién recopilada puede revelar que ha aumentado la probabilidad de ataque a un determinado componente. Los eventos externos pueden revelar información sobre nuevos riesgos para los activos durante un periodo de tiempo o requerir actividades de detección más intensas. En general, la información aporta datos procesables que ayudan a tomar decisiones y gestionar incidentes.

Resultado: Se recopilan y producen datos y conjuntos de datos para crear un contexto operativo o ambiental que pueda ser utilizado por otros servicios y funciones, incluido el análisis, para proporcionar a los constituyentes una imagen coyuntural, identificar alertas o planificar la mitigación de las esferas de mayor riesgo para los activos y las infraestructuras de apoyo.

8.1.4 Función: Procesamiento y preparación de datos

Finalidad: Establecer un conjunto de datos fiables, coherentes y actuales que puedan dar soporte a las actividades del EIISI y a los requisitos del servicio de análisis.

Descripción: El procesamiento y la preparación de datos comprende la transformación, el procesamiento, la normalización y la validación de un conjunto de datos. Es necesario validar la exactitud de las fuentes de datos sobre ciberseguridad, debido al elevado número de falsos positivos. Por otra parte, los datos pertinentes suelen estar en diferentes formatos y los nuevos datos deben combinarse con los datos históricos antes de poder realizar un análisis completo. Es posible que algunos tipos de datos (como los artículos periodísticos) tengan que analizarse o procesarse durante la preparación. Un ejemplo sería extraer la información de seguridad pertinente de un artículo periodístico (por ejemplo, nombres, fechas, lugares, información técnica, puntos débiles, nombres de sistemas) y compararla con los datos internos para determinar los posibles efectos.

Algunos métodos de análisis requieren que los datos se almacenen en el mismo formato o que los archivos tengan el mismo número de registros. Para preparar los datos pueden ser necesarias múltiples etapas de procesamiento. El aumento de los datos (también llamado acumulación) se realiza incluyendo otra información disponible sobre un dato determinado de otras fuentes internas y externas. Por ejemplo, los equipos pueden reunir información relacionada con las direcciones del protocolo de Internet (direcciones IP), como los identificadores de sistemas autónomos, indicativos de país o datos de geolocalización. En cuanto a la información interna sobre los activos, los equipos pueden acumular datos de su inventario de activos con el nombre del propietario del activo, su función, sus permisos sobre otros activos, su ubicación física de trabajo a lo largo del tiempo y otros datos más.

Resultado: Se dispone de datos para ser utilizados por otros servicios o funciones.

8.2 Servicio: Análisis y síntesis

Finalidad: Evaluar cuándo la situación no se ajusta a las expectativas (por ejemplo, cuando determinados activos están a punto de sufrir un evento perjudicial).

Descripción: El proceso de utilizar datos actuales e históricos y técnicas de análisis para determinar si lo que está ocurriendo puede afectar a los activos de los mandantes y a la postura en materia de seguridad, para lo cual a menudo se determina una respuesta a una pregunta o por intuición. El análisis puede revelar si los eventos no coinciden con el comportamiento típico esperado, o puede revelar información sobre las circunstancias, la naturaleza o el origen de los eventos o comportamientos. El análisis puede revelar repercusiones para situaciones actuales y futuras. Por ejemplo: el sistema puede registrar que un ID de usuario ha iniciado sesión en el sistema, pero éste no indica si el evento fue realizado por un usuario legítimo. Será necesario incorporar en el análisis nuevas fuentes (como entrevistas al usuario) para proporcionar una imagen más precisa que permita determinar la legitimidad del evento. Se pueden utilizar diversas técnicas para analizar e interpretar los datos recabados y su efecto en los mandates.

Resultado: Se formula un conjunto de conclusiones sobre los probables eventos presentes, pasados y/o futuros probables en el ámbito de los mandantes. También puede incluir

recomendaciones sobre ciertas decisiones que han de tomar los mandantes. El análisis debe basarse en pruebas empíricas, por ejemplo, datos de observación medidos con sensores y otras fuentes y en la interpretación que de esas pruebas han hecho los analistas por diversos métodos. El análisis puede indicar además los mandantes a los que hay que informar de los resultados y de lo que hay que informarles.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- proyección e inferencia;
- detección de eventos (mediante alerta y/o caza);
- impacto coyuntural.

8.2.1 Función: Proyección e inferencia

Finalidad: Analizar la información recabada durante la adquisición de datos con el fin de identificar los posibles panoramas coyunturales presentes o predecir las futuras.

Descripción: El proceso de inferir la situación actual y predecir los posibles escenarios a corto plazo a partir del estado y la dinámica de los datos recabados. A menudo los datos muestran rápidamente un problema de seguridad.

Resultado: Se actualiza el panorama coyuntural con arreglo a los conocimientos obtenidos cuando dicha imagen cambio o puede cambiar.

8.2.2 Función: Detección de eventos (mediante alerta y/o caza)

Finalidad: Determinar y confirmar los detalles sobre el panorama coyuntural de los mandantes.

Descripción: Búsqueda sistemática y a menudo dirigida de actividades anómalas dentro y fuera de los límites de la red, a partir de información y tendencias externas e internas. Para ayudar a los mandantes a analizar los datos de sus sensores y otras fuentes para sacar conclusiones sobre su entorno y situación. Por ejemplo, si un sensor antivirus envía una alerta de archivo sospechoso, el equipo puede analizar la configuración del sistema, la configuración del sensor, el archivo del caso, la actividad del usuario en ese momento y otros aspectos, para llegar a una conclusión sobre la gravedad de la observación. Esta función puede recibir datos significativos del ámbito de servicio de gestión de eventos de seguridad. Las observaciones de los sensores que se utilizan para detectar eventos pueden ser compartidas entre múltiples servicios.

Los equipos del EIISI también necesitan determinar la coyuntura actual basándose en elementos específicos de información sobre las amenazas. Esta actividad puede denominarse a veces "caza de amenazas". Por lo general, la caza de amenazas implica la preparación del entorno para detectar una actividad de amenaza específica, o bien la búsqueda de una actividad de amenaza específica que pueda estar ya presente.

Resultado: Se actualiza el panorama coyuntural a partir de la detección de eventos en los mandantes.

8.2.3 Función: Ayuda a tomar decisión de gestión de incidentes de seguridad de la información

Finalidad: Identificar nuevas pistas cuando se producen incidentes y contribuir a limitar los daños, mitigar los riesgos futuros o identificar puntos débiles recién creados.

Descripción: La realización de análisis de pruebas específicas ayuda a identificar pistas para la resolución de incidentes. A veces, los EIISI pueden centrar su análisis coyuntural para reforzar un resultado deseado específico como la resolución de incidentes. Ciertas respuestas a incidentes pueden afectar de manera diferente al panorama coyuntural, y los encuestados pueden solicitar un análisis de las opciones (por ejemplo, repercusiones, coste, riesgo de fallo). Las necesidades de los mandantes a la hora de tomar decisiones pueden variar a medida que evoluciona su panorama coyuntural, y el equipo del EIISI puede iniciar nuevos procesos de análisis para ayudarles. Esta actividad guarda relación con el ámbito de servicios de gestión de incidentes. Las funciones de gestión de incidentes cuenta con la ayuda de la consciencia coyuntural y el panorama coyuntural puede cambiar en función de las actividades de gestión de incidentes.

Resultado: Se mejora la consciencia coyuntural para las funciones de gestión de incidentes basadas en nuevas observaciones. Se actualiza el panorama coyuntural a partir de las actividades de gestión de incidentes.

8.2.4 Función: Impacto coyuntural

Finalidad: Determinar el posible impacto esperado de una determinada observación real o de una posible observación en un panorama coyuntural.

Descripción: Esta función identifica el impacto que una proyección o inferencia puede tener sobre una situación presente o futura a corto plazo. El impacto puede incluir el aumento o la disminución de ciertos riesgos como pérdida de datos, tiempo de inactividad del sistema o efectos en la confidencialidad/disponibilidad/integridad de los datos.

Resultado: Se produce un análisis del impacto probable que una inferencia o proyección puede tener sobre una situación.

8.3 Servicio: Comunicación

Finalidad: Notificar a los mandantes u otros interesados de la comunidad de seguridad sobre los cambios en los riesgos del panorama coyuntural.

Descripción: El conocimiento obtenido de la consciencia coyuntural debe comunicarse a los mandantes. De esta manera se les permitirá reaccionar a las observaciones y adoptar las medidas que mejoren la situación defensiva, por ejemplo, mediante la mejora del entorno de seguridad de ciertos proveedores de alto riesgo para reducir el riesgo de terceros.

Resultado: Se suministra a los mandantes información precisa, procesable y oportuna sobre la situación, de modo que puedan comprender mejor su pasado y mejorar el panorama coyuntural presente y futuro.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- comunicación interna y externa;
- informes y recomendaciones;
- implementación;
- divulgación/integración/intercambio de información;
- gestión del intercambio de información.

8.3.1 Función: Comunicación interna y externa

Finalidad: Informar a los mandantes (y otros) del panorama coyuntural actual y cómo podría estar cambiando.

Descripción: Una vez que los resultados del análisis e interpretación estén completos, pueden utilizarse para mejorar la toma de decisiones a través de procesos de comunicación internos y externos. Los elementos concretos de información se distribuyen en función de a quién conciernen. La comunicación consta del método de suministro y del contenido suministrado. El EIISI puede comunicar nueva información y explicar cómo cambiará el panorama coyuntural. Un ejemplo sería informar sobre qué efecto tendría para un mandante el cambio observado durante un incidente de una nueva técnica maliciosa. También puede añadir información sobre tendencias, como las fuentes más útiles para la acumulación de datos y las medidas que pueden tomar los mandantes para mejorar su consciencia coyuntural.

Resultado: Los mandantes están mejor informados y preparados para adoptar medidas o tomar decisiones que mejoren su seguridad o situación.

8.3.2 Función: Información y recomendaciones

Finalidad: Generar resultados, artefactos o hallazgos que comuniquen información esencial descubierta o generada durante el análisis de audiencias en un formato que les resulte fácil de comprender.

Descripción: Los informes y las recomendaciones deben indicar claramente las opciones y las medidas que han de tomar los mandantes e incluir un análisis de las consecuencias previstas para cada opción o medida. La comunicación de hallazgos debe incluir una lista de las pruebas que respalden el análisis y la recomendación (en caso de formular una recomendación). Los métodos utilizados para llegar a esos hallazgos deben explicarse claramente para que los destinatarios puedan juzgar también las alegaciones formuladas. El EIISI puede crear informes sobre un solo evento, una serie de eventos, tendencias, pautas, posibles eventos, etc., para que sus mandantes comprendan la necesidad de conocer el panorama coyuntural.

Resultado: Se mejora la capacidad de proporcionar informes precisos, oportunos y completos sobre el panorama coyuntural, las pruebas que respaldan las conclusiones y/o las recomendaciones sobre las distintas formas de proceder y sus posibles efectos para los mandantes.

8.3.3 Función: Implementación

Finalidad: Adaptar el entorno de mandantes en función de las comunicaciones para que estén más preparados o reaccionen a los cambios en el panorama coyuntural.

Descripción: En algunos casos, el EIISI puede realizar también los ajustes recomendados a partes de la infraestructura de seguridad, por ejemplo, modificar las reglas del cortafuegos o un sistema de señuelos con arreglo al análisis coyuntural.

Resultado: Los mandantes actúan de una manera determinada o modifican la infraestructura con arreglo a las comunicaciones recibidas contenidas en los análisis, proyecciones y/o recomendaciones.

8.3.4 Función: Divulgación/integración/compartición de información

Finalidad: Juntar, normalizar y preparar información para compartirla con los mandantes y otros interesados.

Descripción: Esta función puede constar de las siguientes subfunciones:

- utilizar los resultados del servicio de análisis en los procesos de planificación y toma de decisiones internos y externos;
- identificar los destinatarios adecuados para recibir la información;
- poner a disposición los resultados de los análisis;
- garantizar el suministro adecuado de información;
- rastrear y presentar informes sobre el intercambio de información;
- enviar la información pertinente al servicio de transferencia de conocimientos para su utilización y difusión ulteriores.

Resultado: Los resultados del análisis de consciencia coyuntural se utilizan (tanto a nivel interno como entre los mandantes) en procesos de decisión esenciales, por ejemplo, en la caza de amenazas, el análisis de incidentes y la resolución. Los resultados se divulgan en el marco de la gestión o detección de incidentes. La información y los datos procedentes del análisis de consciencia coyuntural también pueden convertirse en prácticas idóneas, informes, material didáctico y de sensibilización a través del ámbito de servicios de transferencia de conocimientos.

8.3.5 Función: Gestión del intercambio de información

Finalidad: Garantizar la transferencia de información efectiva y útil.

Descripción: Esta función puede constar de las siguientes subfunciones:

- suministrar información a otros grupos;
- dar formato a la información para su transferencia;
- rastrear el proceso de transferencia y su resultado.

Resultado: Se garantiza el intercambio de información adecuada y, una vez compartida, que la reciben los asociados, mandantes y otros miembros de la comunidad. Se redactan informes sobre la actividad de intercambio.

8.3.6 Función: Recepción de opiniones

Finalidad: Mejorar la calidad, la puntualidad, la precisión y la pertinencia de los datos que se reciben de fuentes internas y externas.

Descripción: Esta función consiste en proporcionar y recibir opiniones sobre la información proporcionada, recibida y utilizada por los mandantes, otros proveedores de servicios u otros interesados. ¿La información recibida era exacta, aplicable, oportuna, estratégica, nueva/novedosa, etc.? ¿Resultó útil para resolver la investigación? ¿Aportó nuevas pistas? Para ello puede ser necesario proporcionar información también a otros EIISI (como fuente externa) sobre la utilidad de las signaturas o su modificación, hallazgos sobre señuelos, clases de objetos de información (IOC), alertas, información sobre amenazas, medidas de mitigación, etc. Esta actividad también puede ser realizada por el ámbito de servicio de transferencia de conocimientos. En tal caso, los resultados deben comunicarse al ámbito de servicio de consciencia coyuntural.

Resultado: Se formulan observaciones y se recaba la opinión de fuentes internas y externas para mejorar la exactitud, puntualidad, calidad y utilidad de la información recibida.

9 Ámbito de servicio: Transferencia de conocimientos

Por la naturaleza de sus servicios, los EIISI están en una posición única para recopilar datos pertinentes, realizar análisis detallados e identificar amenazas, tendencias y riesgos, así como para crear las prácticas idóneas operativas actuales que ayuden a las organizaciones a detectar, prevenir y responder a los incidentes de seguridad. La transferencia de estos conocimientos a sus mandantes es fundamental para mejorar la seguridad cibernética en general.

Se considera que este ámbito de servicio en particular presta los siguientes servicios:

- sensibilización;
- formación y educación;
- ejercicios;
- asesoramiento técnico y de políticas.

9.1 Servicio: Sensibilización

Finalidad: Aumentar la postura general de los mandantes respecto de la seguridad y ayudar a sus miembros a detectar, prevenir y recuperarse de incidentes; velar por que los mandantes estén mejor preparados y educados.

Descripción: Este servicio consiste en la colaboración con mandantes, expertos y asociados de confianza para aumentar la comprensión colectiva de las amenazas y las medidas que pueden adoptarse para prevenir o mitigar los riesgos que plantean esas amenazas.

Resultado: Se logra que los mandantes sean conscientes de:

- eventos, actividades y tendencias que pueden afectar a su capacidad de actuar de manera oportuna y segura;
- medidas que deben adoptarse para detectar, prevenir y mitigar las amenazas y las actividades maliciosas;
- seguridad y prácticas idóneas operativas.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- investigación y agregación de información;
- elaboración de informes y material de sensibilización;
- divulgación de la información;
- alcance.

9.1.1 Función: Investigación y agregación de información

Finalidad: Agregar, cotejar y priorizar la información que puede divulgarse al público para mejorar la postura de seguridad y la prevención y mitigación de riesgos.

Descripción: Esta función implica investigar y agregar información relevante para la creación de materiales e informes destinados a la sensibilización, en particular los resultados de otros servicios/funciones, especialmente de los ámbitos de servicio de gestión de eventos de seguridad, gestión de incidentes y consciencia coyuntural.

Resultado: Se agrega información sobre las tendencias pertinentes, los incidentes en curso y las prácticas idóneas, que pueden utilizarse para elaborar informes y materiales de sensibilización para destinatarios diversos.

9.1.2 Función: Elaboración de informes y material destinado a la sensibilización

Finalidad: Utilizar la información agregada e investigada como relevante para producir material en diferentes medios con el objetivo de adaptarlos a diferentes destinatarios o suministrar contenidos específicos de la mejor manera posible.

Descripción: Esta función consiste en elaborar materiales para diversos destinatarios (personal técnico, directivos, usuarios finales, etc.) y en diversos formatos, como ponencias, vídeos breves, dibujos animados, folletos, análisis técnicos, informes de tendencias e informes anuales.

Resultado: El EIISI elabora informes y materiales destinados a la sensibilización con una calidad adecuada para satisfacer las necesidades de los mandantes, utilizando para ello diversas técnicas y plataformas de distribución eficaces.

9.1.3 Función: Divulgación de información

Finalidad: Divulgar información relacionada con la seguridad para mejorar la sensibilización y la aplicación de las prácticas de seguridad.

Descripción: Esta función implica la ejecución de un proceso de divulgación de información que puede ayudar al EIISI a suministrar de manera óptima sus informes y materiales de sensibilización a los mandantes, basándose en las características de los diferentes destinatarios y contenidos.

Resultado: Se establece un marco de divulgación de información para permitir que los mandantes del EIISI tengan acceso a información oportuna y pertinente a través de diferentes métodos, como podcasts, bitácoras, medios sociales y vídeos, comunicados de prensa, anuncios, campañas, informes públicos, etc.

9.1.4 Función: Difusión

Finalidad: Desarrollar y mantener relaciones con expertos u organizaciones que puedan ayudar o participar en la ejecución de la misión del EIISI.

Descripción: Esta función implica la creación de alianzas, el fomento de la cooperación y la participación de los principales interesados, ya sean mandantes internos o externos, con el objetivo de sensibilizar y divulgar prácticas idóneas; ayudar a los mandantes y a interesados externos a comprender los servicios y ventajas que puede aportar el EIISI; ayudar al EIISI a comprender mejor las necesidades de los mandantes; y permitir que el EIISI lleve a cabo su cometido. A tal efecto, se debe garantizar la interoperabilidad o fomentar la colaboración entre organizaciones.

Resultado: Se realizan actividades de divulgación activas y coherentes que pueden incluir, entre otras cosas, la reunión con los principales interesados, la participación en reuniones del sector, la presentación en conferencias y la organización de conferencias.

9.2 Servicio: Formación y educación

Finalidad: Proporcionar formación y educación a los mandantes del EIISI (comprendido personal de la organización y del EIISI) sobre temas relacionados con la ciberseguridad, garantía de la información y gestión de incidentes.

Descripción: Los programas de formación y educación pueden ayudar al EIISI a establecer relaciones y a mejorar la postura general de ciberseguridad de sus mandantes, en particular la capacidad de prevenir futuros incidentes. Un programa de este tipo puede:

- ayudar a sensibilizar al usuario;
- ayudar a los mandantes a entender el panorama cambiante y las amenazas;
- facilitar el intercambio de información entre el EIISI y sus mandantes;
- formar a los mandantes sobre herramientas, procesos y procedimientos relacionados con la seguridad y la gestión de incidentes.

Para ello se puede recurrir a diversos tipos de actividades, como la documentación de los conocimientos, aptitudes y capacidades (KSA) necesarios, la elaboración de material educativo y didáctico, el suministro de contenidos, tutorías y el desarrollo profesional y de aptitudes. Cada una de estas actividades contribuirá colectivamente a la capacitación del equipo y sus mandantes.

Resultado: Se proporciona un programa coherente de formación y educación que permite a los mandantes del EIISI:

- disponer de métodos para detectar, prevenir o responder a las amenazas;
- conocer herramientas y prácticas que contribuyen a proteger los activos críticos;
- comprender los procesos de gestión de incidentes y cómo obtener asistencia.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- recopilación de necesidades en materia de conocimientos, aptitudes y destrezas;
- elaboración de material educativo y didáctico;
- suministro de contenido;

- tutorías;
- desarrollo profesional del personal del EIISI.

9.2.1 Función: Recopilación de necesidades en materia de conocimientos, aptitudes y destrezas

Finalidad: Evaluar, identificar y documentar adecuadamente las necesidades de los mandantes en lo que respecta a los conocimientos, aptitudes y capacidades, a fin de elaborar material educativo y didáctico adecuado y mejorar su nivel de conocimientos.

Descripción: Esta función consiste en recopilar las necesidades de los mandantes en cuanto a conocimientos, aptitudes y destrezas y la competencia de éstos en lo que respecta a la determinación de la formación y educación que se ha de proporcionar.

Resultado: Se caracterizan y documentan las necesidades de conocimientos y aptitudes de los mandantes para que se utilicen en la elaboración de material educativo y didáctico pertinente.

9.2.2 Función: Desarrollo de material educativo y didáctico

Finalidad: Elaborar, a partir de las necesidades de los mandantes, material educativo, instructivo y didáctico que resulte adecuado para los métodos de formación que se consideren mejores para los diferentes destinatarios o para un contenido específico.

Descripción: Esta función implica la creación o adquisición de contenido de material educativo y didáctico como ponencias, conferencias, demostraciones, simulaciones, vídeos, libros, folletos, etc.

Resultado: Se elabora material educativo y didáctico del EIISI utilizando distintas técnicas de presentación eficaces y se desarrollan plataformas con un nivel de calidad adecuado y que satisfacen las necesidades de los interesados.

9.2.3 Función: Suministro de contenido

Finalidad: Desarrollar un proceso oficial para el suministro de contenido que pueda ayudar al EIISI a suministrar a sus mandantes el contenido de manera óptima, con arreglo a las características de los diferentes destinatarios y contenidos.

Descripción: Esta función implica la transferencia de conocimientos y contenidos a "estudiantes", utilizando varios métodos, como la formación electrónica/en línea (CBT/WBT), dirigida por un tutor, virtual, conferencias, presentaciones, laboratorios, concursos de atrapar la bandera (CTF), libros, vídeos en línea, etc.

Resultado: Se diseña un marco de suministro de contenidos para ayudar a los mandantes a aprender habilidades y procesos técnicos e informáticos, utilizando todos los métodos alternativos, como libros, folletos, vídeos en línea, ponencias, laboratorios prácticos, CTF, CBT/WBT, formación presencial, etc. De resultas, los mandantes entienden el contenido suministrado.

9.2.4 Función: Tutorías

Finalidad: Elaborar un programa para que el personal del EIISI, los mandantes o los socios externos de confianza aprendan de un personal experimentado por medio de una relación establecida.

Descripción: El programa de tutorías puede contribuir a ofrecer un mecanismo formal o informal para que el tutor ayude al alumno sobre educación y el desarrollo de habilidades, conocimientos y experiencias de vida y de carrera en una relación extraoficial a la de información y estructura del equipo. Esta ayuda puede implicar visitas *in situ*, rotación (intercambio), supervisión y argumentación sobre decisiones y acciones específicas.

Resultado: Se incrementa la fidelidad, lealtad, confianza y capacidad general de tomar decisiones acertadas del EIISI. Los mandantes mejoran su nivel de conocimientos y su relación con el EIISI. Aumenta la capacidad y habilidad de los mandantes y los miembros del EIISI, comprendidas las relaciones de confianza.

9.2.5 Función: Desarrollo profesional del personal del EIISI

Finalidad: Ayudar a los miembros del personal a planificar y desarrollar adecuadamente sus carreras profesionales.

Descripción: Una vez identificadas las aptitudes adecuadas, el EIISI recurre al desarrollo profesional para promover un proceso de formación continua que permite consolidar nuevos conocimientos, habilidades y destrezas relacionados con la profesión de seguridad, responsabilidades laborales únicas, y el ambiente general del equipo. Puede consistir en la asistencia a conferencias, formación avanzada y en actividades de capacitación mutua, entre otras.

Resultado: Se dispone de personal formado y capacitado con habilidades técnicas e informáticas necesarias y con conocimiento de los procesos, y que mantienen sus conocimientos al día con arreglo a las funciones y necesidades de su trabajo. Los miembros del EIISI están preparados para hacer frente a los retos operacionales diarios, apoyando tanto al equipo como a sus clientes.

9.3 Servicio: Ejercicios

Finalidad: Realizar ejercicios para evaluar y mejorar la eficacia y la eficiencia de los servicios y funciones de seguridad cibernética.

Descripción: La organización ofrece servicios a los mandantes que dan soporte al diseño, la ejecución y la evaluación de los ejercicios cibernéticos destinados a formar y/o evaluar las capacidades de cada uno de los mandantes y de la comunidad de interesados en su conjunto, en particular las capacidades de comunicación. Estos tipos de ejercicios se pueden utilizar para:

- probar políticas y procedimientos: evaluar si existen políticas y procedimientos suficientes para detectar, responder y mitigar eficazmente los incidentes. Se trata, en general, de un ejercicio teórico/analítico;

- poner a prueba la preparación operativa: evaluar si la organización dispone de una capacidad de gestión de incidentes capaz de detectar, responder y mitigar incidentes de manera oportuna y satisfactoria, así como poner a prueba si dispone de personal adecuado, si los directorios están actualizados y si los procedimientos se ejecutan correctamente.

Este servicio atiende tanto a las necesidades de la organización como a las de sus mandantes. Concretamente, mediante la simulación de eventos/incidentes de seguridad cibernética, estos ejercicios pueden servir para uno o varios objetivos:

- Demostración: ilustrar los servicios y funciones de ciberseguridad, así como las vulnerabilidades, amenazas y riesgos, para que se tome conciencia al respecto.
- Capacitación: formar al personal sobre nuevas herramientas, técnicas y procedimientos:
  - Entrenamiento: ofrecer al personal la oportunidad de utilizar las herramientas, técnicas y procedimientos que deben conocer. Es necesario hacer ejercicios para no perder las habilidades y para mejorar y mantener la eficiencia.
  - Evaluar: analizar y comprender el nivel de eficacia y eficiencia de los servicios y funciones de ciberseguridad, así como el nivel de preparación del personal.
  - Verificar: determinar si se puede alcanzar un nivel de eficiencia y/o eficacia determinado para los servicios y funciones de ciberseguridad.

Resultado: Se mejora la eficacia y la eficiencia de los servicios y funciones de ciberseguridad y se identifican los aspectos susceptibles de ser mejorados.

En función de los objetivos específicos del ejercicio, la ciberseguridad también puede servir para hacer demostraciones a los interesados internas o externas, formar al personal y evaluar y/o verificar la eficiencia y eficacia de las herramientas, servicios y funciones. También pueden extraerse conclusiones para mejorar los futuros ejercicios e informar a este respecto a la dirección o a otros interesados importantes.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- análisis de los requisitos;
- definición del formato y contexto;
- preparación de casos;
- realización de ejercicios;
- examen de los resultados del ejercicio.

9.3.1 Función: Análisis de requisitos

Finalidad: Garantizar que el resultado del ejercicio sea eficaz, concentrándose en aspectos específicos para el alcance y el enfoque del mismo.

Descripción: Determinar los objetivos didácticos y el alcance del ejercicio. Definir los servicios, capacidades y temas específicos que formarán parte del ejercicio. Velar por que el ejercicio incluya actividades y temas relacionados con las aptitudes requeridas o deseadas de los participantes, así como los procesos que deben ser probados.

Resultado: Se describe el propósito del ejercicio, junto con un resumen de los objetivos de aprendizaje que deben cumplirse.

9.3.2 Función: Definir el formato y el contexto

Finalidad: Especificar y determinar los recursos internos y externos y la infraestructura necesarios para llevar a cabo el ejercicio.

Descripción: Definir el formato y la plataforma necesarios para cumplir los objetivos y obtener los resultados esperados del ejercicio.

Resultado: Se identifica el tipo de ejercicio (teórico, práctico, de simulación, etc.), así como los recursos internos y externos necesarios para realizarlo.

9.3.3 Función: Preparación de casos

Finalidad: Ofrecer la oportunidad para que los destinatarios mejoren la eficiencia y la eficacia de sus servicios y funciones, así como sus aptitudes, conocimientos y habilidades, mediante la gestión de eventos/incidentes de ciberseguridad simulados, incluidos los aspectos relacionados con las comunicaciones.

Descripción: Preparar distintos casos de ejercicios relacionados con los objetivos de los interesados. Los resultados comprenden también instrucciones y orientación para los participantes y los encargados de los ejercicios; estas instrucciones incluyen acciones recomendadas para los participantes en las que se detallan algunos/todos los pasos del caso.

Resultado: Se desarrolla un caso principal con variantes y diversos tipos de parámetros formalizados, junto con las tareas y asignación de roles al equipo encargado del ejercicio.

9.3.4 Función: Ejecución de ejercicios

Finalidad: Realizar simulacros/ejercicios que permitan al EIISI aumentar su confianza en la validez del plan de EIISI de la organización y su capacidad de ejecución.

Descripción: La función implica realizar pruebas de preparación de los mandantes "estudiantes" para comprobar su capacidad a la hora de aplicar los conocimientos estudiados y desempeñar sus funciones o su tarea. Puede ser en la forma de entornos reales o virtuales, simulaciones, pruebas de campo, ejercicios teóricos, simulaciones, o una combinación, con datos aportados de manera estructurada. Esto también ayudará a determinar el nivel eficacia del equipo, así como qué aspectos, en su caso, se pueden mejorar.

Resultado: El EIISI evalúa su grado de preparación y disposición, y vela por que los conocimientos, aptitudes y destrezas, los procesos fundamentales y la ejecución estén debidamente coordinados , o se deban adaptar/mejorar.

9.3.5 Función: Examen de los resultados del ejercicio

Finalidad: Realizar un análisis formal y objetivo del ejercicio, basado en observaciones objetivas.

Descripción: Elaborar un informe tras el ejercicio que incluya las lecciones extraídas o las conclusiones/prácticas idóneas resultantes del ejercicio, y suministrar una evaluación a los interesados/la dirección.

Resultado: Se crean productos en los que se destaca el éxito del ejercicio, los aspectos susceptibles de mejora, las conclusiones generales y las medidas recomendadas para mejorar: la capacidad de gestión de incidentes de la organización, los procesos del equipo del EIISI y las capacidades de cada mandante y de la comunidad de interesados en su conjunto, incluidas las capacidades y procedimientos de comunicación.

9.4 Servicio: Asesoramiento técnico y de políticas

Finalidad: Garantizar que las políticas y procedimientos de los mandantes incluyan consideraciones adecuadas de gestión de incidentes y, en última instancia, les permitan gestionar mejor los riesgos y amenazas, así como permitir que el EIISI sea más eficaz.

Descripción: Ayudar a los mandantes del EIISI y a los principales interesados, internos o externos, en las actividades relacionadas con la gestión de riesgos y la continuidad de las actividades, prestando asesoramiento técnico cuando sea necesario y contribuyendo a la creación y aplicación de las políticas de los mandantes, así como influyendo en ellas para que el EIISI sea más eficaz. Las políticas también son importantes para legitimar los servicios del EIISI.

Resultado: Se permite a los mandantes tomar decisiones organizativas basadas en las prácticas idóneas de seguridad operativa que incorporen las relativas a la continuidad de las actividades y recuperación en caso de catástrofe, y además se comprende la necesidad de incluir equipos de gestión de incidentes, en calidad de asesores de confianza, en las decisiones empresariales.

Se considera que las siguientes funciones forman parte de la implementación de este servicio:

- ayuda en la gestión de riesgos;
- ayuda en la planificación de la continuidad de las actividades y la recuperación en caso de catástrofe;
- ayuda en materia de política;
- asesoramiento técnico.

9.4.1 Función: Ayuda en la gestión de riesgos

Finalidad: Mejorar la identificación de oportunidades y amenazas, mejorar los controles, mejorar la prevención de pérdidas y la gestión de incidentes junto con la seguridad de la información y otras funciones pertinentes.

Descripción: Ayudar en las actividades relacionadas con la evaluación del riesgo o el cumplimiento. Queda comprendida la realización de una evaluación real o el asesoramiento para evaluar los resultados de una evaluación.

Resultado: Los mandantes pueden identificar los riesgos y amenazas y seleccionar las opciones de gestión de riesgos pertinentes, incluidas las estrategias de gestión de incidentes, los controles de seguridad o la mitigación de amenazas que sean apropiados y eficaces.

9.4.2 Función: Ayuda en la continuidad de las actividades y ayuda a la recuperación en caso de catástrofe

Finalidad: Actuar de asesor fiable en materia de continuidad de las actividades y recuperación en caso de catástrofe mediante el asesoramiento imparcial y empírico, teniendo en cuenta el contexto en el que se puede utilizar el asesoramiento y las limitaciones de recursos aplicables.

Descripción: Ayudar a los mandantes en las actividades relacionadas con la capacidad de recuperación de la organización, habida cuenta de los riesgos identificados.

Resultado: Los mandantes pueden aplicar adecuadamente planes de continuidad de las actividades y de recuperación en caso de catástrofe que estén en consonancia con las estrategias de gestión de incidentes.

9.4.3 Función: Ayuda en materia de políticas

Finalidad: Actuar de asesor fiable en la elaboración y aplicación de políticas mediante asesoramiento imparcial y empírico, teniendo en cuenta el contexto en el que se puede utilizar el asesoramiento y las limitaciones de recursos aplicables.

Descripción: Esta función ayuda a los mandantes en la elaboración, mantenimiento, institucionalización y observancia de políticas, garantizando a su vez que permitan y apoyen las actividades de gestión de incidentes. En el caso de los EIISI internos, normalmente comprende el apoyo a la seguridad de la información y otras políticas operativas. En el caso de los EIISI de coordinación y nacionales, podría abarcar el apoyo a las políticas públicas y a la nueva legislación.

Resultado: Los mandantes pueden desarrollar políticas eficaces, institucionalizar políticas y permitir estrategias efectivas de gestión de incidentes.

9.4.4 Función: Asesoramiento técnico

Finalidad: Proporcionar asesoramiento técnico que pueda ayudar a los mandantes a gestionar mejor los riesgos y amenazas y aplicar las prácticas idóneas operativas y de seguridad vigentes, permitiendo a su vez realizar actividades eficaces de gestión de incidentes.

Descripción: Esta función proporciona ayuda y recomendaciones para la mejora de las infraestructuras, herramientas y servicios relacionados con la ciberseguridad para los mandantes, con el objetivo de mejorar la postura de seguridad y la gestión de incidentes en general.

El asesoramiento puede guardar relación con:

- consideraciones de seguridad para la adquisición, verificación del cumplimiento, mantenimiento y actualizaciones;

- auditorías internas y externas de infraestructuras y herramientas relacionadas con la ciberseguridad;
- requisitos de desarrollo de *software* seguro y codificación segura.

Resultado: Se proporciona apoyo para diseñar, adquirir, gestionar, operar y mantener la infraestructura y los sistemas y herramientas de los mandantes, así como para ayudar en la capacitación, formación y consolidación de las actividades de gestión de incidentes.

Anexo 1: Agradecimientos

Los siguientes voluntarios de las comunidades de EIISI han contribuido considerablemente a esta versión del marco de servicios del EIISI. La lista está en orden alfabético por apellido, sin título pero con afiliación, función y país:

- Vilius Benetis, NRD CIRT (LT)
- Olivier Caleff (Service Area Coordinator), openEIISI Foundation (FR)
- Cristine Hoepers (Service Area Coordinator), CERT.br (BR)
- Angela Horneman, CERT/CC, SEI, CMU (US)
- Allen Householder, CERT/CC, SEI, CMU (US)
- Klaus-Peter Kossakowski (Editor), Hamburg University of Applied Sciences (DE)
- Art Manion, CERT/CC, SEI, CMU (US)
- Amanda Mullens (Co-Service Area Coordinator), CISCO (US)
- Samuel Perl (Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Daniel Roethlisberger (Service Area Coordinator), Swisscom (CH)
- Sigitas Rokas, NRD CIRT (LT)
- Mary Rossell, Intel (US)
- Robin M. Ruefle (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)
- Mark Zajicek (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)

Anexo 2: Términos y definiciones

En esta sección se definen ciertos términos utilizados en el marco de servicios del EIISI.

- **Acción** – Descripción de cómo se hace algo con distintos niveles de detalle.
- **Aviso**[9] – Anuncio o boletín que informa, asesora y alerta acerca de la vulnerabilidad de un producto.
- **Capacidad** – Actividad cuantificable que se efectúa en el marco de las funciones y responsabilidades de una organización. A los efectos del marco de servicios de FIRST, las capacidades pueden definirse como los servicios más amplios o como las funciones necesarias.
- **Volumen de capacidad** – Número de veces que una organización puede ejecutar una determinada capacidad antes de agotar los recursos de algún modo.
- **Riesgo de vulnerabilidades comunes (CVE)**[10] – Lista de registros que contiene el número de identificación, la descripción y al menos una referencia pública para las vulnerabilidades conocidas públicamente. Sirve de identificador normalizado para referirse a las vulnerabilidades.
- **Sistema de puntuación de vulnerabilidad comunes (CVSS)**[11] – Valor numérico que indica la gravedad de la vulnerabilidad.
- **Enumeración de puntos débiles comunes (CWE)**[12] – Lista formal de tipos de puntos débiles del *software* creada para servir de lenguaje común que describe los puntos débiles de la seguridad del *software* en la arquitectura, el diseño o el código; servir de criterio de medición normalizado para las herramientas de seguridad del *software* que se ocupan de estos puntos débiles; y proporcionar una norma de referencia común para la identificación de los puntos débiles, su mitigación y las actividades de prevención.
- **Mandantes** – Grupo concreto de personas y/u organizaciones que tienen acceso a un conjunto de servicios específicos que ofrece el EIISI.
- **Fuente de datos contextuales** – Fuente de datos que da el contexto a ciertos datos concretos, por ejemplo, la identidad, un activo o un evento de seguridad de la información. Entre los ejemplos concretos figuran las bases de datos de usuarios, los inventarios de activos, los servicios de repudio IP o los datos de inteligencia sobre amenazas.
- **Divulgación coordinada de vulnerabilidades** – Término utilizado para designar un proceso de divulgación de manera coordinada. Fuente: ISO/CEI 29147:2018, Términos y definiciones.

---

[9] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.1

[10] https://cve.mitre.org/

[11] https://www.first.org/cvss/

[12] https://cwe.mitre.org/about/index.html

- **Coordinador**[13] – Participante facultativo que puede ayudar a proveedores e inspectores a gestionar y divulgar vulnerabilidades.
- **Casos de detección** – Estado específico que debe ser detectado por el ámbito de servicio gestión de eventos de seguridad de la información. Si bien el término procede de la ingeniería de *software*, ahora se utiliza ampliamente en la ingeniería de detección.
- **Embargo** – Restricción a la publicación de los detalles sobre vulnerabilidades hasta que los proveedores afectados puedan facilitar las actualizaciones de seguridad o las medidas de mitigación y soluciones temporales para proteger a los clientes.
- **Inspector**[14] – Persona u organización que detecta una posible vulnerabilidad en un producto o servicio en línea. Tenga en cuenta que los inspectores pueden ser investigadores, periodistas, compañías de seguridad, piratas informáticos, usuarios, gobiernos o coordinadores.
- **Función** – Actividad o conjunto de actividades destinadas a desempeñar un determinado servicio. Otras definiciones son grupo de acciones conexas[15]; realizar una determinada acción o actividad, trabajar, explotar.[16]
- **Evento de seguridad de la información** – Evento observable en el entorno de TI que atañe a la seguridad; por ejemplo, el inicio de sesión de un usuario o una alerta IDS. Los eventos de seguridad de la información suelen producir algún tipo de prueba, como un registro de auditoría o la inscripción en un archivo de registro, que se puede recopilar y analizar en el marco del ámbito de servicio gestión de eventos de seguridad de la información.
- **Incidente de seguridad de la información**[17] – Cualquier evento (o conjunto de eventos) adverso de seguridad de la información que indique un peligro para algún aspecto de la seguridad de la información del usuario, el sistema, la organización y/o la red. La definición de incidente de seguridad de la información puede variar entre las organizaciones, pero las siguientes categorías son generalmente aplicables:
  - pérdida de la confidencialidad de la información;
  - compromiso de la integridad de la información;
  - denegación de servicio;
  - uso indebido de servicios, sistemas o información;
  - daños en los sistemas.

Los ataques, aunque hayan fallado gracias a una protección adecuada, pueden considerarse como un incidente de seguridad de la información.

---

[13] ISO/CEI 30111:2013 Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.1

[14] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.3

[15] Fuente: https://www.merriam-webster.com/dictionary/function

[16] Fuente: https://www.dictionary.com/browse/function

[17] Según la RFC2350 considerando "seguridad de la información" en lugar de "seguridad TI", https://tools.ietf.org/html/rfc2350

- **Indicador fundamental de rendimiento (IFR)**[18] – Valor cuantificable que indica la eficacia con la que una empresa está logrando los principales objetivos empresariales. Las organizaciones utilizan los indicadores fundamentales de rendimiento en múltiples niveles para evaluar la consecución de sus objetivos.
- **Madurez** – Grado de eficacia con el que una organización ejecuta una capacidad particular con arreglo a su cometido y potestades. Constituye el nivel de competencias adquiridas en acciones o tareas, o en un conjunto de funciones o servicios. La capacidad de una organización estará determinada por el alcance y la calidad de las políticas y la documentación establecidas y la capacidad de ejecutar un proceso determinado.
- **Código abierto** – Obras cuya licencia se otorga para que puedan ser redistribuidas y modificadas libremente, y cuyo código fuente se pone a disposición pública, se distribuye gratuitamente y no discrimina a ninguna persona, grupo o campo de actividad, y además es tecnológicamente neutro. El mantenimiento del *software* de código abierto suele estar a cargo de una comunidad de personas y entidades que colaboran en su creación y mantenimiento.
- **Producto**[19] – Sistema implementado o desarrollado para la venta o que se ofrece gratuitamente.
- **Reparación (o remedio)**[20] – Modificación aportada a un producto o servicio en línea para eliminar o mitigar una vulnerabilidad. La reparación suele consistir en sustituir un archivo binario, cambiar la configuración o parchear y recompilar el código fuente. Para designar una "reparación" se utilizan diversos términos como parche, remedio, actualización, corrección dinámica y actualización. Las mitigaciones también se denominan soluciones provisionales o contramedidas.
- **Divulgación responsable** – Término que se utiliza para referirse a un proceso o modelo en el que una vulnerabilidad no se divulga hasta que no haya transcurrido un periodo de tiempo que permita disponer de una reparación (remedio o parche). No significa necesariamente lo mismo que "divulgación coordinada de vulnerabilidades".
- **Riesgo**[21] – "Efecto de la incertidumbre en los objetivos". En esta definición, por incertidumbre se entiende los eventos (que pueden ocurrir o no) y las incertidumbres causadas por ambigüedad o falta de información.
- **Asunción de riesgos**[22] – Estrategia de respuesta a riesgos que consiste en que el equipo del proyecto decide reconocer el riesgo y no tomar medida alguna hasta que éste ocurra.
- **Registro de riesgos**[23] – Documento en el que se consignan los resultados del análisis de riesgos y de la planificación de respuestas a riesgos.

[18] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator

[19] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.5

[20] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.6

[21] ISO 31000:2009/ISO Guide 73:2002 Risk management – Principles and guidelines – Terms/Definitions 2.1

[22] The Project Management Body of Knowledge (PMBOK) Guide and Standards

[23] The Project Management Body of Knowledge (PMBOK) Guide and Standards

- **Servicio** – Conjunto de funciones reconocibles y coherentes para obtener un resultado específico. Los mandantes, o en su nombre u otros interesados, pueden esperar o exigir que se le ofrezcan estos servicios.
- **Acuerdo de nivel de servicio (SLA)** – Contrato entre el proveedor de servicios (interno o externo) y el usuario final en el que se define el nivel de servicio que cabe esperar del proveedor de servicios.
- **Interesados**[24] – Personas o grupos que definen y modifican los ámbitos de servicio o los servicios y garantizan una estrategia adecuada de comunicación del servicio, y los grupos que pueden beneficiarse de los servicios ofrecidos.
- **Tareas** – Lista de actividades que deben realizarse para llevar a buen término una determinada función.
- **Proveedor**[25] – Persona u organización que desarrolla el producto o servicio o que es responsable de su mantenimiento.
- **Vulnerabilidad**[26] – Punto débil en el *software*, *hardware* o en un servicio en línea que puede explotarse.

[24] Architecture Content Framework

[25] ISO/CEI 30111:2013 Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.7

[26] ISO/CEI 30111:2013 Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.8

Anexo 3: Recursos disponibles

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001.
https://apps.dtic.mil/docs/citations/ADA395859

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8_1
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_1

Boyd, John R. Destruction and Creation. Goal Systems International. September 3, 1976.
http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005.
https://www.hsdl.org/?view&did=685398

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website.* June 23, 2019 [accessed].
https://www.cnss.gov/cnss/

Cybersecurity Situation Awareness. *The MITRE Corporation Website.* June 25, 2019 [accessed].
https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.
https://journals.sagepub.com/doi/10.1518/001872095779049543

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018
https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015
https://www.first.org/global/sigs/vrdx/

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk.* June 11, 2015.
https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014.
https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability disclosure.* Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018
https://www.iso.org/standard/72311.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013
https://www.iso.org/standard/53231.html

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/book/10.1007/978-1-4419-0140-8

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000.
http://www.ti.terena.nl/process/ti-v2.pdf

Manion, Art & Householder, Alan. *Vulnerability Analysis.* CERT Coordination Center (CERT/CC). May 30, 2019.
https://vuls.cert.org/

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium*. Savannah, Georgia, October 2000.

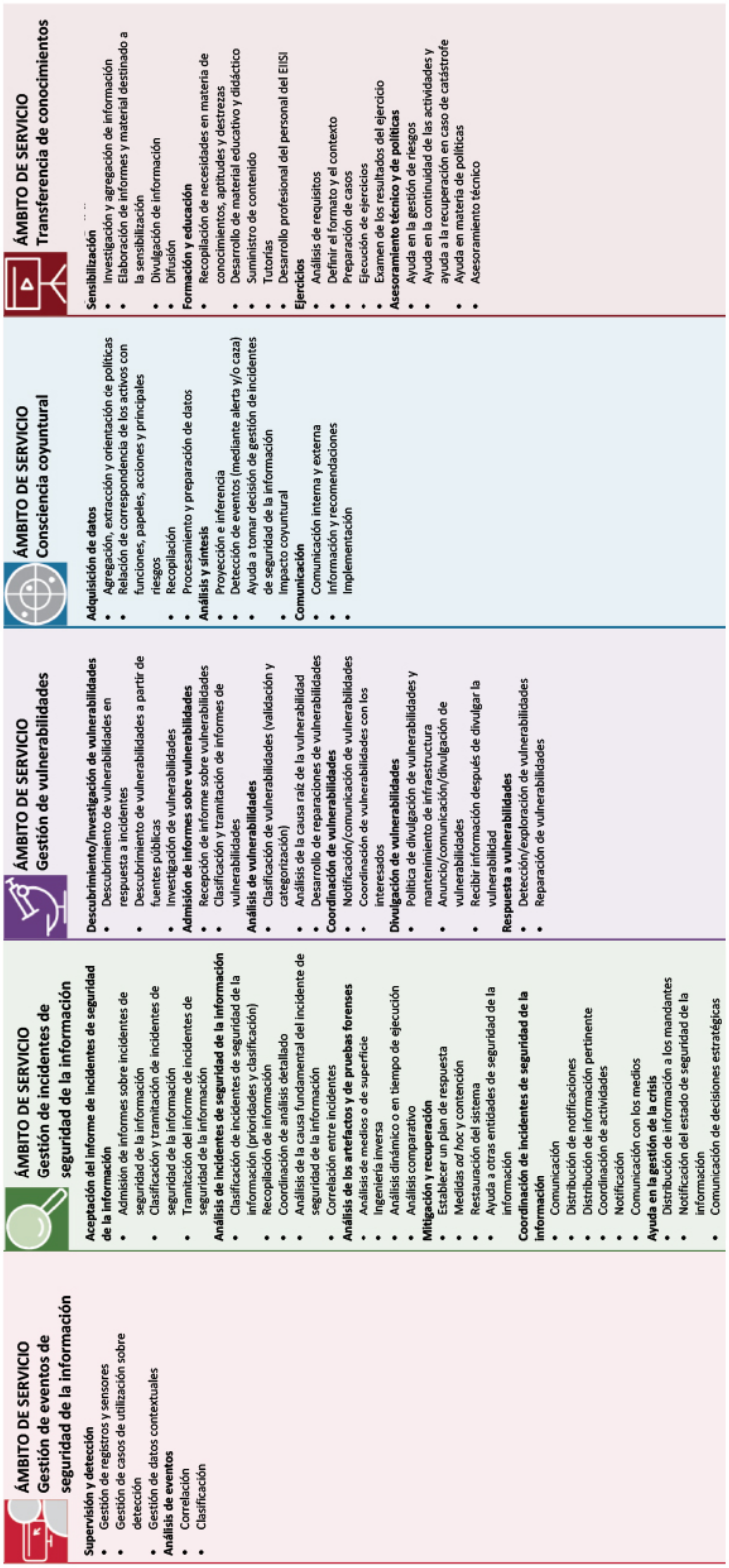
Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005.
https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1

Stone, Steve. Data to Decisions for Cyberspace Operations. *The MITRE Corporation Website*. January 2016
https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. 2010. ISBN 978-1-4419-0140-8
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_2

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

Anexo 4: Descripción general de todos los servicios EIISI y funciones conexas



ÁMBITO DE SERVICIO
Gestión de eventos de seguridad de la información

Supervisión y detección
- Gestión de registros y sensores
- Gestión de casos de utilización sobre detección
- Gestión de datos contextuales

Análisis de eventos
- Correlación
- Clasificación

ÁMBITO DE SERVICIO
Gestión de incidentes de seguridad de la información

Aceptación del informe de incidentes de seguridad de la información
- Admisión de informes sobre incidentes de seguridad de la información
- Clasificación y tramitación de incidentes de seguridad de la información
- Tramitación del informe de incidentes de seguridad de la información

Análisis de incidentes de seguridad de la información
- Clasificación de incidentes de seguridad de la información (prioridades y clasificación)
- Recopilación de información
- Coordinación de análisis detallado
- Análisis de la causa fundamental del incidente de seguridad de la información
- Correlación entre incidentes

Análisis de los artefactos y de pruebas forenses
- Análisis de medios o de superficie
- Ingeniería inversa
- Análisis dinámico o en tiempo de ejecución
- Análisis comparativo

Mitigación y recuperación
- Establecer un plan de respuesta
- Medidas *ad hoc* y contención
- Restauración del sistema
- Ayuda a otras entidades de seguridad de la información

Coordinación de incidentes de seguridad de la información
- Comunicación
- Distribución de notificaciones
- Distribución de información pertinente
- Coordinación de actividades
- Notificación
- Comunicación con los medios

Ayuda en la gestión de la crisis
- Distribución de información a los mandantes
- Notificación del estado de seguridad de la información
- Comunicación de decisiones estratégicas

ÁMBITO DE SERVICIO
Gestión de vulnerabilidades

Descubrimiento/investigación de vulnerabilidades
- Descubrimiento de vulnerabilidades en respuesta a incidentes
- Descubrimiento de vulnerabilidades a partir de fuentes públicas
- Investigación de vulnerabilidades

Admisión de informes sobre vulnerabilidades
- Recepción de informe sobre vulnerabilidades
- Clasificación y tramitación de informes de vulnerabilidades

Análisis de vulnerabilidades
- Clasificación de vulnerabilidades (validación y categorización)
- Análisis de la causa raíz de la vulnerabilidad
- Desarrollo de reparaciones de vulnerabilidades

Coordinación de vulnerabilidades
- Notificación/comunicación de vulnerabilidades
- Coordinación de vulnerabilidades con los interesados

Divulgación de vulnerabilidades
- Política de divulgación de vulnerabilidades y mantenimiento de infraestructura
- Anuncio/comunicación/divulgación de vulnerabilidades
- Recibir información después de divulgar la vulnerabilidad

Respuesta a vulnerabilidades
- Detección/exploración de vulnerabilidades
- Reparación de vulnerabilidades

ÁMBITO DE SERVICIO
Consciencia coyuntural

Adquisición de datos
- Agregación, extracción y orientación de políticas
- Relación de correspondencia de los activos con funciones, papeles, acciones y principales riesgos
- Recopilación
- Procesamiento y preparación de datos

Análisis y síntesis
- Proyección e inferencia
- Detección de eventos (mediante alerta y/o caza)
- Ayuda a tomar decisión de gestión de incidentes de seguridad de la información
- Impacto coyuntural

Comunicación
- Comunicación interna y externa
- Información y recomendaciones
- Implementación

ÁMBITO DE SERVICIO
Transferencia de conocimientos

Sensibilización
- Investigación y agregación de información
- Elaboración de informes y material destinado a la sensibilización
- Divulgación de información
- Difusión

Formación y educación
- Recopilación de necesidades en materia de conocimientos, aptitudes y destrezas
- Desarrollo de material educativo y didáctico
- Suministro de contenido
- Tutorías
- Desarrollo profesional del personal del EIISI

Ejercicios
- Análisis de requisitos
- Definir el formato y el contexto
- Preparación de casos
- Ejecución de ejercicios
- Examen de los resultados del ejercicio

Asesoramiento técnico y de políticas
- Ayuda en la gestión de riesgos
- Ayuda en la continuidad de las actividades y ayuda a la recuperación en caso de catástrofe
- Ayuda en materia de políticas
- Asesoramiento técnico