Spring 2020

Marco de servicios del equipo de intervención en caso de incidentes de seguridad de productos (EIISP)

Versión 1.1

Aviso: En este documento se describen las prácticas que el Foro sobre los equipos de seguridad e intervención en caso de incidente (FIRST.Org) considera idóneas. Estas descripciones son meramente informativas. FIRST.Org no podrá considerarse responsable de los eventuales daños resultantes de la utilización de esta información o relacionados con ella.

Marco de servicios EIISP

Objetivo

Los *Marcos de servicios* son documentos de alto nivel en los que se detallan los servicios que pueden prestar los equipos de intervención en caso de incidentes de seguridad informática (EIISI) y los equipos de intervención en caso de incidentes de seguridad de los productos (EIISP). Estos documentos son obra de expertos reconocidos de la comunidad FIRST. FIRST procura integrar la información recibida de todos los sectores, incluidos los EIISI con responsabilidad nacional, los EIISI y EIISP del sector privado y otros interesados. El objetivo de estos documentos es servir de base para la preparación de nuevo material de formación. Sin embargo, hoy en día se utilizan de manera mucho más amplia, por ejemplo, a la hora de definir el catálogo de servicios inicial de los nuevos equipos.

Al preparar el Marco de servicios EIISI quedó claro que los EIISP ofrecen servicios muy diferentes y suelen intervenir en entornos muy distintos. Se decidió, por tanto, preparar un documento independiente para los EIISP. Estos dos documentos estarán armonizados, subrayando las muchas semejanzas entre ellos. La preparación de los marcos está dirigida por la *Education Advisory Board*.

Los Marcos están destinados a ayudar a las organizaciones a crear, mantener y aumentar las capacidades de sus EIISI o EIISP. Se trata de guías en las que se identifican los diversos modelos, capacidades, servicios y resultados. En este sentido, los equipos son libres de utilizar su propio modelo y de dotarse de las capacidades que responden a las necesidades de sus interesados. Los Marcos son de ayuda a los equipos de intervención en caso de incidentes de seguridad (EIIS) al identificar las responsabilidades primarias y dar orientaciones sobre cómo crear las capacidades acordes a esas responsabilidades, además de facilitar información sobre cómo los equipos pueden aportar y transferir valor a sus organizaciones en términos generales.

Introducción

Un equipo de intervención en caso de incidentes de seguridad de los productos (EIISP) es una entidad dentro de una organización que se dedica principalmente a la identificación, la evaluación y la eliminación de los riesgos provocados por las vulnerabilidades de seguridad de los productos, incluidas las ofertas, soluciones, componentes y/o servicios que la organización produce y/o vende.

Un EIISP adecuadamente configurado no es un grupo operativo independiente, desconectado de la elaboración de los productos de la organización, sino que forma parte de la iniciativa de ingeniería de la seguridad más amplia de la organización. Gracias a esta estructura se garantiza la integración de las actividades relacionadas con la seguridad en el ciclo de producción seguro (CPS).

Los equipos de intervención en caso de incidentes de seguridad de los productos suelen asociarse con la fase de mantenimiento del CPS, pues la mayoría de las vulnerabilidades de

seguridad de los productos se conocen cuando falla la calidad tras la comercialización de los productos. Sin embargo, los EIISP pueden ejercer también su influencia en las fases de arquitectura, diseño, planificación y modelización de riesgos. Los EIISP pueden también revelar su valor al orientar y supervisar el tratamiento de los problemas de seguridad internos.

Estructura del Marco de los EIISP

ESFERAS DE SERVICIO – SERVICIOS – FUNCIONES – SUBFUNCIONES

ESFERAS DE SERVICIO

Las esferas de servicio agrupan los servicios relativos a un aspecto común. Ayudan a organizar los servicios en una clasificación general para facilitar su comprensión. La especificación de cada esfera de servicio contendrá un campo "descripción" consistente en un texto general que describe la esfera de servicio en cuestión y la lista de servicios correspondiente.

SERVICIOS

Un servicio es un conjunto de acciones coherentes y reconocibles encaminadas a un resultado determinado para los mandantes de un equipo de intervención en caso de incidentes, o en su nombre.

La especificación de un servicio contendrá los siguientes campos:

- un campo "descripción" en el que se describe la naturaleza del servicio;
- un campo "objetivo y resultado" que describe la finalidad y los resultados mensurables del servicio.

FUNCIONES

Una función es una actividad o conjunto de actividades destinadas a cumplir el propósito de un servicio concreto. Varios servicios podrán utilizar o compartir una misma función.

La especificación de una función contendrá los siguientes campos:

- un campo "descripción" en el que se describe la función;
- un campo "objetivo y resultado" que describe la finalidad y los resultados mensurables del servicio;
- la lista de subfunciones que pueden ejercerse como parte de la función.

SUBFUNCIONES

Una subfunción es una actividad o conjunto de actividades destinadas a cumplir el propósito de una función concreta. Varias funciones podrán utilizar o compartir una misma subfunción.

Diferencias entre EIISP y EIISI

La dedicación a los productos es la principal diferencia entre los EIISP de una organización y los demás equipos de intervención en caso de incidentes, como los EIISI, de esa misma organización. Por norma general, los EIISI empresariales se centran en la seguridad de los sistemas y/o redes informáticos que forman la infraestructura de una organización.

Aunque hay grandes diferencias entre un EIISI empresarial y un EIISP, hay que reconocer que también hay sinergias entre ambos grupos. Lo que hay que tener presente es que los EIISP no funcionan con independencia de las demás partes de la organización. A lo largo de este marco se resaltarán las esferas de colaboración y sinergia que se deben fomentar.

Estructura orgánica del EIISP

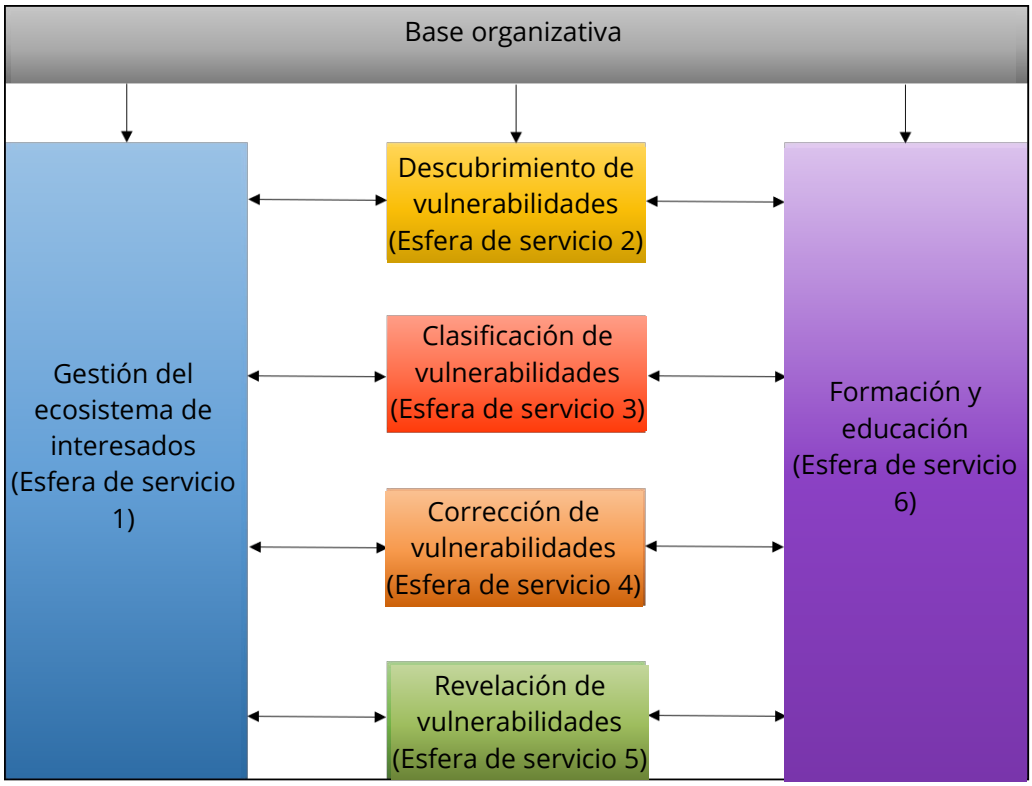


Figura 1: Estructura orgánica

Los EIISP pueden ser tan exclusivos y variados como los productos que ayudan a proteger. Entre las organizaciones dentro de un mismo sector o industria habrá diferencias en términos de características empresariales, modelos operativos, carteras de productos, estructuras organizativas y estrategias de desarrollo de los productos. Por consiguiente, no hay una estrategia o modelo de equipo de intervención en caso de incidentes de seguridad de los productos que se adapte a todas las organizaciones. Sin embargo, la mayoría de empresas recurre a uno de los siguientes tres modelos de EIISP: distribuido, centralizado e híbrido.

Modelo distribuido

El modelo distribuido consiste en un pequeño EIISP núcleo que trabaja con representantes de los equipos de producción para solucionar las vulnerabilidades de seguridad de los productos. Según este modelo, los EIISP reducidos operativos asumen diversas responsabilidades:

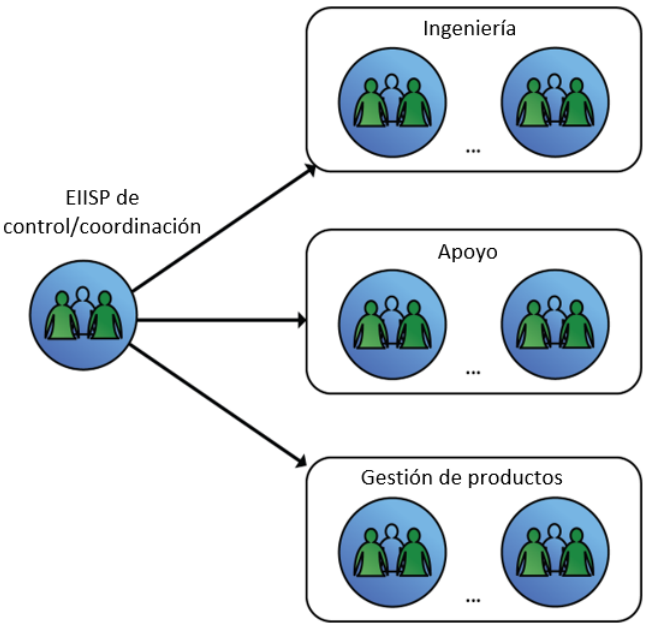


Figura 2: Modelo distribuido

- Crear políticas, procedimientos y directrices para la clasificación, el análisis, la corrección y la comunicación de reparaciones, mitigaciones y consejos para resolver las vulnerabilidades de seguridad.
- Definir una matriz (desglosada) de representantes de ingeniería de la seguridad de los productos de toda la organización.
- Servir de líder y guía en la intervención en caso de vulnerabilidad de la seguridad de los productos y de posible riesgo para la empresa.
- Servir de centro de recepción de las vulnerabilidades de seguridad. La centralización del control crea economías de escala.
- Notificar al propietario/gestor de los productos y al ingeniero de seguridad las nuevas vulnerabilidades de seguridad, ayudar a crear planes correctivos, preparar/publicar comunicaciones de reparaciones o mitigaciones, incluida la gestión de incidentes.

Para una organización con una cartera de productos amplia y diversa puede resultar beneficioso el modelo distribuido, porque el coste del EIISP se diluye a lo largo y ancho de la organización. Con este modelo el EIISP también puede aprovechar las competencias del personal de los equipos de ingeniería de productos.

El problema del modelo EIISP distribuido es que las personas encargadas de la clasificación y facilitación de reparaciones de las vulnerabilidades de seguridad no están directamente controladas por el EIISP de operaciones, ni deben rendirle cuentas.

Modelo centralizado

En el modelo centralizado hay un EIISP más amplio formado por personal de múltiples departamentos que rinde cuentas a uno o más directivos responsables de la seguridad de los productos de la organización. La estructura con este modelo podría ser la siguiente:

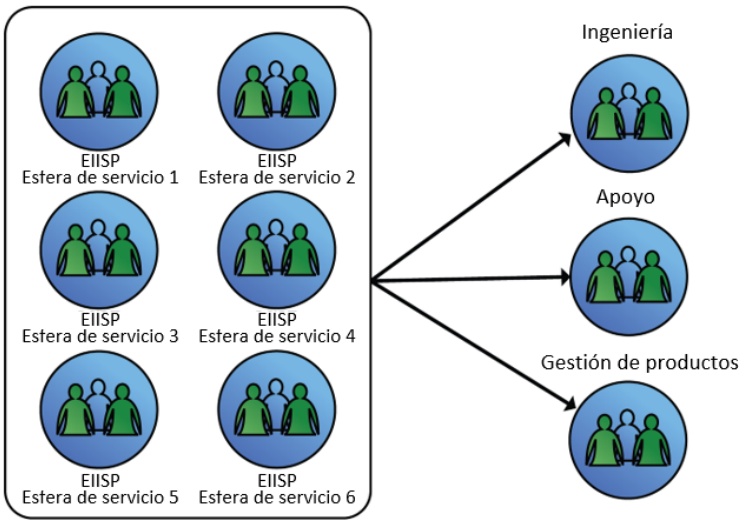


Figura 3: Modelo centralizado

- *Departamento de gestión de programas del EIISP*: crea políticas, procesos y directrices para la clasificación, el análisis, la corrección y la comunicación de reparaciones de vulnerabilidades de seguridad. Gestiona las operaciones del EIISP en general, así como el sistema de partes de incidencia, y representa al EIISP en la organización.
- *Clasificación e información de seguridad del EIISP*: supervisa en diversas fuentes externas las vulnerabilidades de seguridad. Evalúa las consecuencias iniciales de las vulnerabilidades de seguridad para la cartera de productos de la organización.
- *Corrección y comunicaciones del EIISP*: facilita directamente los códigos de reparación de las vulnerabilidades a los equipos de ingeniería de productos.

Este modelo se adapta bien a organizaciones más pequeñas y/o con una cartera de productos homogénea. Este modelo concentra y cultiva un alto nivel de competencias y conocimientos de seguridad en un sector de la organización. El problema de este modelo es el coste que implica el mantenimiento de un equipo especializado centralizado que no es fácil de adaptar si crece y/o se diversifica la cartera de productos.

Modelo híbrido

El modelo híbrido es una variante que aúna características de los modelos centralizado y distribuido. Toda organización que opte por combinar las características y funcionalidades de ambos modelos y crear un híbrido deberá tener en cuenta los siguientes factores:

- estructura y tamaño de la organización;
- tamaño y diversidad de la cartera de productos;

- estrategia de desarrollo de los productos.

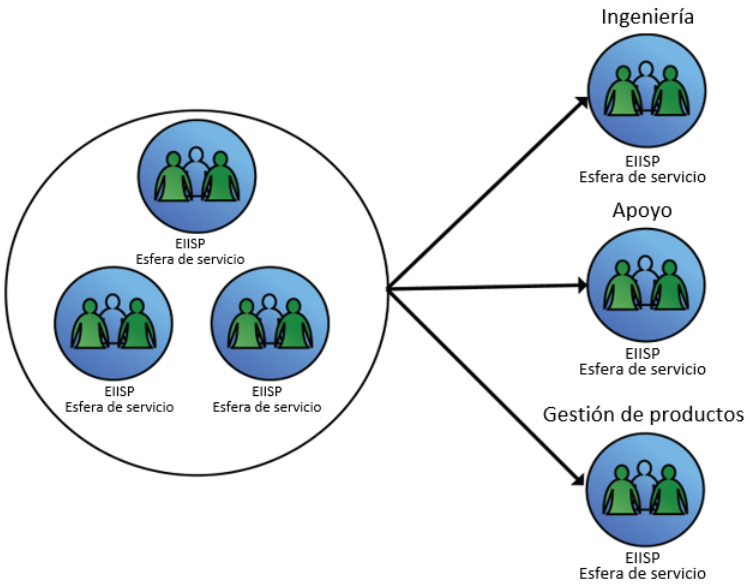


Figura 4: Modelo híbrido

Otras consideraciones

Es importante que un EIISP tenga la autonomía suficiente para conservar una posición independiente y objetiva con respecto a las vulnerabilidades de seguridad de los productos de la organización. Así, al elaborar la estrategia y estructura del EIISP de la organización, ésta debe considerar la mejor manera de integrarlo en la organización y su jerarquía. Es importante que el EIISP rinda cuentas a un directivo de la empresa que confirme su autoridad.

A medida que el EIISP madure, crezca y evolucione su misión, podrá modificarse su composición o jerarquía. El factor determinante de la modificación y madurez de un EIISP serán sus principales interesados y, por desgracia, las consecuencias de las vulnerabilidades graves en un amplio espectro de la base de interesados de la organización. Los interesados suelen estar definidos por el modelo adoptado por la organización, así como por su tamaño.

Interesados

Tener en cuenta las necesidades y requisitos de los interesados es una parte fundamental de la definición de la estrategia y estructura del EIISP. El modelo adoptado por una organización para su EIISP puede definir la identidad de los interesados y la influencia que tienen.

Es fundamental mantener relaciones positivas de manera constante. En la *Esfera de servicio 1: Gestión del ecosistema de interesados* pueden consultarse más detalles acerca del ecosistema de interesados y su gestión.

Un último elemento que hay que tener en cuenta a la hora de formar el equipo de intervención en caso de incidentes de productos y definir su estrategia son los influentes, que se distinguen de los interesados en que éstos son personas particulares o grupos de personas, mientras que los influentes son las normas industriales y gubernamentales, la legislación, la reglamentación y

las tendencias. Los influentes pueden imponer mayores requisitos en relación a la formación, las estrategias, las políticas y las características operativas de los EIISP que los interesados.

¿Qué hace un EIISP?

El modelo utilizado definirá el alcance y las actividades operativas del EIISP, pero no necesariamente modificará las medidas que la organización deberá adoptar para resolver las vulnerabilidades de seguridad de sus productos. El modelo define el alcance de las capacidades, acciones y responsabilidades directamente asignadas al EIISP más que las distribuidas en la organización en su conjunto.

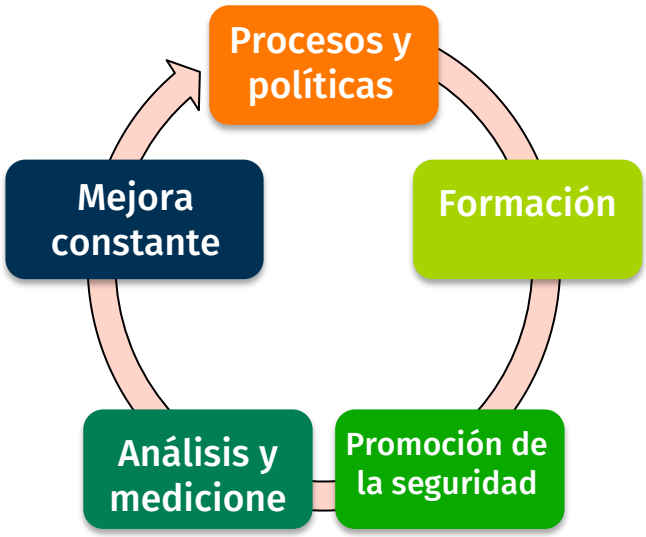


Figura 5: Actividades generales del EIISP

Desarrollo constante de procesos y políticas

Los EIISP definen las políticas de la organización en materia de seguridad de los productos. Las necesidades comerciales determinan y dictan los requisitos del EIISP y no al contrario. Antes de poder aplicar las políticas del EIISP, éstas han de revisarse y recibir el respaldo de la dirección de la organización. Las políticas aprobadas deben aplicarse con procedimientos claros cuyo cumplimiento garantiza la adhesión de la organización a esas políticas.

Formación de los interesados

Además de las políticas y procedimientos, los EIISP deben crear sistemas de gestión y encauzamiento del trabajo que racionalicen la ejecución y compleción de las acciones necesarias para resolver las vulnerabilidades de seguridad de los productos. Esto facilitará que la organización adopte la seguridad de los productos como parte de sus actividades empresariales cotidianas.

A la hora de poner en pie la misión, las políticas y los procedimientos de los EIISP el mayor error sería considerarlos como un requisito o responsabilidad independiente. Por consiguiente, es

fundamental formar a todos los miembros de la organización para que conozcan las nociones básicas de seguridad de los productos y el papel que desempeñan. La organización en su integridad debe ajustarse a los requisitos políticos del EIISP y contar con los conocimientos y herramientas necesarios para ello.

La importancia de la medición

Es esencial medir el éxito de la intervención en caso de incidentes de seguridad de los productos. La medición no define los requisitos, sino que sustenta el programa, ayuda a determinar los recursos necesarios y puede ayudar a identificar las mejoras procesales/instrumentales necesarias. La definición de mediciones y su seguimiento puede también contribuir a la madurez del EIISP descubriendo problemas o puntos de congestión en su despliegue y adopción. En *Servicio 1.7 Datos para los interesados* y *Servicio 5.4 Datos sobre vulnerabilidades* puede encontrarse más información sobre los tipos de mediciones que convendría realizar.

Definiciones

A continuación se definen ciertos términos utilizados en el presente documento. Las esferas de servicios, los servicios y las funciones definen *lo que* se hace a diferentes niveles de detalle, y las tareas y acciones definen *cómo* se hace, también a diferentes niveles de detalle. Las tareas y acciones se publican en un documento adjunto que puede actualizarse, y se actualizará, con mayor frecuencia:

- **Aviso**[1] – Anuncio o boletín que informa, asesora y alerta acerca de la vulnerabilidad de un producto.
- **Barra de errores** – Criterios que definen el tipo de errores que se consideran vulnerabilidades de seguridad. Los errores que se ajustan a estos criterios se tratarán como una vulnerabilidad utilizando los procedimientos operativos normalizados del EIISP.
- **Coordinador**[2] – Participante opcional que puede ayudar a los fabricantes y buscadores a tratar y revelar información sobre vulnerabilidades.
- **Embargo** – Detención de la publicación de los detalles de una vulnerabilidad hasta que los fabricantes afectados puedan facilitar las actualizaciones de seguridad o las medidas correctivas o alternativas necesarias para proteger a los clientes.
- **Buscador**[3] – Persona u organización que identifica una posible vulnerabilidad de un producto o servicio en línea. Los buscadores pueden ser investigadores, periodistas, empresas de seguridad, piratas, usuarios, gobiernos o coordinadores.
- **Código abierto** – Se refiere a las obras cuya licencia permite su libre distribución y modificación, cuyo código fuente está públicamente disponible, se distribuye gratuitamente y no discrimina a persona, grupo o materia alguna, y es tecnológicamente neutro. El

[1] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.1
[2] ISO/CEI 30111:2013 Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.1
[3] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.3

mantenimiento de un *software* de código abierto suele ser responsabilidad de la comunidad de personas o entidades que colaboraron en su creación y mantenimiento.

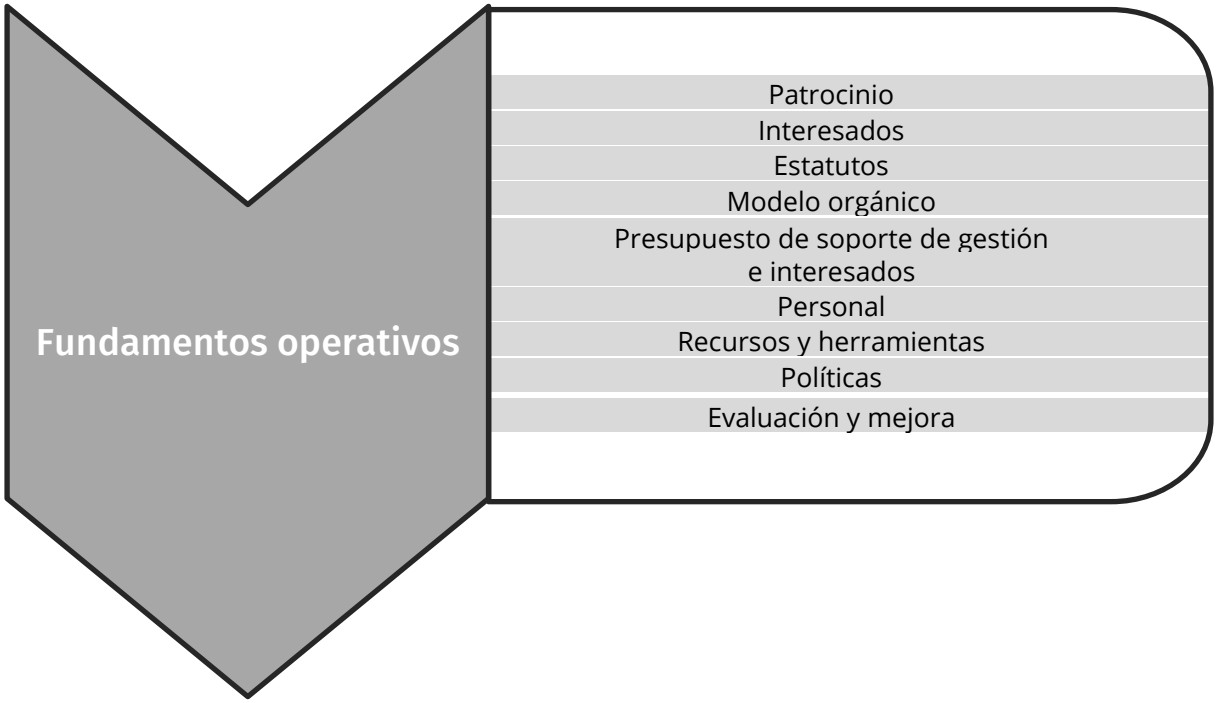
- **Socios** – Fabricantes de equipos originales (OEM), proveedores, fabricantes de diseños originales (ODM).
- **Producto**[4] – Sistema creado o implementado para su venta u oferta gratuita.
- **Umbral de calidad** – Conjunto de criterios que se han de cumplir antes de que un producto pase a la siguiente fase de desarrollo o comercialización.
- **Reparación (o remedio)**[5] – Modificación aportada a un producto o servicio en línea para suprimir o mitigar una vulnerabilidad. Una reparación suele adoptar la forma de una sustitución de fichero binario, un cambio de configuración o un parche y recopilación de código fuente. Para designar una reparación se utilizan diversos términos como parche, arreglo, actualización, parche en caliente y mejora. Las mitigaciones también se denominan alternativas o contramedidas.
- **Riesgo**[6] – "Efecto de la incertidumbre en los objetivos". En esta definición, por incertidumbre se entienden los eventos (que pueden ocurrir o no) y las incertidumbres causadas por ambigüedad o falta de información.
- **Aceptación de riesgos**[7] – Estrategia de respuesta que consiste en que el equipo de proyecto decide reconocer el riesgo y no tomar medidas hasta que éste ocurra.
- **Registro de riesgos**[8] – Documento en el que se registran los resultados del análisis de riesgos y la planificación de respuesta a los riesgos.
- **Ciclo de producción seguro (CPS)** – Proceso de producción que ayuda a los creadores a producir productos más seguros y respetar los requisitos de seguridad, reduciendo al mismo tiempo los costes de producción.
- **Acuerdo de nivel de servicio (SLA)** – Contrato concluido entre el proveedor de servicios (interno o externo) y el usuario extremo que define el nivel de servicio que se espera del proveedor de servicios.
- **Interesados**[9] – Los interesados del EIISP son los grupos que crean y modifican el producto o los componentes del producto, que garantizan la estrategia de comunicación del producto adecuada, y los grupos en cuyo beneficio redunda la seguridad del producto. Dicho de otro modo, los interesados del EIISP contribuyen a la seguridad del producto y la intervención en caso de incidente o se benefician de ellas.
- **Tercero** – Todo proveedor o productor que aporta componentes integrados en un producto o solución/servicio.

[4] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.5
[5] ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure – Terms/Definitions 3.6
[6] ISO 31000:2009/ ISO Guide 73:2002 Risk management – Principles and guidelines – Terms/Definitions 2.1
[7] The Project Management Body of Knowledge (PMBOK) Guide and Standards
[8] The Project Management Body of Knowledge (PMBOK) Guide and Standards
[9] Architecture Content Framework

- **Fabricante**[10] – Persona u organización que crea el producto o servicio y es responsable de su mantenimiento.
- **Vulnerabilidad**[11] – Punto débil de un *software*, un *hardware* o un servicio en línea que puede explotarse.

[10] ISO/CEI 30111:2013 Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.7
[11] ISO/CEI 30111:2013 Information technology – Security techniques – Vulnerability handling processes – Terms/Definitions 3.8

Fundamentos operativos



En esta sección se identifican y describen los fundamentos de los componentes clave que una organización necesita para la adecuada planificación, creación y funcionamiento de un EIISP.

> ***Propósito**: Permitir a una organización planificar e implantar los componentes básicos para la creación y el funcionamiento de un EIISP.*
>
> ***Resultado**: La identificación, planificación e implantación de los componentes básicos operativos del EIISP ayuda a la organización a crear su EIISP y prepararlo para llevar a cabo su misión y ayudar a la empresa a facilitar sus productos y servicios a los interesados definidos.*

I Elementos estratégicos

A. Patrocinio ejecutivo

Obtener el patrocinio de la dirección de la organización y de las principales entidades decisorias.

> ***Propósito***
> *Informar a los directivos de la organización (por ejemplo, altos ejecutivos, junta de administración) u otras entidades decisorias, y obtener su acuerdo (adopción), para que el EIISP funcione adecuadamente.*
>
> ***Resultado***
> *Financiación y apoyo constantes sobre la base de la evaluación empresarial deseada.*

Para obtener el patrocinio ejecutivo la organización debe informar o formar a los ejecutivos y facilitarles un plan, u otro tipo de información, que les ayude a entender el objetivo, la

importancia y los beneficios que puede reportar el EIISP y los riesgos potenciales que plantean las vulnerabilidades de seguridad (véanse "Estatuto del EIISP" y "Presupuesto" *infra*).

Véase más información al respecto en *Servicio 1.1 Gestión de interesados internos*.

B. Interesados

Identificar a los interesados y la relación que el EIISP tendrá con esos grupos.

Propósito
Entender a quién servirá el EIISP y con quién interactuará.

Resultado
Lista de partes interesadas claramente definidas.

Deben incluirse los interesados externos, a saber, los clientes de la organización, los investigadores en seguridad externos, los EIISI y otros EIISP, así como los interesados internos, como los creadores de *software*, los ingenieros y los servicios jurídico, de atención al cliente y de relaciones públicas/institucionales/con los medios.

Véase más información al respecto en *Esfera de servicio 1 Gestión del ecosistema de interesados* (*Servicio 1.1 Gestión de interesados internos, Servicio 1.2 Implicación de la comunidad de buscadores, Servicio 1.3 Implicación comunitaria y de la organización* y *Servicio 1.4 Gestión de interesados descendentes*).

C. Estatutos del EIISP

Elaborar un estatuto o documento afín (por ejemplo, plan estratégico, plan de implementación o documento conceptual de operaciones).

Propósito
Identificar, describir y documentar los elementos programáticos básicos de acuerdo con los que funcionará el EIISP.

Resultado
Documento que describe los motivos de creación/fundación del EIISP y los resultados que se esperan del EIISP.

En el estatuto/plan del EIISP debe definirse lo siguiente:

- misión del EIISP (debe servir la misión de la organización y armonizarse con ella);
- objetivo, funciones y responsabilidades;
- productos y servicios (por ejemplo, recepción de informes de vulnerabilidad, creación de arreglos o parches, divulgación de anuncios de parches).

D. Modelo organizativo

Determinar y documentar la estructura organizativa y el modelo que adoptará el EIISP.

Propósito
Identificar, describir y documentar el modelo organizativo según el cual funcionará el EIISP.

Resultado
Crear una estructura bien definida con funciones y responsabilidades documentadas.

El modelo organizativo documentado debe describir la estructura de la jerarquía interna del EIISP e identificar la autoridad a que está sometido. Véanse en "Estructura organizativa del EIISP" las descripciones de los modelos organizativos más comunes (a saber, modelo distribuido, modelo centralizado, modelo híbrido). Véase más información al respecto en *Servicio 1.5 Coordinación de comunicación de incidentes dentro de la organización.*

E. Apoyo de la dirección y los interesados

Obtener el apoyo y adhesión de la dirección de la organización y de los interesados internos.

Propósito
Informar a la dirección y los interesados internos y obtener su apoyo y adhesión para que el EIISP funcione adecuadamente.

Resultado
Se informa a los interesados de las principales métricas empresariales para garantizar su apoyo constante.

Véase más información al respecto en *Servicio 1.1 Gestión de interesados internos*.

II Elementos tácticos

A. Presupuesto

Identificar los costes de los recursos necesarios para el funcionamiento del EIISP y obtener los fondos necesarios para financiar esos recursos.

Propósito
Identificar, describir y documentar el modelo organizativo con el que se financiará y funcionará el EIISP.

Resultado
Documentación de los costes operativos, los gastos y el modelo de financiación del EIISP.

En el presupuesto deben incluirse los gastos de personal (salarios, prestaciones y otros gastos conexos), de equipos y otros gastos de capital (por ejemplo, sistemas/dispositivos de tecnologías de la información, licencias de *software*) y de formación (incluidos los gastos de viaje) del EIISP.

B. Personal

Identificar los recursos de personal necesarios para la prestación de los servicios del EIISP y que el personal esté adecuadamente formado.

Propósito
Identificar, describir y documentar el modelo organizativo en función del cual se dotará al EIISP.

Resultado
Es necesario documentar los recursos de personal del EIISP.

Esto implica la identificación de los diversos puestos o de las funciones y responsabilidades de cada uno de los miembros del EIISP, así como las competencias (habilidades, aptitudes y conocimientos (HAC)) y demás requisitos (por ejemplo, formación, experiencia, certificación) de esas funciones. Pueden ocupar esos puestos o ejercer esas funciones empleados a tiempo completo, fabricantes, proveedores o una combinación de éstos.

En el plan de dotación de personal (o en un documento independiente) deberán identificarse y planificarse los requisitos de formación, incluida la formación general para todo el personal del EIISP y las formaciones específicas según las funciones (por ejemplo, formación inicial/de bienvenida; formación práctica y teórica continua y sensibilización; formación específica para el desarrollo profesional).

Véase más información al respecto en *Servicio 6.1 Formación del EIISP*.

C. Recursos y herramientas

Identificar y adquirir otros recursos y herramientas necesarios.

Propósito
Identificar y adquirir los recursos, equipos y herramientas necesarias para el funcionamiento del EIISP.

Resultado
Se documentarán y entenderán las necesidades del EIISP en materia de herramientas y recursos.

Entre estos recursos y herramientas se cuentan los siguientes:

- infraestructura, como las instalaciones (espacio de oficina);
- herramientas/tecnologías/equipos (*hardware*, *software*) (por ejemplo, véase *Servicio 3.3 Reproducción de vulnerabilidades*);
- sistemas/métodos de comunicación de vulnerabilidades (por ejemplo, sitio web, correo-e, teléfono) (véase *Servicio 2.1 Recepción de informes de vulnerabilidades*);
- comunicaciones seguras (por ejemplo, PGP/encriptación) (véase *Función 1.5.2 Gestión de comunicaciones seguras*);
- base de datos/sistema de trazabilidad de vulnerabilidades (por ejemplo, véanse *Función 1.5.3 Actualización del sistema de rastreo de defectos de seguridad* y *Función 3.2.1 Base de datos de buscadores*).

III Elementos operativos

A. Políticas y procedimientos

Documentar las políticas, procesos y procedimientos pertinentes para la realización de las operaciones del EIISP.

Propósito
Identificar, describir y documentar las políticas y procedimientos de acuerdo con los que funcionará el EIISP.

Resultado
El EIISP dispondrá de políticas formales que describan la autoridad del EIISP y la gobernanza/las operaciones que ejerce. El EIISP dispondrá también de procedimientos/directrices documentados en los que se describa cómo llevar a cabo su misión.

La documentación de políticas y procedimientos garantizará su interpretación común por todo el personal del EIISP, aportará coherencia y repetibilidad a los productos y servicios proporcionados por el EIISP y servirá de recurso formativo para el personal nuevo del EIISP.

B. Evaluación y mejoras

Identificar las métricas para evaluar el rendimiento y/o la eficacia con el fin de determinar las posibles mejoras.

Propósito
Valorar o evaluar el funcionamiento del EIISP e identificar las potenciales mejoras.

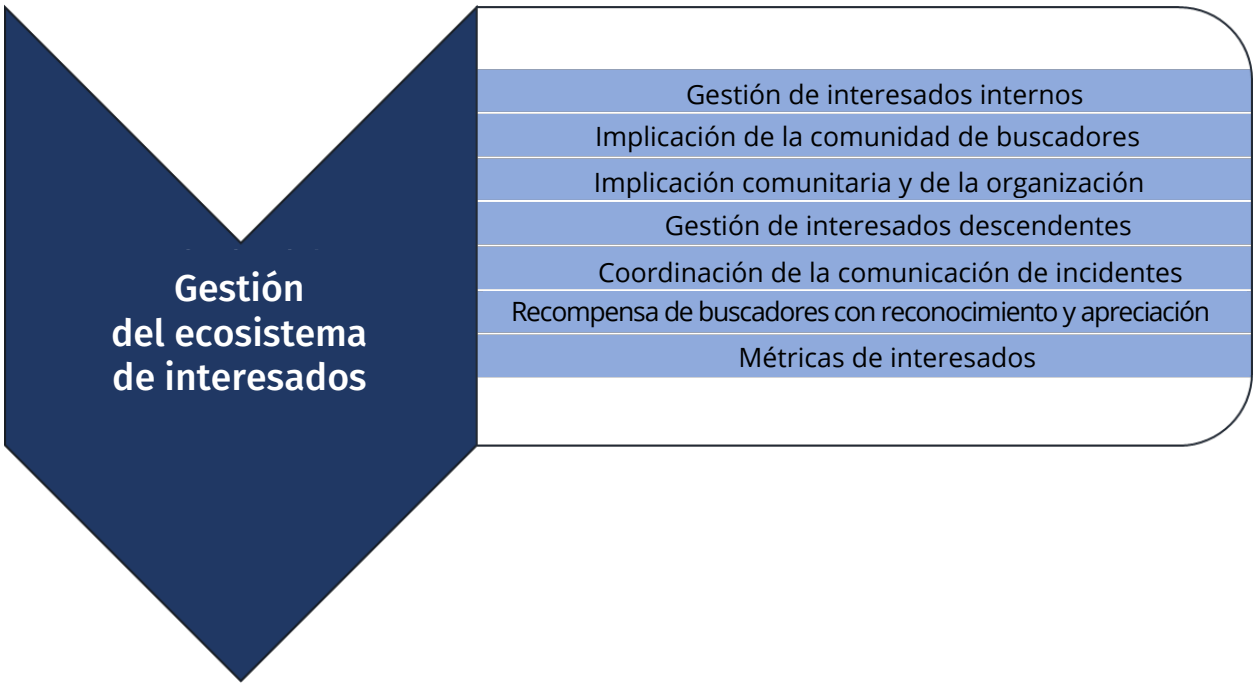
Resultado
El EIISP podrá medir su rendimiento y conocer las esferas cuya mejora es deseable.

El EIISP debe valorar o evaluar constante y/o periódicamente su rendimiento (prestación de productos y servicios) e identificar las esferas que cabe mejorar.

Las métricas y métodos de evaluación pueden ser informales (por ejemplo, recabar la opinión de los interesados) o formales y aplicarse en función de las necesidades (por ejemplo, documentar las lecciones extraídas [véase la *Función 1.1.3 Proceso posterior a los incidentes*]) o siguiendo un calendario determinado.

La información facilitada en este Marco de los EIISP puede servir para definir los criterios o capacidades empleados para evaluar el funcionamiento de los EIISP.

Esfera de servicio 1



Esta esfera de servicio comprende los servicios y funciones que un EIISP puede llevar a cabo para implicar adecuadamente a los interesados internos y externos. La ejecución de los servicios de esta esfera se lleva a cabo a lo largo de todo el ciclo de un incidente o del ciclo de madurez del EIISP. Esta esfera de servicio se dedica a garantizar que todos los interesados del EIISP están adecuadamente informados y se implican en el proceso de intervención en caso de incidente.

Antes de prestar formalmente estos servicios, el EIISP debe identificar en primer lugar a los interesados pertinentes para sus operaciones. Esos interesados pueden ser ejecutivos o directivos de la empresa, equipos de desarrollo internos, proveedores o creadores de componentes externos o, incluso, la base de clientes de la organización. Para racionalizar el proceso de comunicación puede resultar extremadamente útil elaborar una matriz de interesados en función de los productos/versiones. Antes de entablar la comunicación con esos interesados convendría entender la perspectiva, los medios o métodos por los que desean implicarse (portal web, correo-e personalizado, chat Internet, sistema de partes de incidencia, etc.). A los efectos de este documento, los interesados se dividen en varios grupos (en función de las circunstancias específicas de la empresa, puede haber otros): buscadores, pares/socios, equipos internos y consumidores de los productos.

Propósito
Poner de manifiesto los procesos y mecanismos para compartir la información con los interesados con los que un EIISP puede y debe interactuar.

Resultado
Una satisfactoria implicación del ecosistema de interesados del EIISP garantizará la oportuna comunicación de las vulnerabilidades descubiertas y que los interesados/socios se sientan satisfechos cuando se hayan de comunicar las vulnerabilidades de seguridad a los interesados de la organización.

Servicio 1.1 Gestión de interesados internos

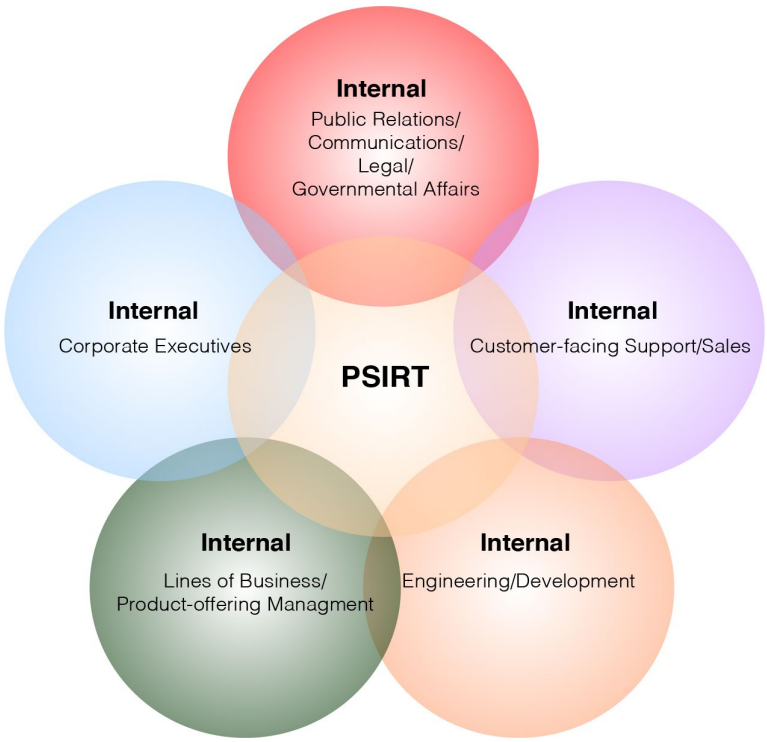


Figura 6: Gestión de interesados internos

Leyenda de la Figura 6:

EIISP	
Interno	*Relaciones públicas/Comunicaciones/Asuntos jurídicos/Asuntos gubernamentales*
Interno	*Dirección ejecutiva*
Interno	*Atención al cliente/Ventas*
Interno	*Líneas de negocio/Gestión de la cartera de productos*
Interno	*Ingeniería/Desarrollo*

Definir los procesos relacionados con la implicación de interesados internos para garantizar tanto su sensibilización como su asistencia en caso de incidente. La satisfactoria implicación de los interesados internos mejorará la comunicación y las intervenciones ayudando a explicar la función del EIISP dentro de la organización y estableciendo conexiones internas entre los equipos de productos y los analistas de seguridad.

Propósito

Asentar la autoridad y experiencia del EIISP ante los interesados internos para facilitar la coordinación en la reparación de vulnerabilidades y la seguridad de los productos.

Resultado

Si los interesados internos están muy implicados, todos los procesos y resultados del EIISP fluirán más fácilmente. Por ejemplo, los fallos descubiertos por los empleados eliminan la presión que suponen los embargos externos o el escrutinio de los medios, permitiendo así que el problema se resuelva en un plazo que beneficie a la organización, los consumidores y la comunidad en su conjunto, minimizando además el riesgo de revelación pública de vulnerabilidades.

Función 1.1.1 Implicación de interesados internos

Mantener un diálogo activo con los equipos internos implicados en el desarrollo, las pruebas, el empaquetado y el mantenimiento de las ofertas de la organización. Los interesados internos no son sólo los recursos de ingeniería, sino que también pueden ser los equipos de pruebas/garantía de calidad, ingeniería de comercialización, atención al cliente, ventas y comercialización y demás expertos en la materia.

Propósito
Imponerse en las plataformas de información/mensajería interna para notificar a los asociados internos la existencia, los procesos y las funciones del EIISP.

Resultado
El EIISP dispondrá de una lista de interesados internos y de una interpretación de sus funciones y responsabilidades formalmente documentadas.

Subfunción 1.1.1.1 Implicar a los directivos y ejecutivos de la organización/empresa

Para ser eficaz el EIISP debe entender el entorno de la organización y poder reaccionar a él. La colaboración con los directivos y ejecutivos ayuda al EIISP de varias maneras. Contribuye a legitimar el trabajo del EIISP dentro de la organización gracias al apoyo de la directiva. También permite al EIISP compartir información con la dirección para que ésta tome sus decisiones con conocimiento de causa. Al mismo tiempo permite a la dirección modificar las políticas u orientaciones que puedan alterar la misión del EIISP.

Subfunción 1.1.1.2 Implicar a los departamentos jurídico, de relaciones públicas y de comunicación corporativa

La colaboración con los equipos jurídico y de comunicaciones internos garantizará que el EIISP se ajuste a las normas de marca y comunicación en vigor, así como al marco reglamentario/jurídico al que se acoge la organización (por ejemplo, privacidad, espacio federal). Cada uno de estos interesados ofrece al EIISP vías de comunicación con interesados esenciales que se han de establecer antes de que ocurran eventos o incidentes críticos para garantizar que todas las partes pueden trabajar efectivamente de consuno.

Subfunción 1.1.1.3 Implicación de las líneas de producción

La colaboración con los creadores garantiza que se documenten, prioricen y solucionen adecuadamente todos los problemas. Por ejemplo, los ingenieros del EIISP o sus delegados autorizados tendrán que coordinar la eliminación de vulnerabilidades con los grupos de ingeniería de *software* responsables de los códigos fallidos. En caso de incidente, estas asociaciones contribuyen también a la rápida transmisión de información y a la rápida y efectiva solución de los problemas. Los interesados aquí son los gestores de programas o productos, los grupos de supervisión del CPS, los gestores de proyectos, los propietarios de los productos y otros con responsabilidades similares dentro de la empresa.

Subfunción 1.1.1.4 Implicación de creadores/ingenieros

Los ingenieros del EIISP deben coordinar la eliminación de vulnerabilidades con los grupos de ingeniería de *software* responsables de los códigos erróneos. La colaboración con los interesados creadores garantiza la adecuada documentación, priorización y solución de los problemas. En caso de incidente, estas asociaciones contribuyen también a la rápida transmisión de información y a la rápida y efectiva solución de los problemas.

Subfunción 1.1.1.5 Implicación de los equipos de venta y atención al cliente

Los ingenieros del EIISP han de comunicar a los equipos de atención a los interesados las explicaciones y hechos pertinentes para que, en caso de problema y su divulgación pública, estos equipos puedan responder a las dudas y peticiones de ayuda de los interesados. Entre otros, los equipos de "atención" son el personal de primera línea (también denominado, servicio de asistencia), los equipos de atención superior (por ejemplo, gestión de cuentas técnica, gestión de la satisfacción de los interesados, etc.), los equipos de ventas internos/externos y los recursos en el terreno (consultoría, ingeniería de ventas, etc.).

Subfunción 1.1.1.6 Participación en grupos de trabajo internos

En organizaciones más maduras, los ingenieros del EIISP pueden establecer e intensificar relaciones con los interesados internos participando en diversas iniciativas o grupos de trabajo internos. De este modo se reafirma/determina la experiencia técnica del EIISP y se crean los canales de comunicación/colaboración que podrán ser necesarios en el futuro.

Función 1.1.2 Ciclo de producción segura interno

Mantener e imponer el concepto de ciclo de producción segura es vital a la hora de inspirar a los interesados confianza en los productos de la organización. Si no se puede demostrar la capacidad de aplicar repetidamente las normas de seguridad a lo largo del ciclo de vida del producto, es posible que los interesados pierdan la fe en los productos de la organización, impongan requisitos más estrictos a la organización (carga probatoria, derecho de auditoría, etc.) y, en último término, se generen pérdidas de ingresos y de confianza de los interesados.

Propósito
Las organizaciones cuyas prácticas en materia de ciclo de producción segura son adecuadas gastarán menos en la solución de fallos de seguridad de sus productos al detectarlos en fases más tempranas de la producción. Todos los participantes en este ciclo conocerán perfectamente las expectativas en cuanto a características, funcionalidades y requisitos de seguridad de los productos y entenderán cuáles son sus funciones y responsabilidades dentro de ese ciclo.

Resultado
El EIISP dispondrá de información clara sobre la comercialización de los productos y podrá facilitar métricas y datos relativos al rendimiento de la prestación. En organizaciones maduras el EIISP puede facilitar datos históricos sobre vulnerabilidades comunes para evitar cometer los mismos errores en el futuro.

Subfunción 1.1.2.1 Participar en actividades de CPS

El CPS es un proceso de gobernanza clave que ayuda a la organización a producir productos estables y repetibles respetando normas comunes. La participación del EIISP en la creación y mantenimiento del CPS de la organización contribuye a garantizar que se siguen las prácticas de seguridad adecuadas y se efectúan las verificaciones pertinentes.

Subfunción 1.1.2.2 Participación en la gobernanza del CPS

El CPS es un proceso de gobernanza clave que ayuda a la organización a producir productos estables y repetibles respetando normas comunes. La participación del EIISP en la gobernanza y aplicación del CPS de la organización contribuye a garantizar que se siguen las prácticas de seguridad y se efectúan las verificaciones adecuadas, y que se documentan y revisan convenientemente las excepciones.

Función 1.1.3 Proceso posterior a los incidentes

Cuando se descubren vulnerabilidades en los productos de la organización, el EIISP debe proceder al examen de esos problemas, ya estén relacionados con los códigos, los procesos o el personal, y rendir informe a los interesados y dirigentes de la organización. Algunas vulnerabilidades de seguridad graves o muy públicas podrán necesitar un análisis más detallado de la reacción y corrección de los problemas por la empresa. Una reunión *post mortem* es aquella en la que participan todos los interesados implicados en la corrección y la comunicación para documentar lo que se hizo bien, lo que podía haberse hecho mejor y las modificaciones que se harán de cara al futuro.

Propósito
Dar cuenta clara y factual de lo acaecido en respuesta a una vulnerabilidad, incluidos los incidentes de seguridad, desde el punto de vista de todas las partes/equipos implicados. En caso de problema grave, el EIISP puede participar o liderar la respuesta de la organización para solucionar un problema conocido y de grandes consecuencias.

Resultado
El EIISP facilitará datos acerca de la reacción de la organización a las vulnerabilidades de software. Estos datos se integrarán en las "lecciones extraídas" para mejorar esa reacción en eventos futuros.

Subfunción 1.1.3.1 Creación de un proceso de revisión de defectos de seguridad de los productos

Creación de un proceso coherente para el examen *post mortem* de los problemas que ayude a garantizar la constante mejora de los productos a partir de las lecciones extraídas.

Subfunción 1.1.3.2 Examen de los plazos de los procesos y la publicación de actualizaciones

Seguimiento de puntos fuertes y débiles.

Subfunción 1.1.3.3 Examen de incidentes de gran impacto

Coordinar las respuestas y lecciones extraídas de la organización, examinar los incidentes de gran impacto y facilitar datos al respecto a los interesados de la organización y de otro tipo, según proceda.

Servicio 1.2 Implicación de la comunidad de buscadores

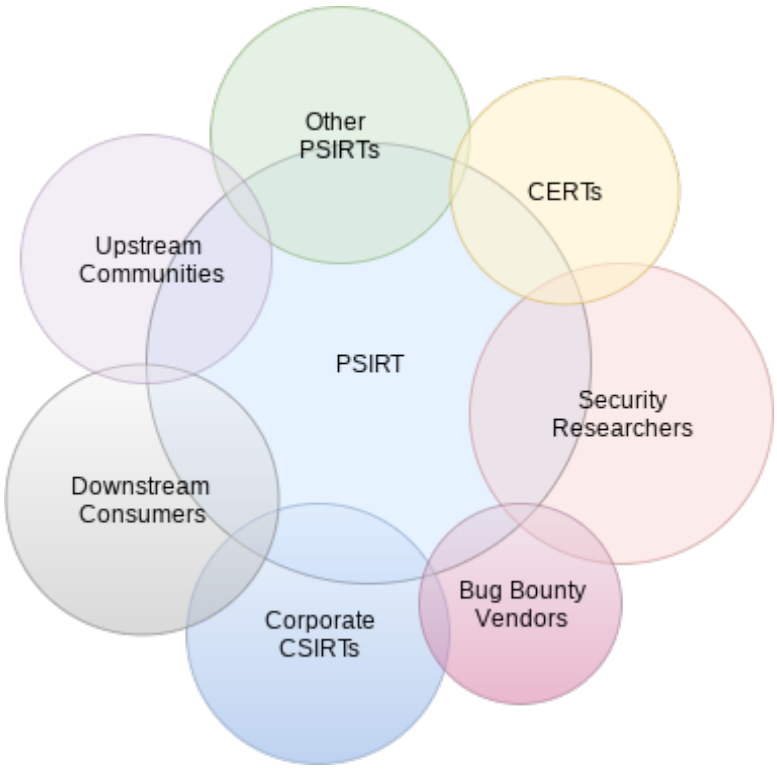


Figura 7: Ejemplos de interesados externos del EIISP

Leyenda de la Figura 7:
EIISP
Otros EIISP
EIEI
Investigadores en seguridad
Cazadores de errores
EIII de empresa
Consumidores descendentes
Comunidades ascendentes

Servicios relacionados con la implicación de la comunidad investigadora como interesado. Los buscadores desempeñan diversas funciones desde sus perspectivas individuales. Puede tratarse de personal académico, creadores profesionales, buscadores de seguridad profesionales o aficionados. Los buscadores pueden buscar ataques o fallos teóricos con fines de investigación y publicación académica, mientras que los profesionales pueden tener motivos financieros o empresariales. Otros pueden ser aficionados que participan en su tiempo libre con miras, quizá, a ganar el respeto y el

reconocimiento de sus comunidades. La implicación de la comunidad de buscadores es un método proactivo de intervención en caso de incidente de seguridad de los productos.

Propósito
Situar al EIISP de la organización como participante activo de la comunidad investigadora y dar a conocer las amenazas que pueden afectar a la seguridad de los productos de una organización. Una relación negativa o antagonista con los buscadores puede hacer que se retrase la notificación de investigaciones, lo que podría menoscabar la reacción de la organización a las vulnerabilidades de seguridad, repercutiendo en el sentimiento de los interesados hacia la organización.

Resultado
La satisfactoria implicación de la comunidad reforzará la reputación de la organización y su posición en el mercado como defensor de la seguridad de los productos. Además, la colaboración positiva con los buscadores puede dar acceso temprano a las investigaciones y/o publicaciones de vulnerabilidades de seguridad que pueden ayudar a la organización a preparar su reacción en caso de divulgación pública.

Función 1.2.1 Implicación de buscadores

Implementar actividades diseñadas para mantener un diálogo activo con los buscadores que tienen experiencia en el ámbito de la seguridad de los productos de una empresa y acceder a distintos canales. El EIISP puede realizar diversas actividades para implicarse más profundamente con las comunidades de buscadores, por ejemplo, contratar a buscadores cualificados, contactar con ellos en conferencias y otros eventos o patrocinar estudios académicos.

Propósito
Tener presencia en los medios sociales. Seguir los medios sociales y otros sitios/foros comunes en busca de indicadores de que los buscadores o interesados han encontrado problemas. Considerar la posibilidad de asistir regularmente a conferencias de seguridad a las que puedan asistir los buscadores.

Resultado
El EIISP recibirá de los buscadores muy implicados informes de mayor calidad con una frecuencia y antelación superiores, gracias a las expectativas de comunicación bien definidas.

Función 1.2.2 Colaboración con otros EIISP

Cultivar las relaciones con otros EIISP puede redundar en la compartición de información y la prestación de asistencia mutua y/o coordinación en caso de incidente. El trabajo con organizaciones pares puede ayudar a obtener datos esenciales para la solución de vulnerabilidades y permite a la organización beneficiarse de la experiencia de los pares cuando los grupos se consultan problemas. El EIISP debe crear canales de comunicación (normales y seguros) con los EIISP pares más importantes. El establecimiento y cultivo de relaciones con pares industriales es fundamental para la compartición de información y la coordinación de problemas que afectan a ambas organizaciones.

Propósito
Crear canales de comunicación entre la organización propia y otros EIISP para compartir información sobre vulnerabilidades, amenazas y prácticas idóneas.

Resultado
Una comunidad de EIISP pares ayuda a responder a las vulnerabilidades en la cadena de producción de software. Puede esperarse una respuesta más rápida.

Subfunción 1.2.2.1 Documentación y definición de EIISP pares

Recopilar información de contacto y procesos de implicación para el futuro. El EIISP debe colaborar e interactuar con la comunidad de EIISP general para compartir prácticas idóneas e información sobre las lecciones extraídas. Cuando surgen vulnerabilidades, éstas suelen solucionarse de manera colaborativa y grupal y el EIISP puede aumentar sus capacidades internas aprovechando la información y/o asistencia de sus pares externos.

Subfunción 1.2.2.2 Definición del proceso de revelación coordinado

El EIISP debe documentar detalladamente los parámetros y acuerdos de compartición de información sobre vulnerabilidades. El EIISP deberá respetar los parámetros de embargo definidos por los buscadores de vulnerabilidades y/o la organización informante (y esperar que se respeten los suyos propios).

Subfunción 1.2.2.3 Establecimiento de un procedimiento de compartición de información segura

El EIISP debe definir dos métodos para compartir de manera segura la información sobre vulnerabilidades y confidencial de otro tipo con las partes involucradas en el acuerdo de revelación coordinada. Las opciones son, entre otras, la comunicación no electrónica fuera de banda, los correos electrónicos/portales encriptados o las listas de correo privadas.

Subfunción 1.2.2.4 Participación en los grupos de trabajo y grupos de interés especial de la industria

La colaboración con los pares sobre temas de interés para la industria propicia y cultiva las relaciones y aumenta la profesionalización de la industria al resolver los problemas de manera colaborativa.

Función 1.2.3 Implicación de coordinadores (EIISI y otras organizaciones centrales de coordinación)

La colaboración con los EIISI gubernamentales aumenta la confianza a la hora de compartir información y ayuda a los EIISP a ganar la confianza y el respeto de pares reputados. Otras organizaciones con intereses o comunidades pertinentes son, entre otras, FIRST, MITRE, Advancing Open Standards for the Information Society (OASIS), Industry Consortium for Advancement of Security on the Internet (ICASI) y Organización Internacional de Normalización (ISO). Los grupos participantes pueden ser de ámbito nacional, empresarial, regional o industrial.

Propósito
Las organizaciones suelen ser el objetivo de atacantes que amenazan con explotar vulnerabilidades desconocidas para penetrar en las redes. Establecer relaciones con los EIISI

genera confianza y ofrece los contactos necesarios para recibir con prontitud los informes de vulnerabilidad.

Resultado
Mantener una buena relación con los EIISI y otras organizaciones centrales de coordinación permite conocer rápidamente las vulnerabilidades, permitiendo así una intervención más rápida.

Subfunción 1.2.3.1 Implicación de comunidades y socios

El EIISP debe averiguar donde dialogan los grupos externos de interés y procurar participar en esos foros.

Función 1.2.4 Implicación de investigadores en seguridad

Hay distintos tipos de investigadores en seguridad: académicos, aficionados y profesionales de la seguridad, por citar sólo algunos. Éstos son los principales buscadores de vulnerabilidades dentro de la industria. Los investigadores procurarán ponerse en contacto con el propietario de los productos, pero es posible que, por diversos motivos, no siempre den con la persona adecuada. Los EIISP recibirán de manera pasiva los informes de estas personas o grupos y se verán obligados a trabajar en plazos controlados por terceros. Es más conveniente para los EIISP adoptar una táctica proactiva con los investigadores en seguridad en esferas que pueden afectar a los productos del EIISP y colaborar positivamente con esos grupos para tener una mejor visibilidad de los problemas descubiertos.

Subfunción 1.2.4.1 Implicación de suministradores de seguridad

Los grandes suministradores de seguridad comerciales trabajan con los interesados en caso de fallo y con frecuencia dispondrán de datos forenses a los que normalmente no tendrá acceso el EIISP. El cultivo de relaciones con esos suministradores contribuirá a crear una confianza y respeto mutuos y, en el mejor de los casos, puede ofrecer al EIISP acceso a datos de amenazas críticas que de otro modo no podría conocer.

Subfunción 1.2.4.2 Documentación de suministradores de seguridad pertinentes

Conocer y entablar relaciones con los suministradores de seguridad puede acelerar las comunicaciones y los esfuerzos de comunicación/solución de vulnerabilidades cuando se remite esa información al EIISP. Hay que saber a qué información tendrán acceso esos suministradores y qué información retendrán. La relación entre la organización y los cazadores de errores deberá estar perfectamente documentada y prohibida antes de concluir un acuerdo mediante el cual todas las partes involucradas sepan cómo se deben comportar, a qué recursos tienen acceso, cómo se comparten los datos y con quién.

Subfunción 1.2.4.3 Documentación de métodos para colaborar con suministradores de seguridad

El EIISP debe averiguar donde dialogan los grupos externos de interés y procurar participar en esos foros.

Función 1.2.5 Implicación de cazadores de errores

Establecer una relación con cazadores de errores para mejorar la comunicación y la compartición de datos en el marco de la gestión de vulnerabilidades.

Propósito
Si la organización recibe con frecuencia informes de vulnerabilidades de fabricantes/distribuidores que contratan a buscadores de errores, se deberá considerar la posibilidad de mantener una relación directa con esas organizaciones, que suelen concluir acuerdos de nivel de servicio (SLA) para la eliminación de vulnerabilidades.

Resultado
Mantener una relación directa con los cazadores de errores puede permitir establecer un diálogo directo en el marco de la publicación de parches de seguridad. Además de concluir SLA convenientes, esa relación contribuirá a reducir el riesgo de vulnerabilidades del día cero en beneficio de todos los interesados.

Subfunción 1.2.5.1 Documentación y definición de programas de caza de errores pertinentes

Documentar y definir quiénes son los cazadores de errores pertinentes para los productos de la organización.

Subfunción 1.2.5.2 Implicación de cazadores de errores

Identificar canales para entablar un diálogo activo con los cazadores de errores.

Función 1.2.6 Anticipar las necesidades de los EIISI

Los EIISI son un tipo especial de interesados "descendentes", que se centran exclusivamente en los problemas de seguridad. Sin bien normalmente es posible interactuar con estos grupos mediante la implicación de interesados y la gestión de clientes tradicionales, el EIISP debe entender los requisitos y perspectivas propios de estos grupos centrados en la seguridad, que se pondrán en contacto con el EIISP y consumirán su información. Esto incluye los formatos y plazos de revelación (véase *Servicio 5.3 Revelación*), así como los canales de comunicación para solicitudes específicas.

Servicio 1.3 Implicación comunitaria y de la organización

Hay dos grupos de interesados con los que interactuará el EIISP que merecen una atención especial. En ocasiones denominados "ascendentes" y "descendentes", la participación de estas comunidades es fundamental en los esfuerzos de resolución y la ayuda mutua entre grupos pares de la organización. "Ascendente" es el término utilizado para calificar a los grupos o personas de la organización propia que provee los componentes o proyectos para los productos. "Descendentes" son las personas, grupos u organizaciones que incluyen los productos de la organización en sus ofertas. La implicación de entidades descendentes se contempla en *Servicio 1.4 Gestión de interesados descendentes*.

Una comunidad ascendente activa permite introducir innovaciones en las cadenas de producción y alivia la carga cuando la solución de vulnerabilidades es compleja, compensando a menudo la carencia de conocimientos especializados de la organización. Del mismo modo, el establecimiento de relaciones profesionales con personas y equipos de otras organizaciones puede contribuir a ampliar las capacidades del EIISP dándole acceso a perspectivas, capacidades y conocimientos externos. Esto puede lograrse implicando proactivamente a la comunidad de seguridad como interesado, estableciendo relaciones con socios y EIISP pares.

Propósito
El EIISP debe construir y mantener un ecosistema activo de socios y pares. Estas asociaciones comunitarias pueden ayudar a encontrar y solucionar fallos al haber "muchos ojos" y a compartir prácticas idóneas entre distintos grupos para mejorar la solución de vulnerabilidades en general.

Resultado
Una buena relación y un ecosistema activo de socios y pares facilitará la compartición de información sobre amenazas y prácticas idóneas. Un EIISP con una buena reputación entre la comunidad de seguridad puede atraer recursos y colaboradores para solucionar situaciones críticas.

Función 1.3.1 Definir e implicar a las comunidades y socios ascendentes

Con frecuencia los productos incluirán códigos o componentes ajenos a la organización. Los creadores de ese material suelen denominarse terceros, proveedores, fabricantes ascendentes, fabricantes de equipos originales (OEM) o socios, simplemente. Conviene identificar a esos socios dentro del ecosistema y determinar cómo la organización se pondrá en contacto con ellos y los implicará cuando se descubran vulnerabilidades en el código de terceros.

Propósito
Establecer relaciones laborales cordiales con las personas o grupos de los que se reciben componentes o los grupos que reciben componentes de la organización. Entender cómo y a través de quién contactar con esos grupos ayudará al EIISP a mantenerse informado de los problemas potenciales y entender a quién se ha de informar cuando se descubran componentes afectados que se suministran a otros.

Resultado
El EIISP entenderá mejor de dónde y quién proceden los componentes, gracias a lo cual se podrá acceder más rápidamente a la información y las soluciones cuando se descubran fallos en los componentes.

Subfunción 1.3.1.1 Documentación y definición de comunidades y socios ascendentes

Las comunidades y socios ascendente facilitan códigos y/o conocimientos y capacidades que se integran en los productos de la organización. Es fundamental conocer y colaborar con esos proveedores para garantizar una rápida y eficaz interacción cuando se comunican vulnerabilidades de seguridad y el EIISP se ocupa de ellas. En una configuración ideal esas relaciones se documentan en contratos y están cubiertas por acuerdos de no divulgación y otros mecanismos de protección de la organización.

Subfunción 1.3.1.2 Implicación de comunidades y socios

Cada comunidad o socio ascendente puede utilizar métodos o herramientas distintos para crear *software*/productos y comunicar al respecto. El EIISP debe saber cómo contactar con esos grupos y asegurarse de que dispone de los contactos/métodos adecuados para colaborar con ellos en caso de problema de seguridad.

Subfunción 1.3.1.3 Participación en comunidades ascendentes

La participación con comunidades y socios ascendentes contribuye a crear una valiosa confianza entre los grupos y a aumentar las capacidades del equipo externo gracias a los conocimientos que pueda aportar la organización.

Subfunción 1.3.1.4 Participación en los eventos comunitarios e industriales

Las conferencias y reuniones profesionales de organizaciones brindan al EIISP grandes ocasiones para interactuar con los interesados y los socios, recibiendo información directa para la organización y generando un clima de confianza y buena reputación en la comunidad externa, que podrá aprovecharse en caso de coordinación/colaboración futura.

Subfunción 1.3.1.5 Implicación de equipos de seguridad comunitarios

Es fundamental que el EIISP sepa cómo y a través de quién ponerse en contacto con los equipos de seguridad de *software*/*hardware*/proveedores de servicio ascendentes (EIISP, EIISI, ingenieros de seguridad). Establecer vías de comunicación e información entre el EIISP y estos grupos redunda en una interacción natural en caso de crisis y de solución de vulnerabilidades.

Función 1.3.2 Definir e implicar a las comunidades y socios descendentes

El término "descendente" tiene muchas connotaciones, pero no implica que el EIISP deba ignorar a estos importantes grupos de interesados. Por "descendente" se entiende todo producto, organización o persona que utiliza los productos y ofertas de la empresa del EIISP para sus propios fines. Generalmente se trata de clientes o consumidores de los bienes y servicios ofrecidos, aunque no siempre es el caso. Con frecuencia otra empresa puede utilizar u obtener una licencia para los productos de la empresa del EIISP y revenderlos como tercero. En el caso del *software* de código abierto suele pasar que un grupo creará y mantendrá el *software* y un amplio grupo de partes auxiliares se aprovechará de esos recursos, que recibirán de la fuente.

Subfunción 1.3.2.1 Documentación y definición de comunidades, consumidores y socios descendentes

Las comunidades y socios descendentes consumen los códigos y/o conocimientos y experiencia integrados en los productos de la organización. En una configuración ideal estas relaciones se documentan en contratos, cubiertos por acuerdos de confidencialidad y otras cláusulas que protegen a la organización.

Subfunción 1.3.2.2 Implicación de las comunidades descendentes

Cada comunidad o socio descendente puede emplear distintos métodos o herramientas para crear su *software*/producto y comunicar al respecto. El EIISP debe saber cómo ponerse en contacto con esos grupos externos y asegurarse de que cuenta con los contactos/métodos adecuados para colaborar en caso de problema de seguridad que implique a esas partes externas.

Servicio 1.4 Gestión de interesados descendentes

Para implicar a los interesados, el EIISP debe definir procesos y métodos de interacción con la comunidad de interesados en el marco de las intervenciones de seguridad de los productos. Es fundamental que los interesados en los productos de la organización estén satisfechos, pues representan las fuentes actuales y futuras de ingresos de la organización.

Propósito
El EIISP debe crear y mantener vías de comunicación con la base de interesados de la organización a fin de transmitir información sobre las vulnerabilidades de seguridad de los productos o cuando se interviene en caso de incidente.

Resultado
Mantener una buena relación con los interesados no sólo conservará (y en ocasiones aumentará) los ingresos, sino que permitirá a los interesados opinar sobre el producto, dándoles una sensación de importancia y participación en la solución.

Función 1.4.1 Implicación de interesados descendentes

Los interesados en los productos y servicios deben disponer de medios para compartir informaciones y opiniones y conocer cómo la organización gestiona las vulnerabilidades de seguridad. Colaborar proactivamente con los interesados de la organización ayuda a dar una imagen positiva de la marca y conservar/aumentar la lealtad de los interesados.

Propósito
Ofrecer métodos de comunicación de los interesados descendentes de la organización con el EIISP y ayuda en caso de problema de seguridad. No reaccionar adecuadamente a las dudas o peticiones de los interesados puede menoscabar la imagen de marca a causa de los comentarios públicos negativos, la no renovación de abonos o la pérdida de oportunidades comerciales.

Resultado
Los interesados descendentes deben recibir rápidamente orientaciones claras sobre los fallos de seguridad. Esto aumentará la confianza en los productos y la lealtad hacia la marca. Se creará una experiencia globalmente positiva con la ayuda del EIISP y hará que el EIISP gane experiencia con los interesados. En general, se mejorará la opinión de los interesados acerca de la marca.

Subfunción 1.4.1.1 Facilitación de políticas de ciclo de vida y apoyo claras

La organización debe describir clara y públicamente cuáles deben ser las expectativas de los interesados en relación con la solución de vulnerabilidades de seguridad y durante

cuánto tiempo recibirán ayuda con los productos. Véase más información al respecto en ***Esfera de servicio 4***.

Subfunción 1.4.1.2 Implicación de interesados

Los interesados en los productos y servicios de la organización plantearán preguntas, necesitarán asistencia o que se solucionen los fallos de seguridad anunciados. El EIISP debe responder activamente a las solicitudes de los interesados, dar orientaciones claras y precisas en relación con las vulnerabilidades de seguridad y mitigar los riesgos hasta que pueda darse una solución a los interesados.

Servicio 1.5 Coordinación de comunicación de incidentes dentro de la organización

Los incidentes de seguridad afectan a muchos grupos internos, y posiblemente productos, de la organización. El EIISP es el punto central desde el que se coordinan los esfuerzos de eliminación de las vulnerabilidades y donde se comparten las informaciones sobre el evento con los interesados internos autorizados.

Propósito
Garantizar que todas las partes de la organización disponen de información sobre las vulnerabilidades de seguridad a fin de tomar con conocimiento de causa decisiones sobre las medidas que se han de tomar al respecto. La comunicación puede hacerse de diversas maneras (correo electrónico, correo tradicional, RSS, medios sociales, etc.), pero en último término se facilita información clara, puntual y precisa sobre las vulnerabilidades de seguridad y los incidentes que afectan a los interesados.

Resultado
Se informará a los interesados internos del alcance y repercusión de las amenazas a los productos de la organización. Es necesario informar a los interesados a fin de que puedan tomar las medidas adecuadas cuando se solucione la vulnerabilidad de seguridad y se disponga de las medidas correctivas.

Función 1.5.1 Ofrecer canales/medios de comunicación

Para comunicar eficazmente con los interesados el EIISP debe contar con diversos canales. Cada interesado utilizará el canal de su preferencia. Al preparar y publicar las comunicaciones el EIISP deberá dirigirse a la mayor cantidad de gente posible. El EIISP también deberá estar preparado para recibir informes de seguridad, comentarios y preguntas de diversas fuentes.

Propósito
Ofrecer a los interesados métodos de comunicación con el EIISP.

Resultado
Estos canales, ya sean correo-e, chat, formularios web, etc., permitirán a los interesados internos comunicar y compartir información con el EIISP.

Subfunción 1.5.1.1 Ofrecer canales de comunicación claros

Los interesados deben tener la posibilidad de plantear preguntas, verificar el estado de los fallos y comunicar problemas al EIISP. Si un interesado descubre una vulnerabilidad de seguridad, o se ve afectado por ella, debe poder preparar y enviar un informe al EIISP con facilidad.

Subfunción 1.5.1.2 Ofrecer canales de comunicación interna

Para trabajar con los interesados internos, el EIISP debe ofrecer canales de comunicación a través de los cuales informar acerca del proceso de solución de las vulnerabilidades. Los interesados internos deben poder ponerse en contacto fácilmente con el EIISP y saber qué respuesta pueden recibir a sus preguntas.

Subfunción 1.5.1.3 Ofrecer canales de comunicación externa

Para trabajar con los interesados externos, el EIISP debe ofrecer canales de comunicación a través de los cuales informar acerca del proceso de solución de las vulnerabilidades. Esto incluye la prohibición/autorización de la comunicación externa para garantizar su validez y adecuado encaminamiento a los asociados internos.

Función 1.5.2 Gestión de comunicaciones seguras

Con frecuencia el EIISP debe tratar información que se considera confidencial (es decir, problemas sobre los que hay un embargo informativo). El EIISP debe poder comunicar de manera segura y privada con los buscadores, otras organizaciones o los recursos internos correspondientes. El respeto de los acuerdos de confidencialidad y la comunicación exclusivamente por medios privados contribuye a la confianza de los buscadores. La protección de la información confidencial sobre vulnerabilidades contra las partes no autorizadas también contribuye a la gestión adecuada y efectiva del problema, de conformidad con los términos del embargo. La utilización de canales seguros también ayuda a proteger la identidad de los buscadores, si éstos no quieren revelarla. Debe definirse una política de retención para garantizar que los datos se destruyen convenientemente tras su utilización.

Propósito
Ofrecer los medios necesarios para intercambiar información sobre vulnerabilidades de seguridad de manera privada. Estos canales protegen la confidencialidad de las vulnerabilidades de seguridad y de los buscadores hasta el momento en que pueda divulgarse públicamente esa información.

Resultado
Las partes implicadas en los problemas de seguridad pueden compartir de manera privada información con las partes pertinentes. Hay más probabilidades de que los buscadores vuelvan a colaborar con la organización si sienten que ésta protege sus intereses.

Subfunción 1.5.2.1 Ofrecer canales de comunicación segura

El EIISP debe garantizar que los buscadores de vulnerabilidades y los socios implicados en las vulnerabilidades que atañen a los productos de la organización disponen de métodos privados y seguros para compartir información.

Función 1.5.3 Actualización del sistema de rastreo de defectos de seguridad

El EIISP debe tener acceso al/a los sistema(s) de registro de defectos de todos los productos y debe poder crear y utilizar un sistema para rastrear y compartir información sobre vulnerabilidades de seguridad.

Propósito
El adecuado registro y rastreo de los defectos de seguridad permite a la organización conocer dónde y cuándo se solucionaron las vulnerabilidades. Este sistema permite también la comunicación entre el EIISP, los buscadores y los ingenieros que trabajan activamente en la solución de los problemas.

Resultado
La utilización de un sistema para rastrear adecuadamente las vulnerabilidades de seguridad permite a todas las partes que necesitan esa información conocer los antecedentes y la evolución del caso, y formular comentarios al respecto.

Subfunción 1.5.3.1 Rastreo de defectos y fallos de seguridad de los productos

Es necesario hacer un seguimiento de los defectos de seguridad y a ese sistema han de poder acceder (en el modelo de menos privilegios) partes internas y externas (si procede) para actualizar y rastrear la información. Los buscadores externos han de recibir información adecuada sobre la evolución de los casos que hayan comunicado al EIISP.

Subfunción 1.5.3.2 Crear y publicar un proceso de rastreo de defectos de seguridad

El EIISP debe garantizar que los buscadores de vulnerabilidades y los socios implicados en las vulnerabilidades que atañen a los productos de la organización disponen de métodos privados y seguros para compartir información.

Función 1.5.4 Compartición y publicación de información

Una vez solucionado un problema, el EIISP debe dar a conocer la vulnerabilidad de seguridad, utilizando CVSS como factor, su gravedad y consecuencias, su riesgo potencial de explotación y la manera de resolver o paliar el problema. Una manera muy común de dar a conocer amplia o públicamente la información sobre vulnerabilidades es adquirir una entrada CVE

para la vulnerabilidad en cuestión. De este modo se garantiza que el problema se identifica unívocamente con un número de identificación, una descripción y, al menos, una referencia pública.

Propósito
Compartir información sobre las vulnerabilidades de seguridad comunicadas y solucionadas. Los interesados deben poder recibir las soluciones o los métodos alternativos para reducir los riesgos hasta que se solucione formalmente la vulnerabilidad.

Resultado
Se informará a los interesados acerca de los problemas de seguridad, cómo pueden afectarles y

cómo se van a solucionar. Los interesados que reciban puntualmente informaciones y actualizaciones serán más proclives a tener una opinión positiva de la organización y seguir utilizando sus productos o adoptar otros nuevos.

Subfunción 1.5.4.1 Ofrecer múltiples medios de comunicación

A la hora de revelar públicamente las vulnerabilidades, cada interesado optará por un método de interacción/comunicación diferente. El EIISP debe asegurarse de que, además de los avisos tradicionales, se utilizan otros métodos para garantizar la máxima implicación/información de los interesados en relación con la vulnerabilidad. Una vez solucionadas las vulnerabilidades, el EIISP debe comunicar esa información utilizando múltiples métodos.

Subfunción 1.5.4.2 Retroinformación a los interesados

La retroinformación mejora los procesos e intervenciones de cara al futuro. Puede poner de manifiesto los puntos fuertes del EIISP y señalar las esferas en las que el EIISP debe mejorar.

Servicio 1.6 Recompensa de buscadores con reconocimiento y apreciación

El reconocimiento otorgado a los buscadores permite asentar su credibilidad y la de su organización (si procede) en el seno de la comunidad, además de expresar agradecimiento del EIISP por su asociación en el marco del fallo en cuestión.

Propósito
Se reconocen a los buscadores sus esfuerzos por coordinar la revelación de las vulnerabilidades de los productos. Los buscadores pueden forjar su reputación gracias a ese reconocimiento, documentar su experiencia y mostrar su valor para la organización.

Resultado
Una colaboración positiva con los buscadores mejorará la seguridad de los productos. El reconocimiento otorgado a los buscadores es benéfico para los empleados internos, pues contribuye a forjar su reputación y demuestra su experiencia.

Función 1.6.1 Otorgar reconocimiento

Otorgar reconocimiento a la(s) persona(s) responsable(s) del descubrimiento de una vulnerabilidad de seguridad es fundamental dentro del flujo de trabajo de las vulnerabilidades de seguridad. Una pequeña expresión de gratitud alienta la confianza y el respeto en la comunidad y muestra que la organización interviene rápidamente en caso de problema de seguridad.

Propósito
Reconocer a los buscadores sus esfuerzos por revelar responsablemente las vulnerabilidades del producto. Los buscadores pueden forjar su reputación gracias a ese reconocimiento y documentar su experiencia.

Resultado
Una colaboración positiva con los buscadores mejorará la seguridad de los productos. El reconocimiento otorgado a los buscadores es benéfico para su reputación y les anima a comunicar futuras vulnerabilidades al EIISP.

Subfunción 1.6.1.1 Otorgar reconocimiento

Reconocer por escrito los esfuerzos de los buscadores y su implicación en el descubrimiento de una vulnerabilidad de seguridad es la herramienta más barata y eficaz a disposición del EIISP para recompensarlos. Habitualmente se incluye un reconocimiento a los buscadores en los avisos de seguridad, las notas de publicación de *software* y CVE. El EIISP tendrá que saber cómo se comunicará la atribución interna de las vulnerabilidades detectadas.

Función 1.6.2 Recompensa de buscadores

Para generar resultados positivos para los interesados y fomentar la compartición de las investigaciones, el EIISP puede optar por crear un programa de recompensa o incentivo de esta colaboración con la esperanza de que prosiga y se amplíe en el futuro.

Propósito
Recompensar a la(s) persona(s) que comunique(n) fallos de seguridad en los productos y servicios de la organización. Las recompensas pueden ser de varios tipos, desde notas de agradecimiento electrónicas/físicas a premios de la organización, monetarios o incentivos de otro tipo. El EIISP debe ser transparente en relación con las recompensas otorgadas y las normas aplicables a su concesión.

Resultado
Esta práctica está diseñada para dar una imagen positiva de la organización y fomentar una constante colaboración en relación con problemas de seguridad.

Subfunción 1.6.2.1 Crear programas de recompensa para los buscadores

El EIISP puede patrocinar programas de recompensa diseñados para fomentar comportamientos positivos de los buscadores de seguridad. Las recompensas pueden ser monetarias, materiales o de otro tipo, que los buscadores consideren valiosas, además del reconocimiento otorgado por descubrir el problema.

Subfunción 1.6.2.2 Recompensa por errores

Un tipo de recompensa es el dinero. Algunas organizaciones pagarán a los buscadores que les comuniquen información sobre vulnerabilidades.

Subfunción 1.6.2.3 Clasificación

Otra forma de compensación es el establecimiento de una "clasificación". Esto convierte el hallazgo y la comunicación de vulnerabilidades de seguridad en un juego y alienta una sana competencia entre los buscadores en torno a la clasificación y quién ocupa la cabeza.

Servicio 1.7 Datos para los interesados

La comunicación de datos acerca del volumen, el rendimiento u otros parámetros del EIISP es fundamental a la hora de dar a conocer a los interesados la eficacia del EIISP. Cada interesado tiene un punto de vista al que se ha de responder con datos (u opiniones) en distintos formatos. El EIISP debe saber cómo desea cada grupo de interesados consumir esa información. Estos datos pueden ser los indicadores fundamentales de rendimiento (IFR) del EIISP. En la *Función 2.5.1* se trata de los informes operativos y de las maneras en que el EIISP puede presentar esos informes para garantizar un funcionamiento sin problemas. En la *Función 2.5.2* se abordan los informes de empresa, que el EIISP puede presentar a los interesados.

Propósito
Ofrecer datos acerca del EIISP y su rendimiento que ayudan a los interesados a entender la eficacia del EIISP en relación con diversas esferas o servicios.

Resultado
Al consultar las métricas del EIISP, los interesados deben saber cómo el EIISP ofrece efectivamente un servicio y deben poder dar su opinión al respecto a fin de ajustar la prestación de ese servicio.

Función 1.7.1 Comprensión de los requisitos de los interesados

A fin de articular efectivamente la prestación de los servicios del EIISP hay que entender las perspectivas de cada uno de los grupos de interesados. A algunos puede interesarles la puntualidad de los parches de seguridad, mientras que otros se centrarán en la dimensión financiera del funcionamiento del EIISP. Cada perspectiva es válida y necesita unos datos diferentes para comunicar efectivamente la información deseada. Se ha de consultar con cada grupo de interesados para entender los aspectos del EIISP que desean conocer detalladamente y determinar el mejor método para compartir esa información.

Propósito
Entender lo que importa a los interesados en relación con el funcionamiento y los servicios del EIISP. Una vez conocidos y acordados esos requisitos, se escogerá un método/medio de comunicación y la periodicidad con que se comunicarán las actualizaciones.

Resultado
Se creará y mantendrá una lista documentada de requisitos y preferencias de los interesados (informes/opiniones/anuncios).

Subfunción 1.7.1.1 Obtención de los requisitos de los interesados

Las preferencias de los interesados en cuanto a datos concretos serán propias a cada uno de ellos. Por ejemplo, pueden recopilarse datos sobre el rendimiento del equipo de parches en general, sus costes y su calidad.

Función 1.7.2 Recopilación de datos para los interesados

Se trata de los procesos y acciones necesarios para documentar los datos solicitados por cada uno de los grupos de interesados. Siempre que sea posible, las herramientas utilizadas por el EIISP podrán recopilar y ofrecer información sobre los procesos del EIISP y su rendimiento. En

una configuración ideal esos datos se almacenarán de manera centralizada (base de datos, hoja de cálculo u otras herramientas) a fin de poder examinar periódicamente el historial de rendimiento y que cada interesado pueda acceder a los datos que le atañen con un mínimo de esfuerzo adicional.

Propósito
Obtener, generar, agregar y/o recopilar los datos necesarios para satisfacer los requisitos de los interesados en relación con el rendimiento del EIISP en diversas esferas. Esta información debe almacenarse de manera centralizada para que los interesados puedan conocer los antecedentes y reutilizar la información (cuando dos o más grupos de interesados desean la misma información).

Resultado
Se recopilarán los datos para los interesados a fin de darles forma (informes, opiniones, anuncios, etc.).

Subfunción 1.7.2.1 Obtención de datos para los interesados

El EIISP definirá los procesos y métodos necesarios para recopilar los datos necesarios con la periodicidad prescrita (SLA/OLA).

Subfunción 1.7.2.2 Almacenamiento de datos para los interesados

El EIISP deberá realizar un análisis histórico de su rendimiento y de otras tendencias a fin de crear un repositorio de datos y poder seguir utilizando esa información en el futuro.

Función 1.7.3 Análisis de los datos para los interesados

Los datos sin contexto no tienen sentido, pues pueden formularse supuestos incorrectos y no ajustar debidamente los servicios a la evolución del negocio o las demandas de los interesados. Una vez recopilados los datos necesarios, el EIISP debe dedicarse a la revisión de los datos aportándoles el contexto necesario para que los datos tengan sentido para los interesados.

Propósito
Entender el significado de los datos obtenidos y facilitar a los interesados el contexto necesario para saber lo que se ha de hacer con la información. En una configuración ideal, los interesados sabrán cómo funcionan los indicadores fundamentales de rendimiento (IFR), cuáles son los factores que han influido en ellos durante el periodo considerado, y podrán reconocer la tendencia de cada IFR.

***Resultado**: Los datos históricos se conservarán y compararán con el rendimiento presente para identificar las tendencias.*

Subfunción 1.7.3.1 Análisis y revisión de los datos

El EIISP deberá invertir tiempo y esfuerzos en revisar los datos obtenidos y definir su contexto al elaborar los informes correspondientes.

Subfunción 1.7.3.2 Análisis de las tendencias de datos y el rendimiento histórico

Cuando se obtienen datos históricos se pueden identificar tendencias puntuales o crónicas que el EIISP o sus socios pueden corregir.

Subfunción 1.7.3.3 Determinación del contexto de los datos

Se han de poner los datos dentro de su contexto para que los interesados puedan entenderlos adecuadamente y definir cómo resolver problemas o inquietudes.

Función 1.7.4 Comunicación de los datos a los interesados

Una vez recopilados y analizados, se han de presentar los datos a los interesados en el formato acordado. El formato puede considerarse un instrumento o manera de presentar los datos de la manera más adaptada al interesado. Estos instrumentos pueden ser páginas web, correos-e, informes formales, etc.

Propósito
Los datos han de comunicarse a los interesados en un formato que les sea útil para conocer y entender el rendimiento del EIISP a la hora de prestar servicios. Estos datos han de ser comprensibles y situarse dentro de un contexto suficiente para que los interesados tomen decisiones en función de ese rendimiento.

Resultado
Se comunican a los interesados los datos en el formato adecuado y dentro de los plazos acordados.

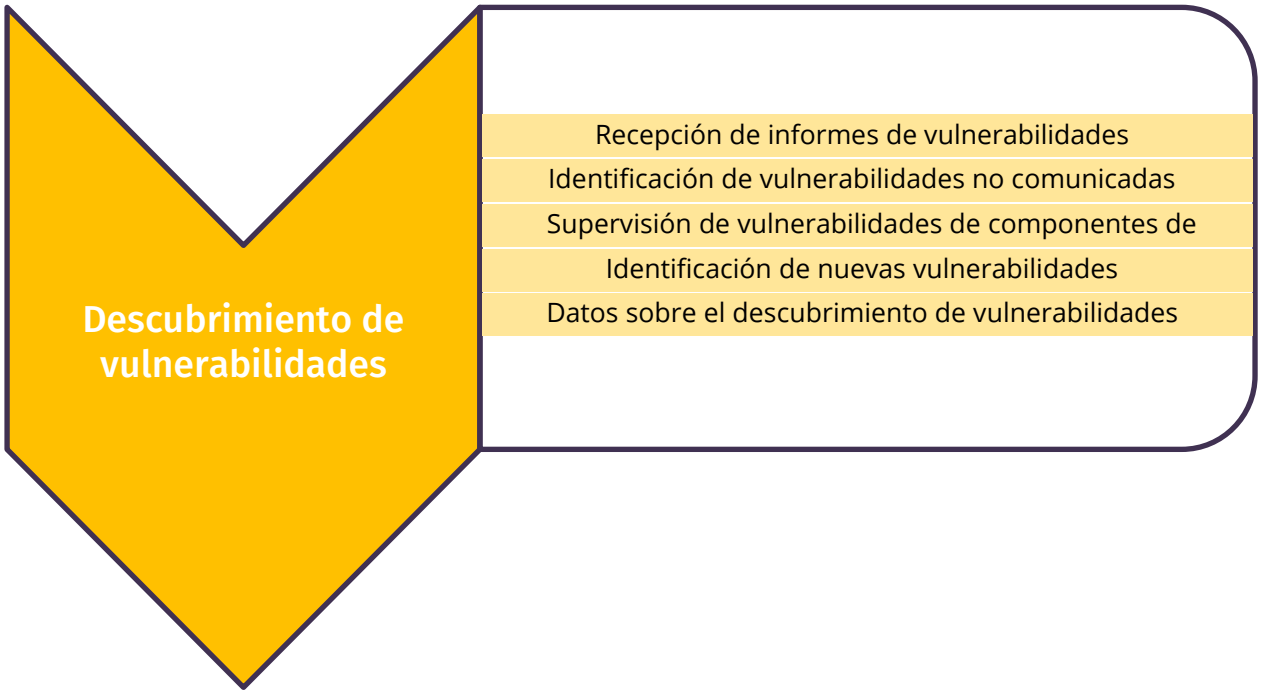
Subfunción 1.7.4.1 Presentación de instrumentos de datos a los interesados

Cada interesado tiene su propia perspectiva, a la que es necesario responder con datos, presentándolos con el formato adecuado. Los instrumentos de presentación de datos podrán ser distintos en función de las diversas perspectivas y pueden ser correos electrónicos, publicaciones en páginas web, portales web dinámicos, informes ejecutivos, gráficos, diagramas o cualquier otro medio de presentación.

Subfunción 1.7.4.2 Examen de los datos y lecciones extraídas

Uno de los principales objetivos del EIISP es mejorar constantemente el proceso de gestión de vulnerabilidades. La revisión de los datos de rendimiento y la retroinformación de los interesados ayuda al EIISP a identificar las esferas prioritarias o que se deben mejorar.

Esfera de servicio 2



En esta esfera de servicio se describen los servicios y funciones que un EIISP puede realizar para descubrir posibles vulnerabilidades. A esta esfera de servicio pertenece el tratamiento de vulnerabilidades descrito en otras secciones de este documento. La madurez de un EIISP puede medirse a través de la disponibilidad y eficacia de los distintos servicios prescritos para esta esfera de servicio.

Propósito
Establecer procesos y mecanismos de recopilación de información sobre las vulnerabilidades de los productos, los componentes de terceros vulnerables o las debilidades arquitectónicas de distintas procedencias.

Resultado
Mejorar el conocimiento de la situación en relación con los informes y posibles vulnerabilidades que exigen la intervención de los interesados.

Servicio 2.1 Recepción de informes de vulnerabilidades

Los EIISP sirven principalmente para recibir informes relativos a los productos de los interesados. Para recibir informes de vulnerabilidades lo más importante es crear y mantener la infraestructura necesaria, definir y dar a conocer quiénes son las personas de contacto y definir y mantener la preparación necesaria.

Propósito
Definir los procesos y mecanismos que permitirán a una entidad dar fácilmente cuenta de las vulnerabilidades en los productos de los interesados y mantener la preparación del EIISP en caso de recepción de un informe de vulnerabilidad.

Resultado
Preparación del EIISP para la recepción profesional de informes de vulnerabilidades.

Función 2.1.1 Garantizar la accesibilidad

Los EIISP deben dar a conocer su existencia y disponibilidad a las partes externas o indicar cuáles son las vías de comunicación internas. Disponer de un canal de comunicación claro y definido puede ser útil para los buscadores, socios o interesados a la hora de comunicar vulnerabilidades a los EIISP.

Propósito
Permitir a las entidades interesadas en comunicar vulnerabilidades encontrar fácilmente la información de contacto necesaria y el medio de comunicación preferido.

Resultado
Recibir un mayor número de informes y evitar que se diga que el EIISP no estaba disponible para aceptar informaciones sobre vulnerabilidades.

Subfunción 2.1.1.1 Definición del formato de presentación de informes preferido

Se prevé que la información sobre vulnerabilidades se reciba por distintos canales y con grados de calidad variables. Aun así resulta útil definir la mejor manera de procesar un informe. Puede tratarse de formularios web, sistemas de partes de incidencia públicos, direcciones de correo-e, servicio de asistencia telefónica, etc.

Subfunción 2.1.1.2 Publicación de datos de contacto

La información de contacto del EIISP debe figurar en la documentación del producto y en la página web de la empresa; debe estar indexada en los motores de búsqueda y registrada en las principales listas de EIISI/EIISP; debe comunicarse a las entidades expendedoras de enumeración de vulnerabilidades comunes (CVE), como las autoridades de numeración CVE (CNA), y debe darse a conocer a las comunidades de seguridad.

Subfunción 2.1.1.3 Registro de puntos de contacto comunes

Conviene reservar los términos comunes relativos al EIISP, como "eiisp@", "incidentes@" o "seguridad@" dentro del nombre de dominio de la empresa en cuestión. Esto ayudará a comunicar directamente al EIISP la información pertinente.

Subfunción 2.1.1.4 Conexión del EIISP dentro de la empresa

Verificar que el servicio de interesados (para las solicitudes o informes de vulnerabilidades de los interesados), el departamento de comunicaciones (para las preguntas de los medios de comunicación) y los equipos de producción (para la comunicación interna de descubrimientos) conocen el EIISP y saben cómo ponerse en contacto con él.

Subfunción 2.1.1.5 Definición y mantenimiento de la preparación

En función del sector y de los requisitos definidos por los interesados, establecer un servicio a la demanda o ininterrumpido para estar convenientemente preparado para responder a informes críticos.

Subfunción 2.1.1.6 Preparación para comunicaciones encriptadas

Los informes de vulnerabilidades suelen contener información sensible sobre el entorno operativo y los productos en los que se ha observado la vulnerabilidad. Para evitar fugas o revelaciones accidentales de información, conviene fomentar la presentación de informes encriptados, como correos-e con protección S/MIME o PGP o formularios web en formato HTTPS.

Función 2.1.2 Tratamiento de informes de vulnerabilidades

Los informes de vulnerabilidades proceden de distintas fuentes y tienen diferentes formatos. Es fundamental supervisar periódicamente los canales de comunicación entrantes y responder puntualmente a los informes recibidos. Los plazos de respuesta a los buscadores externos deben definirse en SLA confidenciales de la empresa.

Propósito
Facilitar procesos y mecanismos para la recepción de informes de vulnerabilidades procedentes de otras partes de la empresa, de interesados y de terceros (buscadores, otros EIISP, EIISI, etc.).

Resultado
Tratamiento profesional de los informes de vulnerabilidades procedentes de terceros.

Subfunción 2.1.2.1 Supervisión de los canales de comunicación

Verificar periódicamente los medios de contacto con el EIISP anunciados, así como otros canales, como las bandejas de entrada de correo-e generales o las cuentas de medios sociales de la empresa.

Subfunción 2.1.2.2 Tratamiento aislado de informes

El EIISP estudiará los informes de vulnerabilidades, por lo que se convertirá en un objetivo fácil de alcanzar mediante una comunicación maligna. Deberán prepararse políticas y procedimientos técnicos de protección del entorno de trabajo contra esos ataques que ofrezcan una manera segura de procesar los informes de vulnerabilidades.

Subfunción 2.1.2.3 Acuse de recibo puntual de los informes

Analizar detalladamente un informe suele ser un proceso complejo y cronófago, pero es fácil acusar recibo del informe. La prontitud en la respuesta muestra que el informe se toma en serio y contribuye en gran medida a crear una relación de confianza. Toda comunicación posterior a lo largo del procesamiento puede basarse en este primer compromiso y muestra que el EIISP se compromete a resolver el problema.

Servicio 2.2 Identificar vulnerabilidades no comunicadas

Las vulnerabilidades reveladas directamente al fabricante o procedentes de otras partes pueden recibirse directamente. Sin embargo, es importante ser consciente de que hay otras vulnerabilidades que pueden revelarse por medios informales, como boletines de noticias, blogs técnicos, bases de datos de expertos, medios sociales o publicaciones y conferencias técnicas.

Propósito
Mantenerse al día de la situación, reducir los plazos de detección de las amenazas que acechan a los productos de los interesados y reducir las posibilidades de revelación pública de la información.

Resultado
Mejor conocimiento de las amenazas de seguridad que acechan a la cartera de productos de los interesados.

Función 2.2.1 Supervisión de las bases de datos de explotación

Se han de supervisar activamente las bases de datos de explotación públicas y las líneas de información comerciales para descubrir posibles vulnerabilidades del día cero que requieran una investigación. Una supervisión plenamente funcional puede dar pie a establecer una comunicación proactiva entre la empresa y sus interesados.

Propósito
Descubrir vulnerabilidades nunca comunicadas por los canales oficiales.

Resultado
Mejor conocimiento de la existencia de la explotación de vulnerabilidades en el mercado.

Función 2.2.2 Seguimiento de programas de conferencias

Se debe hacer un seguimiento de las conferencias de seguridad pertinentes para mantenerse informado de las comunicaciones interesantes. Además de referirse directamente a productos o marcas, esas comunicaciones pueden abordar temas más amplios, como los fallos de protocolos que puedan requerir la intervención de los EIISP. Si el resumen plantea dudas, convendría ponerse rápidamente en contacto con el buscador para saber si es necesario tomar medidas al respecto. Además, la asistencia a las conferencias y la colaboración proactiva con los autores puede fomentar que se contacte directamente con el EIISP en el marco de futuras investigaciones.

Propósito
Evitar sorpresas por revelaciones no coordinadas o identificar fallos que podrían afectar directa o indirectamente a productos de los interesados que los autores aún no hayan considerado.

Resultado
Oportunidad para contactar activamente con los autores antes de la publicación para aclarar si los productos de los interesados se ven afectados o si ha habido problemas con la presentación de los informes.

Función 2.2.3 Seguimiento de las publicaciones de buscadores reputados

Prestar atención a las publicaciones de buscadores que ya hayan publicado informes relevantes o tengan una amplia experiencia en la industria o en relación con los productos y servicios de una empresa concreta. En artículos científicos, blogs o listas de correo pueden encontrarse pistas sobre vulnerabilidades o puntos débiles que requieran atención.

Propósito
Mantenerse al día, desde un punto de vista técnico y científico, de los temas de seguridad pertinentes para los interesados.

Resultado
Ganar experiencia en materia de amenazas comunes, vulnerabilidades y las posibles medidas correctivas para ayudar a los interesados a resolver problemas de seguridad de los productos.

Función 2.2.4 Seguimiento de los medios de comunicación

Los medios de comunicación suelen ser los primeros en dar cuenta de los incidentes que afectan a las instalaciones o el personal de los interesados, sobre todo cuando las consecuencias son catastróficas. Un seguimiento de los medios de comunicación puede ayudar a detectar problemas cuando los interesados del EIISP pueden ser proveedores importantes o predominantes.

Propósito
Refutar que la vulnerabilidad de un producto ha causado el incidente.

Resultado
Mejor preparación en caso de que los interesados o los medios se interesen por las vulnerabilidades del producto que puedan haber causado el incidente.

Servicio 2.3 Supervisión de las vulnerabilidades de componentes de productos

Las vulnerabilidades pueden clasificarse en tres grandes categorías: 1) vulnerabilidades del código fuente de un producto, 2) vulnerabilidades de los componentes de un producto cuyo mantenimiento depende del fabricante, y 3) vulnerabilidades de los componentes suministrados por fuentes externas (terceros). Desde el punto de vista de los productos, las categorías 2) y 3) atañen a componentes externos, pero las vulnerabilidades de esos componentes pueden, en último término, afectar al producto en que se integran. Aunque el propietario de un producto sólo puede controlar indirectamente la solución del problema subyacente, el interesado considera que hay un cierto grado de responsabilidad sobre la cadena de producción y la solución de la vulnerabilidad del producto afectado, en particular cuando el componente vulnerable no puede arreglarse con independencia del producto en el que se integra. Los componentes de código abierto también se consideran componentes de terceros.

Propósito
Identificar, conocer y supervisar las vulnerabilidades de la cadena de producción de los productos de los interesados, y notificar a los equipos de producción las vulnerabilidades que afectan a sus productos.

Resultado
Mejor conocimiento de la identificación temprana de vulnerabilidades de las cadenas de producción que afectan a los productos de los interesados.

Función 2.3.1 Inventario de componentes de productos

Mantener una lista de fabricantes, productos y versiones suministrados por partes internas y externas integrados en los productos. Resulta fundamental para identificar rápidamente los productos afectados por vulnerabilidades heredadas.

Propósito
Identificar los productos con componentes vulnerables que pueden causar vulnerabilidades en el producto mismo.

Resultado
Inventario completo de los materiales de todos los productos para la detección de componentes de productos vulnerables.

Función 2.3.2 Supervisión de avisos de terceros

Obtener puntualmente la información sobre vulnerabilidades de componentes de terceros mediante la suscripción a los avisos de los fabricantes o estableciendo canales de comunicación específicos con los proveedores. Suscripción a las listas de correo de seguridad de los proyectos de código abierto. Puede recurrirse a proveedores de información sobre vulnerabilidades.

Propósito
Identificar vulnerabilidades en componentes de terceros que pueden causar vulnerabilidades en los productos de los interesados.

Resultado
Poder iniciar el proceso de tratamiento de vulnerabilidades antes de que se reciba un informe externo sobre los productos afectados.

Función 2.3.3 Supervisión de las fuentes de información sobre vulnerabilidades

No siempre es posible suscribirse a los avisos de los fabricantes de componentes de terceros, por ejemplo porque el fabricante no emite avisos o ha cesado su actividad o por que la comunidad de código abierto del componente no es proactiva. Recursos como las bases de datos de vulnerabilidades nacionales (NVD) o las fuentes de información comerciales pueden ayudar a identificar las vulnerabilidades no comunicadas.

Propósito
Identificar en componentes de terceros vulnerabilidades que no se han comunicado.

Resultado
Mejor conocimiento de vulnerabilidades que no se habrían detectado de otra manera.

Función 2.3.4 Definición de procedimientos para la recepción de vulnerabilidades de la cadena de producción interna del fabricante

En la mayoría de los casos no se emitirán avisos públicos sobre los problemas de seguridad resueltos de componentes de productos internos del fabricante. Para obtener información sobre las vulnerabilidades de la cadena de producción interna del fabricante se deberán establecer canales de comunicación específicos con esos proveedores.

Propósito
Identificar vulnerabilidades de la cadena de producción interna del fabricante que causa vulnerabilidades en los productos de los interesados.

Resultado
Mejor conocimiento de las vulnerabilidades de la cadena de producción interna del fabricante que no se habrían detectado de otra manera.

Función 2.3.5 Notificación a equipos de producción internos

Establecimiento de canales automáticos para la distribución de notificaciones de vulnerabilidades de terceros identificadas directamente a los equipos de producción de los productos afectados. Generalmente basta con seguir las instrucciones de los fabricantes ascendentes para resolver el problema en el producto descendente. De acuerdo con la política de establecimiento de prioridades, hay que definir cuándo se clasificarán las vulnerabilidades de manera distinta y se remitirán al EIISP para su tratamiento. Esto último es particularmente importante si los interesados han de tomar medidas para obtener la versión corregida de los productos para asegurar el funcionamiento.

Propósito
Informar selectivamente a los equipos de producción acerca de las dependencias vulnerables y los parches (de haberlos) correctivos para la próxima emisión de productos.

Resultado
Reducir la necesidad de que el EIISP trate manualmente las vulnerabilidades, pues la información de terceros puede procesarse directamente en la producción.

Servicio 2.4 Identificación de nuevas vulnerabilidades

Un EIISP puede participar activamente en el descubrimiento interno de nuevas vulnerabilidades a fin de resolver problemas de seguridad de los productos con una menor necesidad de gestionar las relaciones externas y posiblemente reducir la coordinación global necesaria. Esas actividades deben complementar las de verificación de seguridad que son parte del CPS. El EIISP puede efectuar evaluaciones de seguridad antes de la comercialización de los productos o durante la fase de mantenimiento, además de ofrecer su experiencia con las herramientas de pruebas de seguridad al departamento de investigación y desarrollo. Las vulnerabilidades detectadas a nivel interno que tengan consecuencias para los usuarios finales deberán tratarse como las vulnerabilidades detectadas a nivel externo y someterse asimismo a las fases de clasificación e información en coordinación con la emisión de las medidas correctivas.

Propósito
Detectar y solucionar vulnerabilidades de los productos antes de su descubrimiento a nivel externo.

Resultado
Experiencia, procedimientos y mecanismos para el descubrimiento interno de vulnerabilidades de los productos y posible reducción de las necesidades de coordinación.

Función 2.4.1 Evaluación de la seguridad de los productos

La evaluación de la seguridad de los productos consiste en intentar descubrir vulnerabilidades desconocidas hasta el momento. Para ello puede utilizarse una amplia gama de técnicas y herramientas, como las pruebas de penetración o los escáneres de vulnerabilidades. Estas técnicas de evaluación de la seguridad de caja gris/caja negra simulan un pirateo externo a la empresa utilizando una metodología según la cual el atacante tiene un conocimiento escaso o nulo del sistema que ataca.

Propósito
Detectar vulnerabilidades con mecanismos proactivos.

Resultado
Medidas de garantía de la calidad que complementan las de verificación de la seguridad del CPS.

Subfunción 2.4.1.1 Evaluación de la seguridad de los productos propios

Los resultados de una evaluación de la seguridad de los controles de seguridad de los productos propios pueden servir de gran ayuda a los creadores que busquen mejorar sus productos antes de su comercialización o durante la fase de preparación de una solución correctiva.

Subfunción 2.4.1.2 Evaluación de la seguridad de componentes de terceros

En el caso de los componentes obtenidos de terceros se recomienda efectuar una evaluación de la seguridad más profunda, además de aplicar los procedimientos de gestión de adquisiciones de orden general. Esto es particularmente necesario en el caso de los componentes esenciales a fin de garantizar una debida diligencia de alta calidad.

Función 2.4.2 Formación continua en herramientas de pruebas de seguridad

Tanto las entidades comerciales como las comunidades diseñan constantemente nuevos análisis de seguridad y herramientas ofensivas. El EIISP debe estar perfectamente al día de las herramientas disponibles, pues ello resulta útil para evaluar los productos, validar las conclusiones de buscadores externos o ayudar a los equipos de producción a escoger las herramientas adecuadas para sus pruebas internas.

Propósito
Dotar a los equipos de expertos cualificados con las competencias necesarias para utilizar herramientas complejas y dar asesoramiento al respecto.

Resultado
Aprovechamiento de las mejores herramientas disponibles.

Subfunción 2.4.2.1 Formación del personal del EIISP en herramientas de pruebas de seguridad

La formación del personal es fundamental para mantenerse al día de las herramientas de pruebas de seguridad disponibles. En *Servicio 6.3 Validación segura* se detalla la formación del personal del EIISP.

Servicio 2.5 Datos sobre el descubrimiento de vulnerabilidades

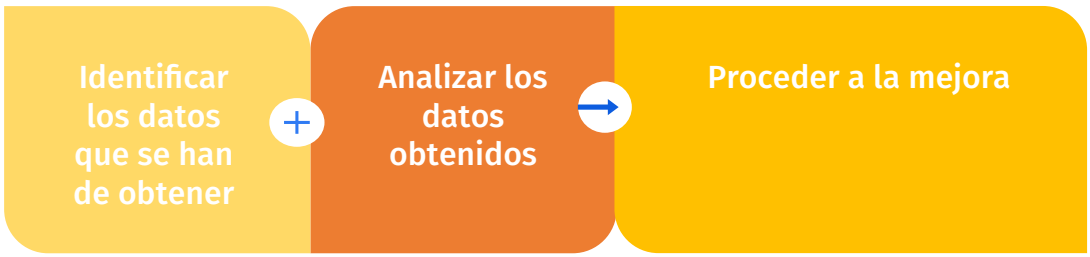


Figura 8: Procesamiento de datos sobre descubrimiento de vulnerabilidades

Para mantener a los interesados informados acerca de la eficacia del EIISP es fundamental facilitarles datos sobre su volumen y su rendimiento, entre otras cosas (véase también la *Sección III: Elementos operativos: Evaluación y mejoras)*. Cada interesado tiene un punto de vista al que se ha de responder con datos (u opiniones) en distintos formatos. El EIISP debe saber cómo desea cada grupo de interesados consumir esa información. Estos datos pueden ser los indicadores fundamentales de rendimiento (IFR) del EIISP.

Propósito
Ofrecer datos acerca del EIISP y su rendimiento que ayudan a los interesados a entender la eficacia del EIISP en relación con diversas esferas o servicios.

Resultado
Al consultar las métricas del EIISP, los interesados deben saber cómo el EIISP ofrece efectivamente un servicio y deben poder dar su opinión al respecto a fin de ajustar la prestación de ese servicio.

Función 2.5.1 Informes operativos

Los informes operativos contienen información sobre el volumen y los tipos de vulnerabilidades descubiertas. Estos informes pueden distribuirse periódicamente al EIISP y a los interesados internos.

Propósito
Obtener periódicamente datos para el informe general.

Resultado
Determinar las esferas que se han de analizar y que necesitan recursos y mejoras.

Subfunción 2.5.1.1 Relación entre vulnerabilidades descubiertas totales y confirmadas

Estos datos ayudan a conocer el volumen de casos tratados por el EIISP desde la perspectiva de los recursos. Estos datos pueden desglosarse por unidad comercial, tipo de producto o productos específicos.

Subfunción 2.5.1.2 Vulnerabilidades confirmadas totales desglosadas por componentes de terceros

Estos datos ayudan a conocer el riesgo asociado a cada componente de terceros específico.

Subfunción 2.5.1.3 Vulnerabilidades confirmadas totales desglosadas por CWE

Estos datos pueden revertirse al ciclo de producción segura e influir en la formación y capacitación. Estos datos pueden desglosarse por unidad comercial, tipo de producto o productos específicos.

Subfunción 2.5.1.4 Vulnerabilidades descubiertas totales desglosadas por método de descubrimiento

Gracias a estos datos se pueden identificar vulnerabilidades fáciles de detectar y revertirlas al ciclo de producción segura. Estos datos pueden desglosarse por unidad comercial, tipo de producto o productos específicos.

Subfunción 2.5.1.5 Vulnerabilidades descubiertas totales desglosadas por origen

Gracias a estos datos puede definirse el grado de popularidad del EIISP.

Función 2.5.2 Informe de gestión

Los informes de gestión contienen información sobre la calidad de la respuesta de la organización a las vulnerabilidades en términos de tratamiento y resolución de vulnerabilidades de seguridad.

Propósito
Definir una escala para determinar lo que la organización considera un éxito y obtener periódicamente datos para informar a la dirección acerca de la identificación de riesgos.

Resultado
Ilustración gráfica de los éxitos y los márgenes de mejora.

Subfunción 2.5.2.1 Tasa de puntualidad de la respuesta

Estos datos ayudan a conocer el rendimiento del EIISP en cuanto a respuesta inicial a los informes de vulnerabilidades dentro de los plazos fijados por los SLA correspondientes.

Subfunción 2.5.2.2 Tiempo total de indisponibilidad de los canales de comunicación del EIISP

Estos datos ayudan a conocer si la disponibilidad de los canales de comunicación del EIISP se ajustan a los SLA.

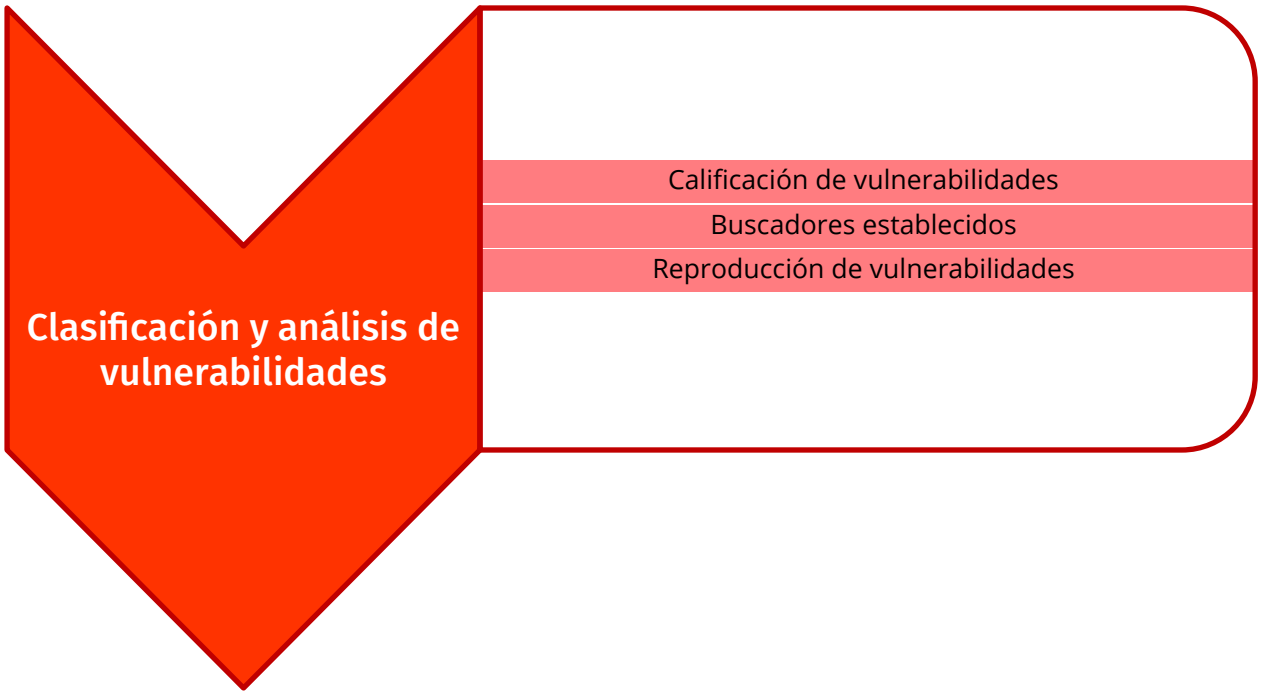
Subfunción 2.5.2.3 Tiempo medio de clasificación

Se mide aquí el tiempo transcurrido entre la recepción de un informe y la finalización de la clasificación. Se mide el rendimiento y/o la carga de trabajo del personal del EIISP.

Subfunción 2.5.2.4 Número de revelaciones, de vulnerabilidades explotadas y de vulnerabilidades identificadas por los medios de comunicación

Se mide el riesgo que corren los productos de los interesados.

Esfera de servicio 3 Clasificación y análisis de vulnerabilidades



La recepción y clasificación de vulnerabilidades es una de las funciones de gestión del EIISP. Si bien el orden en que se efectúan las operaciones es muy similar para todos los EIISP, puede haber variaciones en cuanto al momento exacto en que se inicia un "caso" o a las personas que ejercen las distintas funciones en relación con ese caso. Cuando las organizaciones reciban un gran volumen de informes de vulnerabilidad, podrán considerar la posibilidad de realizar una clasificación inicial a fin de validar los informes antes de iniciar los casos. Por el contrario, cuando el volumen de informes de vulnerabilidades sea bajo, los casos podrán crearse antes de su clasificación. El objetivo último de los EIISP es definir un proceso claro y eficiente.

Propósito
Definir la clasificación de los informes de vulnerabilidades.

Resultado
Definir el proceso que seguirán el EIISP y los equipos de ingenieros conexos.

Servicio 3.1 Calificación de vulnerabilidades

Las organizaciones definirán los criterios de calificación que se ajusten al tipo y ámbito de los problemas que desean resolver. Esos criterios de calificación ayudarán a definir la seguridad básica y a clasificar eficazmente los informes de vulnerabilidades entrantes.

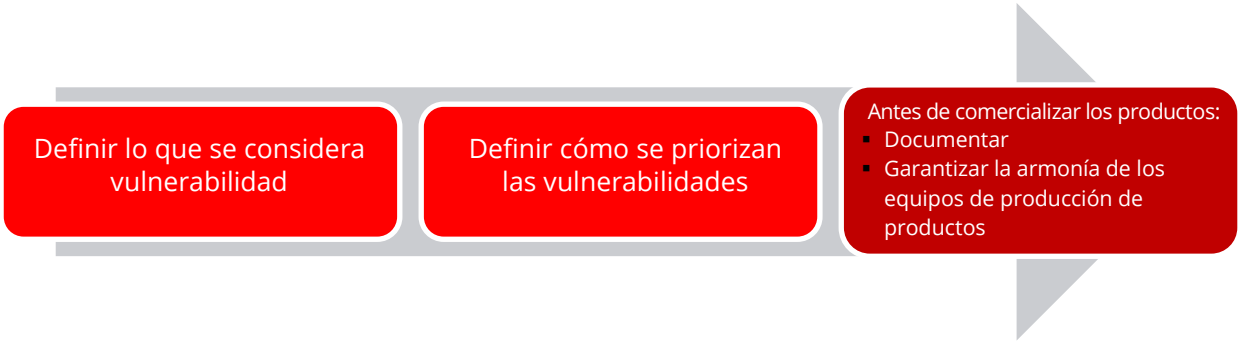


Figura 9: Proceso de calificación de vulnerabilidades

Función 3.1.1 Umbral de calidad y barras de errores

El sistema común de puntuación de la vulnerabilidad (CVSS) proporciona un modo de capturar las características principales de una vulnerabilidad y genera una puntuación numérica que refleja su gravedad. A continuación la puntuación numérica puede traducirse en una puntuación cualitativa (por ejemplo, baja, media y crítica) para que las organizaciones evalúen y prioricen adecuadamente sus procesos de gestión de vulnerabilidades, en ocasiones denominados umbral de calidad y/o barras de errores, que se utilizan para determinar los niveles mínimos aceptables de calidad de la seguridad, y los criterios de priorización de las vulnerabilidades de seguridad. La definición de esos criterios antes de la comercialización de los productos aporta transparencia al tratamiento de las vulnerabilidades al determinar con antelación lo que el EIISP considerará una vulnerabilidad de producto que se ha de remediar. Para aportar claridad al problema se suelen utilizar las vulnerabilidades y exposiciones comunes (CVE), una lista de entradas con un número de identificación, una descripción y al menos una referencia pública.

Propósito
Definir normas mínimas claras y criterios de priorización en pro de la transparencia de cara a los interesados internos y externos.

Resultado
Definir claramente lo que se considera vulnerabilidad para los ingenieros y buscadores. Los criterios de priorización evitarán confusiones y problemas a la hora de gestionar el ciclo de vida de la vulnerabilidad, desde la clasificación inicial a la comunicación de los parches.

Subfunción 3.1.1.1 Documentación de las definiciones de vulnerabilidades de seguridad de los productos

Es necesario documentar y almacenar de manera centralizada el umbral de calidad o las barras de errores, y que sean parte de la formación habitual de los creadores/ingenieros.

Subfunción 3.1.1.2 Implicación de los equipos de producción de productos

Cuando una organización cuente con múltiples productos y equipos de producción, es fundamental implicarlos a todos en la formulación de la definición de vulnerabilidad de seguridad del producto.

Función 3.1.2 Mejora constante

Un EIISP maduro debe procurar mejorar constantemente y revisar sus criterios de calificación, siempre que proceda, a fin de incorporar la experiencia adquirida, las prácticas idóneas de la industria, la evolución de los productos y la retroinformación de los interesados. Para gestionar las expectativas de los interesados internos y externos es importante comunicarles todos los cambios realizados.

Propósito
Reconocer que los criterios de calificación pueden revisarse. Es muy probable que los elementos dinámicos del EIISP, a saber, las expectativas de los interesados, las tendencias de la industria o el volumen de vulnerabilidades comunicadas, den lugar a ajustes frecuentes.

Resultado
Unos criterios de calificación fluidos permitirán calificar eficazmente las vulnerabilidades.

Subfunción 3.1.2.1 Obtención de datos

Obtener datos sobre el proceso de clasificación, incluidos el número de informes recibidos, cuántos de ellos se consideran vulnerabilidades, cuántos no se consideran vulnerabilidades y toda discrepancia detectada.

Propósito
Lograr mejoras a partir de los datos.

Resultado
Los umbrales de datos y barras de errores se modifican en función de los datos.

Servicio 3.2 Buscadores establecidos

A medida que el EIISP de una organización madura, el equipo puede detectar que un grupo de buscadores habituales comunica un volumen de vulnerabilidades por encima de lo normal. Se recomienda estudiar la reputación de los buscadores y el historial de comunicaciones de alta calidad a fin de poder obviar algunas fases, como la calificación y la clasificación, y pasar directamente a analizar las causas primeras y proceder a la resolución del problema. De este modo se puede aumentar la eficacia del proceso y estrechar las relaciones con los buscadores.

Propósito
Conocer a la comunidad investigadora y a los que con más frecuencia informan de vulnerabilidades de los productos y servicios, y considerar la posibilidad de aceptar inmediatamente los informes de buscadores muy fiables.

Resultado
Reducir el tiempo de respuesta cuando la información procede de buscadores muy fiables.

Función 3.2.1 Base de datos de buscadores

Crear y mantener una base de datos de personas y organizaciones que comunican vulnerabilidades a fin de disponer de un registro cronológico, hacer un inventario de los resultados y demás consideraciones en relación con los buscadores.

Propósito
Aumentar la eficacia del proceso de clasificación y mejorar las relaciones con los buscadores con un historial de informes de calidad.

Resultado
Los informes de buscadores cualificados pasan más rápido por el sistema. Los buscadores están satisfechos con los resultados y se encuentran soluciones antes de que el problema pueda hacerse público.

Función 3.2.2 Tratamiento acelerado de la información procedente de buscadores establecidos

Algunos buscadores pueden ser prolíficos o coherentes (credibilidad contrastada) a la hora de encontrar errores en el *software* de los productos y servicios y dar cuenta de ellos. Por ejemplo, pueden utilizar herramientas de *fuzzing* comunes e informar acerca de fallos sin demostraciones escritas o conceptuales concretas. Cuando se conoce bien al buscador y se determina que la mayoría de problemas que comunica han necesitado una intervención, puede considerarse la posibilidad de obviar la fase de calificación/contrastación y pasar directamente a la solución.

Propósito
Aumentar la eficacia del proceso de clasificación y mejorar las relaciones con los buscadores con un historial de informes de calidad.

Resultado
Los informes de buscadores cualificados pasan más rápido por el sistema. Los buscadores están satisfechos con los resultados y se encuentran soluciones antes de que el problema pueda hacerse público.

Función 3.2.3 Perfil de buscador

Se pueden definir los perfiles de los buscadores para que los encargados del tratamiento de los errores sepan cómo trabajar con ellos. En los perfiles se pueden incluir datos como la ubicación geográfica, los idiomas hablados, las conferencias en que han intervenido, los métodos empleados para encontrar vulnerabilidades, los productos/tecnologías en que se suelen centrar, si suelen coordinar la revelación de vulnerabilidades, si prefieren presentar sus hallazgos en conferencias, si se les ofrecen recompensas u otro tipo de incentivos, etc. Es necesario consultar con los equipos jurídico y/o de conformidad qué tipo de información se puede obtener y durante cuánto tiempo se puede conservar.

Propósito
Conocer a las personas que encuentran vulnerabilidades en los productos.

Resultado
A fin de conseguir los mejores resultados, el tratamiento puede personalizarse para buscadores específicos.

Función 3.2.4 Definición de la calidad de los informes de buscadores

Es posible que las organizaciones deseen definir y publicar directrices acerca de la calidad mínima que ha de poseer un informe de vulnerabilidades a fin de orientar a los buscadores sobre el tipo de información que se necesita para evaluar rápidamente los informes. Como mínimo puede incluirse, aunque no únicamente, una explicación escrita, la definición de las fases de reproducción, las plataformas probadas y una prueba conceptual.

Propósito
Ofrecer a los buscadores unas directrices sobre la calidad mínima exigida para los informes de vulnerabilidades.

Resultado
Se minimizan las interacciones entre fabricantes y buscadores y los fabricantes pueden proceder rápidamente a encontrar una solución.

Servicio 3.3 Reproducción de vulnerabilidades

A menos que se especifique lo contrario, además de la calificación, el EIISP debe asegurarse de que el informe del buscador es reproducible a fin de validar y entender las condiciones que han dado lugar a la vulnerabilidad.

Propósito
Ofrecer las herramientas y el contexto necesarios para calificar los informes de vulnerabilidades.

Resultado
Validación de informes de vulnerabilidad eficaz, segura y protegida.

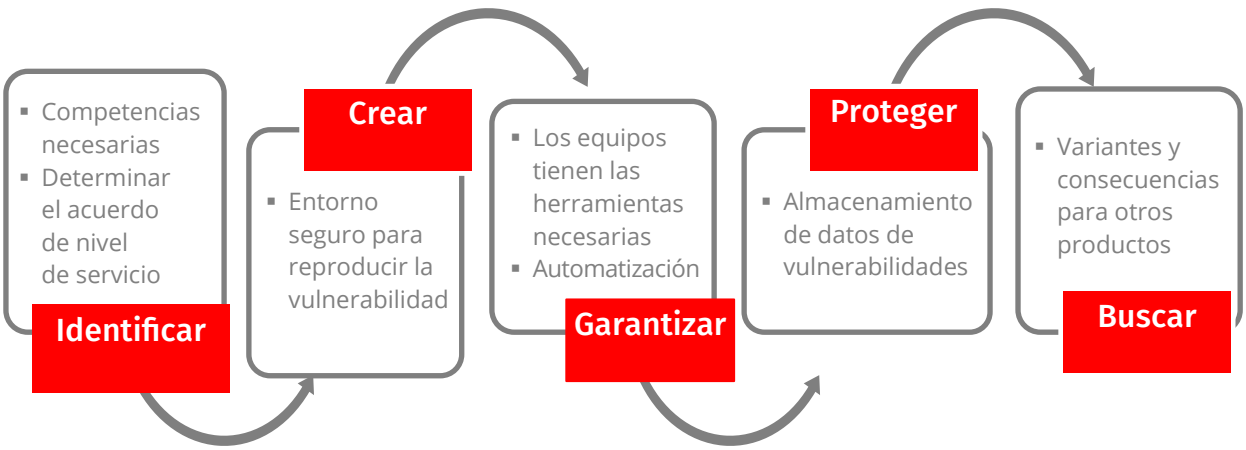


Figura 10: Verificación/reproducción de vulnerabilidades

Función 3.3.1 Concluir acuerdos de nivel de servicio para la reproducción de vulnerabilidades

Es posible que el EIISP no disponga del nivel técnico suficiente para reproducir todas las vulnerabilidades comunicadas. El EIISP podrá tener que consultar y colaborar con otros

equipos, o depender de su experiencia en materia de creación de productos, por lo que es importante disponer de un acuerdo claramente armonizado y definido para garantizar que se dispone de los conocimientos necesarios. En una configuración ideal se recomienda contar con un experto a tiempo completo o parcial. Sin embargo, si por motivos presupuestarios no fuera posible, como mínimo se preidentificarán los expertos que pueden participar en el proceso del EIISP con rapidez y durante periodos limitados de tiempo en caso de incidente.

Propósito
Reconocer que el EIISP no dispone de los conocimientos técnicos necesarios para reproducir todas las vulnerabilidades comunicadas.

Resultado
La armonización interna garantizará que los expertos están disponibles cuando sea necesario para reproducir vulnerabilidades.

Función 3.3.2 Entorno de pruebas de reproducción

El EIISP o el equipo designado deberán configurar el entorno de prueba específico para reproducir la vulnerabilidad. El entorno de prueba debe estar aislado para evitar las actividades malignas y validar el informe del buscador. Siempre que proceda se podrán emplear entornos de red ex profeso, simulaciones o virtualizaciones para crear un entorno seguro.

Propósito
Crear un entorno seguro que permita la inspección y reproducción de vulnerabilidades.

Resultado
Un entorno de pruebas de reproducción bien configurado facilitará el proceso y permitirá calificar eficazmente las vulnerabilidades, restringiendo al mismo tiempo la vulnerabilidad al alcance del entorno de prueba.

Función 3.3.3 Herramientas de reproducción

Los equipos implicados en la reproducción de vulnerabilidades comunicadas necesitan herramientas y licencias de productos actualizadas para efectuar esa operación (por ejemplo, un depurador).

Propósito
Garantizar que los equipos de reproducción tienen las herramientas necesarias.

Resultado
Garantizar que la reproducción de vulnerabilidades comunicadas es lo más eficaz posible.

Función 3.3.4 Almacenamiento de vulnerabilidades

Se recomienda almacenar la información sensible, como los informes de vulnerabilidades, ficheros de pruebas conceptuales, etc., de manera segura y que sólo tengan acceso a ella aquéllos que la necesiten, además de garantizar la seguridad de la información cuando se transmite y cuando no se está utilizando. Por ejemplo, véase ISO 27001.

Propósito
Mantener segura la información sobre vulnerabilidades sensible y potencialmente peligrosa.

Resultado
Se mantiene segura la información sensible, limitando su acceso y las posibilidades de que ponga en peligro la red primaria de la organización.

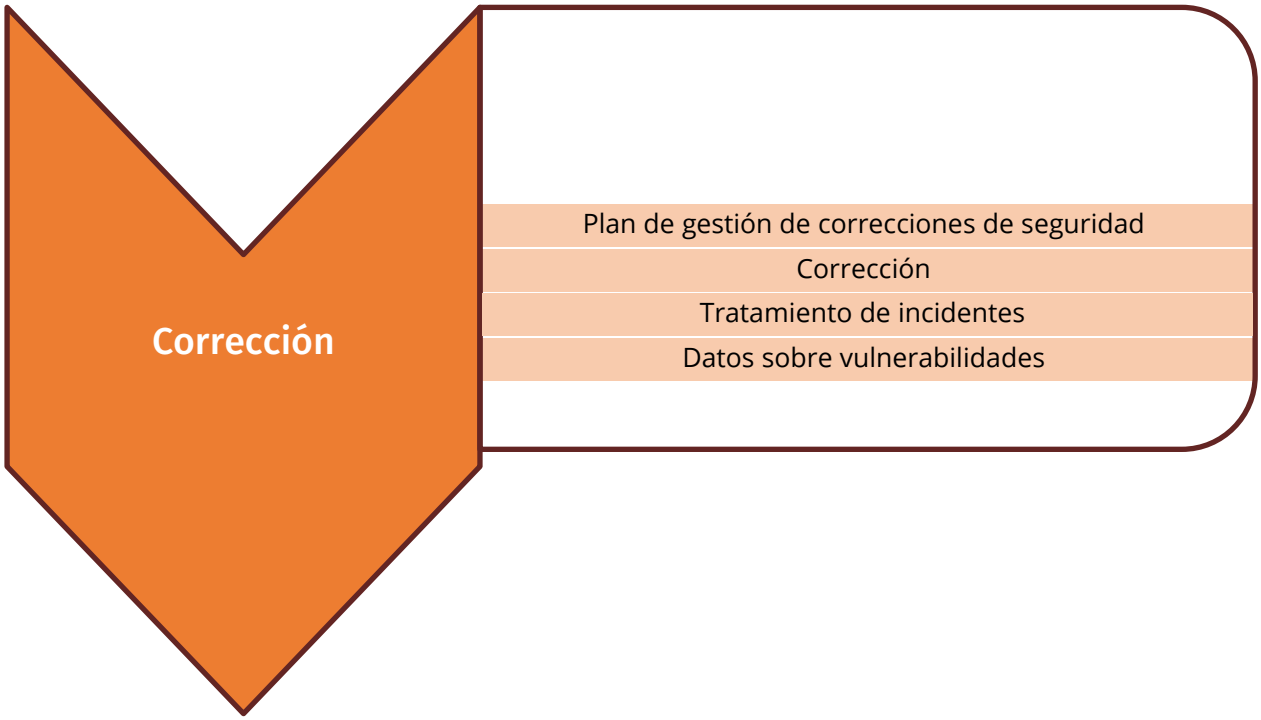
Función 3.3.5 Productos afectados

Durante la reproducción, el equipo que realiza el análisis debe procurar determinar qué productos se ven afectados y si existen variantes de la vulnerabilidad. Véase también la *Sección 4.1.1 Gestión del ciclo de vida de los productos*.

Propósito
Comprender perfectamente las vulnerabilidades y su alcance en los productos.

Resultado
La vulnerabilidad se solucionará en todos los productos afectados.

Esfera de servicio 4



Esta esfera de servicio comprende los distintos servicios necesarios para anunciar y facilitar soluciones correctivas a los interesados y fabricantes descendentes. El mecanismo de entrega de soluciones correctivas dependerá de las consecuencias que tenga la explotación de la vulnerabilidad para los interesados. Se han de definir procesos para garantizar que las correcciones se entregan de acuerdo con un calendario establecido a fin de que los interesados y fabricantes descendentes puedan planificar convenientemente las pruebas y la aplicación de esas correcciones.

Propósito
Resaltar los procesos y mecanismos necesarios para anunciar y facilitar soluciones correctivas a los interesados y fabricantes descendentes.

Resultado
Permitir a los interesados y fabricantes descendentes planificar convenientemente sus acciones en relación con las correcciones.

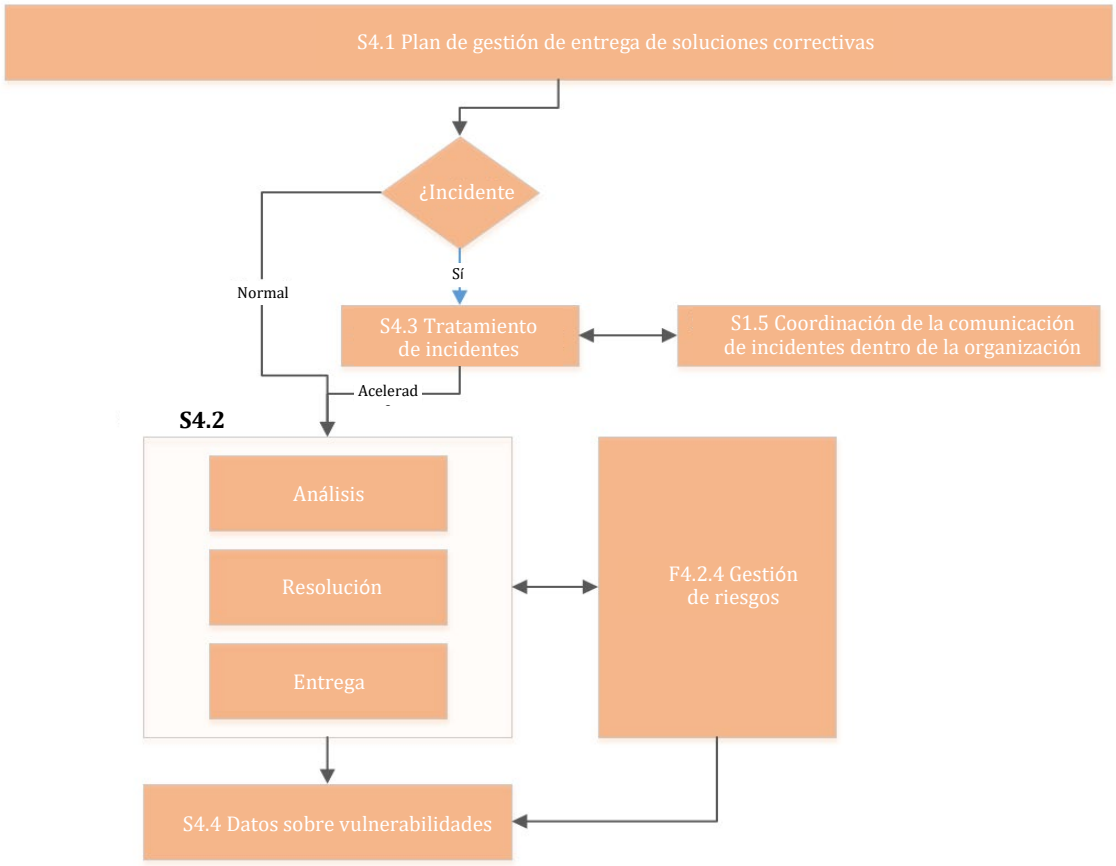


Figura 11: Ejemplo de proceso de entrega de soluciones correctivas

Servicio 4.1 Plan de gestión de entrega de soluciones correctivas

Este servicio se centra en ofrecer orientaciones sobre cómo el fabricante planifica la cadencia de entrega de una solución correctiva para las versiones afectadas del producto comercializado. Los interesados, sobre todo dentro de la empresa, deben planear la aplicación de la corrección. Algunas aplicaciones, como la nube, pueden contar con actualizaciones automáticas o políticas de gestión de parches de otro tipo.

Propósito

Dar a conocer qué productos se soportarán, los mecanismos de entrega de correcciones y la cadencia a la que se irán entregando.

Resultado

Los interesados podrán planificar con antelación la aplicación de soluciones de seguridad.

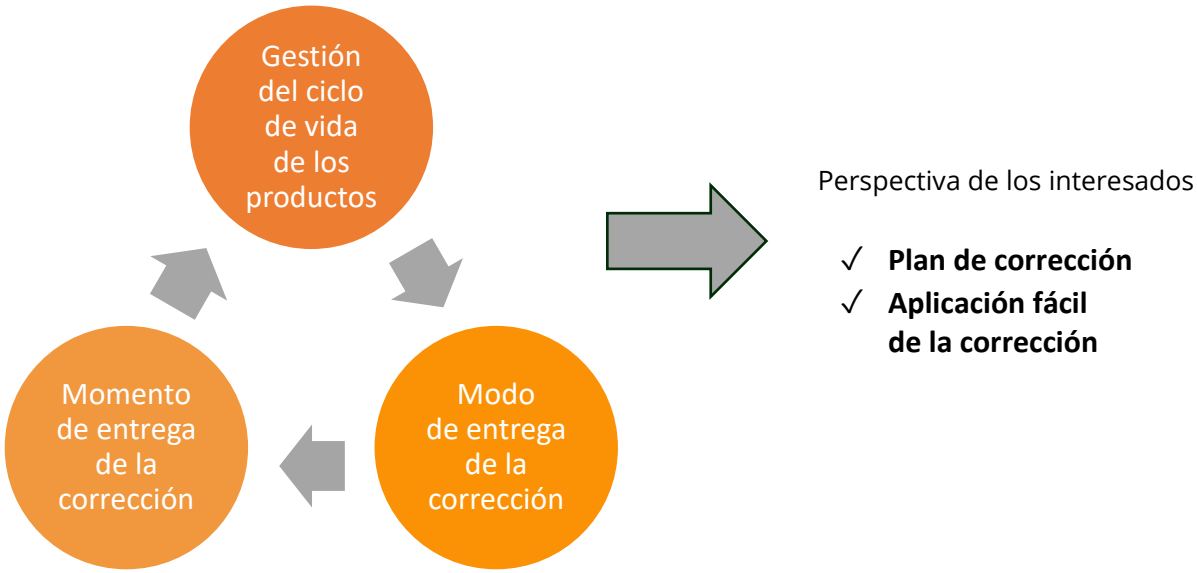


Figura 12: Bases para la coherencia

Función 4.1.1 Gestión del ciclo de vida de los productos

Las empresas pueden definir diversas políticas y acuerdos de asistencia a los interesados en función de los cuales el EIISP podrá asociarse con unidades/líneas de producción y de ayuda al interesado para determinar si se seguirá dando mantenimiento a los productos de las obligaciones contraídas y cómo se hará. Esto dependerá de la gravedad de las vulnerabilidades y puede implicar a las unidades/líneas de producción y de ayuda al interesado.

Propósito
Define para los equipos de productos una política clara sobre cómo la organización dará soporte a los productos con vulnerabilidades de seguridad.

Resultado
Política clara sobre las expectativas de las unidades/líneas de producción a la hora de ofrecer soluciones para esos productos.

Subfunción 4.1.1.1 Inventario de productos

Hacer un inventario de todos los productos comercializados para garantizar que se evalúan todos los productos correspondientes y se aportan las soluciones del caso.

Subfunción 4.1.1.2 Modelos de mantenimiento

Comprender los distintos tipos de mantenimiento de los productos, incluidos los servicios de pago, las extensiones de garantía y los acuerdos o contratos de mantenimiento con interesados concretos.

Subfunción 4.1.1.3 Ciclo de vida del producto

Determinar a partir de qué momento del ciclo de vida del producto se cesa su mantenimiento.

Función 4.1.2 Método de entrega

El EIISP puede asociarse con los equipos de productos y de ayuda a los interesados para identificar las diversas opciones de entrega de correcciones a los interesados. También deben definirse los criterios para determinar cuándo entregar la corrección por los medios identificados.

Propósito
Mantener un mecanismo coherente para entregar las correcciones de vulnerabilidades de acuerdo con unas condiciones predefinidas.

Resultado
Los interesados pueden planificar y aplicar fácilmente las correcciones.

Subfunción 4.1.2.1 Formatos de empaquetado de productos

Conocer los distintos formatos de empaquetado pertinentes para la entrega de correcciones (por ejemplo, ejecutable binario, distintos códigos fuente, etc.).

Subfunción 4.1.2.2 Entrega de correcciones

Conocer los distintos mecanismos de entrega y distribución de correcciones, por ejemplo, parche en caliente, parche, versiones de mantenimiento o actualización de *firmware*.

Subfunción 4.1.2.3 Aplicación de correcciones

Identificar cómo se puede aplicar la corrección en distintos productos, por ejemplo, a distancia, instalable por el cliente, actualización automática o intervención directa.

Función 4.1.3 Cadencia de entrega

Los interesados y fabricantes descendentes deben planificar las correcciones a fin de poder mantener la seguridad en su entorno. Al fijar una cadencia de entrega de correcciones, los interesados podrán planificar el tiempo y los recursos necesarios para actualizar convenientemente sus entornos.

Propósito
Mantener una cadencia coherente de entrega de correcciones a los interesados.

Resultado
Los interesados pueden planificar y aplicar las correcciones.

Subfunción 4.1.3.1 Cadencia de entrega de correcciones

Asociación con los equipos de gestión de productos y gestión de entregas para determinar la cadencia de entrega de las correcciones. Algunas correcciones se integran en las nuevas versiones publicadas y se ajustarán a su calendario. Otras deberán aplicarse con carácter urgente en lo que se consideran versiones fuera de banda.

Subfunción 4.1.3.2 Documentación de excepciones

Identificar y documentar las excepciones en que una corrección no se entrega siguiendo la cadencia normal.

Servicio 4.2 Corrección

Este servicio está relacionado con la gestión de vulnerabilidades comunicadas por los buscadores y comprende el análisis de respuesta, así como la mitigación, y define qué versiones se corregirán, pudiendo además tomar en consideración cómo se entregará esa corrección. También puede comprender las soluciones alternativas que el interesado puede aplicar inmediatamente, antes de que se le entregue la corrección.

Propósito
Definir los procesos y prácticas idóneas de entrega de correcciones a los interesados en función de los productos, versiones e interesados afectados.

Resultado
Corrección compatible con los productos afectados y las necesidades de los interesados.

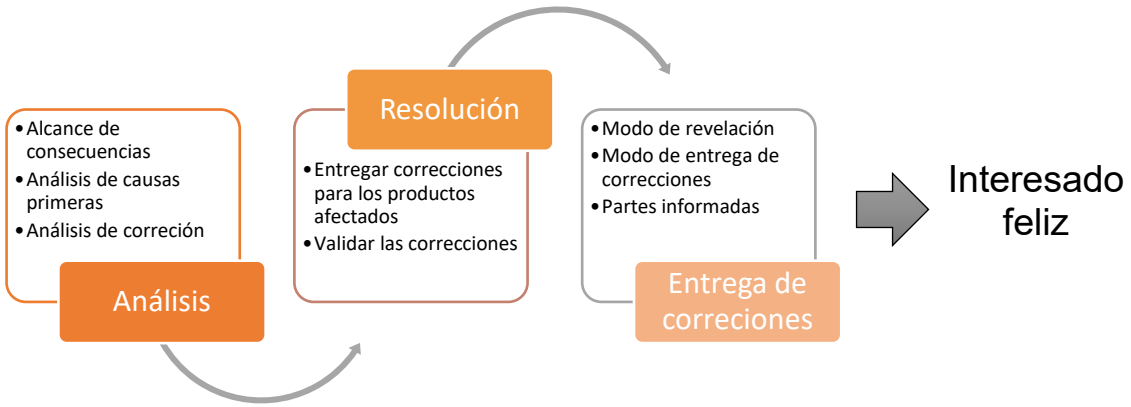


Figura 13: Proceso de corrección de vulnerabilidades comunicadas

Función 4.2.1 Análisis

Los productos afectados pueden contener una única aplicación de *software*, *firmware* o múltiples programas de *hardware* con distintas versiones de *software* o *firmware*. Se ha de

tener en cuenta una serie de parámetros a la hora de diseñar un plan de corrección para garantizar que se colman las necesidades de los interesados.

Propósito
Determinar los productos, las versiones y los interesados afectados.

Resultado
Corrección acorde con los productos afectados y las necesidades de los interesados.

Subfunción 4.2.1.1 Validación de vulnerabilidades

Validar el informe de vulnerabilidad o el incidente en función del umbral de calidad o la barra de errores. Véase la *Función 3.1.1 Umbral de calidad y barras de errores*.

Subfunción 4.2.1.2 Corrección de versiones de productos

Identificar los productos y versiones afectados, así como toda variante que se haya de corregir al mismo tiempo.

Subfunción 4.2.1.3 Revisión de los acuerdos de mantenimiento

Revisar los acuerdos y modelos de mantenimiento asociados a las versiones afectadas de los productos. Véase la *Subfunción 4.1.1.2 Modelos de mantenimiento*.

Subfunción 4.2.1.4 Análisis de causas primeras

Comprender el fallo de diseño o implementación que causa la vulnerabilidad.

Subfunción 4.2.1.5 Determinación del mecanismo de rechazo de vulnerabilidades

Por ejemplo, una vulnerabilidad puede ser un falso positivo o un fallo de diseño de la seguridad.

Subfunción 4.2.1.6 Análisis de correcciones

Determinar los medios para paliar o eliminar los riesgos generados por la vulnerabilidad.

Subfunción 4.2.1.7 Soluciones alternativas

Identificar las eventuales soluciones alternativas que pueden aplicarse para paliar la vulnerabilidad mientras se crea la corrección necesaria.

Subfunción 4.2.1.8 Excepciones

Identificar las excepciones en que no es posible corregir la vulnerabilidad. Véase la *Función 4.2.4 Proceso de gestión de riesgos.*

Función 4.2.2 Resolución de correcciones

Antes de entregar una corrección para una vulnerabilidad comunicada, es necesario validarla mediante garantías de calidad (QA), pruebas de seguridad y, si procede, el buscador que comunicó la vulnerabilidad. Se describen aquí el proceso y los mecanismos de validación interna de las correcciones y de asociación con los buscadores para validar y dar por buena la corrección.

Propósito
Definir un proceso y un mecanismo para validar a nivel interno la corrección y para la asociación con el buscador a fin de dar por buena la corrección, si procede.

Resultado
Aprobación por los buscadores internos y/o externos de la corrección que se va a entregar.

Subfunción 4.2.2.1 Validación de vulnerabilidades comunicadas que se han corregido

Validación para garantizar a todas las partes que se han corregido las vulnerabilidades comunicadas en todas las versiones de los productos afectadas.

Subfunción 4.2.2.2 Aprobación de correcciones

Obtener la aprobación de la corrección del ingeniero o equipo de QA responsable. La validación de las correcciones debe integrarse en los procesos de pruebas/QA normalizados.

Subfunción 4.2.2.3 Validación de correcciones por los buscadores

Asociación con buscadores o interesados terceros para validar las correcciones.

Función 4.2.3 Entrega de correcciones

En el contexto de la entrega de correcciones para vulnerabilidades comunicadas, los plazos de revelación pueden depender de las necesidades comerciales de la organización. Por ejemplo, en algunos casos la información puede divulgarse cuando las correcciones están disponibles, en otros casos la información puede divulgarse después de las correcciones, sobre todo si éstas se han facilitado por fases, y en algunos casos puede darse prioridad a la divulgación de acuerdo con las relaciones con los interesados (por ejemplo, socios o entidades críticos). En cualquier caso será necesario mantener informados de esos plazos a los principales interesados, incluidos los buscadores.

Propósito
La divulgación de la información se planifica de acuerdo con las correcciones y se mantiene informados a los interesados acerca de los plazos.

Resultado
Facilitar a los interesados una corrección al tiempo que se revela la vulnerabilidad.

Subfunción 4.2.3.1 Tipo de revelación

Determinar el mecanismo preferido para revelar las vulnerabilidades. Puede depender de la gravedad o el tipo de la vulnerabilidad.

Subfunción 4.2.3.2 Coordinación de la revelación, si procede

Subfunción 4.2.3.3 Publicación de correcciones en base de datos interna

Asociación con los equipos de asistencia a los interesados o con otros interesados para publicar las correcciones en el portal web, el sitio de asistencia a interesados o la remisión a manufactura (RTM), por ejemplo.

Subfunción 4.2.3.4 Divulgación de la correcciones

Asociación con los interesados o equipos de asistencia a los interesados para divulgar las vulnerabilidades comunicadas.

Función 4.2.4 Proceso de gestión de riesgos

Es responsabilidad del EIISP dar a los interesados información suficiente para que puedan evaluar los riesgos que para sus sistemas se derivan de las vulnerabilidades de los sistemas y productos de cuyo mantenimiento se ocupa la organización del EIISP. Cuando una vulnerabilidad no se corrige dentro de los plazos especificados (por los acuerdos de nivel de servicio o lo objetivos) se ha de evaluar la gestión de riesgos en toda la organización. Esto comprende un mecanismo de transparencia para cuantificar los riesgos y darlos a conocer a los interesados que figuran en el registro de riesgos de la organización.

Propósito
Definir un proceso para la aceptación formal de riesgos en caso de que las vulnerabilidades no se remedien de conformidad con los plazos prescritos por los SLA internos.

Resultado
Transparencia en la organización acerca de los riesgos y garantía de que éstos se reconocen y dan a conocer convenientemente.

Subfunción 4.2.4.1 Funciones de autoridad

Identificar las funciones con autoridad para aceptar riesgos, por ejemplo, jefe de seguridad informática/jefe de seguridad o gestor de riesgos, y las funciones a las que se ha de informar de los riesgos.

Subfunción 4.2.4.2 Definición del proceso de gestión de riesgos

Definir la gestión de riesgos en el marco del tratamiento y la respuesta a los riesgos dentro de la organización, incluidas las condiciones que activan el proceso.

Subfunción 4.2.4.3 Evaluación y cuantificación del riesgo

Evaluar y cuantificar los riesgos mediante una evaluación de riesgos para entender las amenazas para la empresa y sus consecuencias.

Subfunción 4.2.4.4 Documentación de riesgos en el registro de riesgos

Ayudar al jefe de seguridad, el gestor de riesgos u otros interesados a hacer un seguimiento de la evaluación de los riesgos y la correspondiente implementación de recomendaciones.

Subfunción 4.2.4.5 Recomendaciones

Actualizar el registro de riesgos con conclusiones y recomendaciones.

Servicio 4.3 Tratamiento de incidentes

El EIISP necesita un mecanismo para acelerar la corrección de "vulnerabilidades críticas", que pueden definirse como vulnerabilidades que se explotan, vulnerabilidades del día cero y revelaciones públicas no coordinadas. Este servicio ofrece orientaciones para el incidente, alerta a los interesados y coordina las actividades relativas a la respuesta a los incidentes, su mitigación y la recuperación posterior a fin de reducir los plazos necesarios para la entrega de correcciones.

Propósito
Elaborar un plan para gestionar vulnerabilidades críticas y poder movilizar todos los recursos necesarios para solucionarlas.

Resultado
Entrega de correcciones de emergencia antes o después de la revelación de una vulnerabilidad o en casos en que los interesados corren riesgos y es necesario intervenir con rapidez.

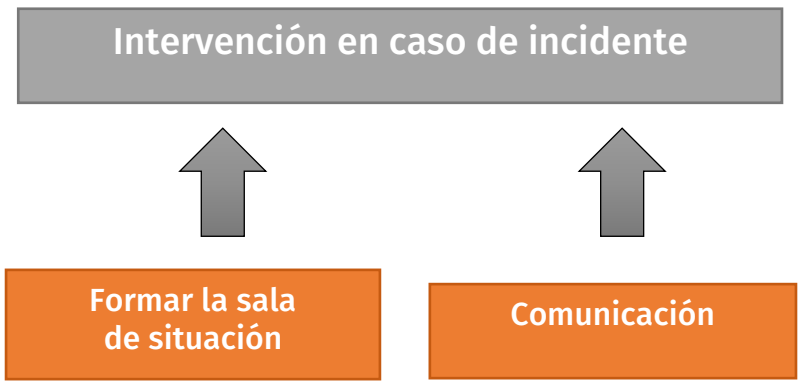


Figura 14: Tratamiento de incidentes

Función 4.3.1 Formar la sala de situación

Cuando sea necesario gestionar un incidente, deberá formarse una sala de situación en la que participen el EIISP y los departamentos necesarios, entre otros, por ejemplo, el jurídico, de comunicaciones, de producción, de asistencia a interesados y de proveedores. La sala puede ser física o virtual, siempre y cuando todas las partes puedan intervenir cuando sea necesario

de manera segura. Normalmente, para garantizar la asistencia de los interesados, la sala debe ser tanto física como virtual. A fin de llevar a cabo el proceso de gestión de incidentes adecuadamente, será necesario identificar los recursos con antelación.

Propósito
Garantizar que los interesados pueden responder a las preguntas planteadas y dar orientaciones. Garantizar que se han asignado a la gestión del incidente los recursos adecuados.

Resultado
Organización de recursos garantizados.

Subfunción 4.3.1.1 Plan de gestión de incidentes

Elaborar un plan para gestionar vulnerabilidades críticas y poder movilizar todos los recursos necesarios para solucionarlas. Es importante evaluar la preparación para intervenir en caso de incidente a fin de verificar la disposición de este plan para hacer frente a eventos inesperados y emergencias.

Subfunción 4.3.1.2 Identificación de los recursos necesarios para tratar y gestionar incidentes

Los recursos pueden incluir las salas de reunión, las líneas privadas y el personal adicional. Para las intervenciones prolongadas habrán de preverse alimentos y alojamiento.

Subfunción 4.3.1.3 Implicación de los interesados en el plan de intervención en caso de incidente

Identificar en el plan de intervención en caso de incidente a todos los interesados que deben participar en la intervención. Véanse *Servicio 1.1 Gestión de interesados internos* y *Servicio 1.5 Comunicación de incidentes.*

Subfunción 4.3.1.4 Asignación clara de funciones y responsabilidades para gestionar el incidente

El personal debe saber qué papel desempeña y conocer el orden de las operaciones en caso de intervención. Se impartirán formaciones y se efectuarán simulaciones teóricas para preparar a los participantes clave.

Función 4.3.2 Gestión de incidentes

En caso de incidente el principal objetivo del EIISP, en asociación con los interesados, es reducir las consecuencias de ese incidente y procurar restaurar las funciones comerciales del producto y de sus interesados.

Propósito
Preparar un libreto y ejecutar un plan para contener el incidente.

Resultado
Restaurar lo antes posible las operaciones de los equipos de productos y de los interesados.

Subfunción 4.3.2.1 Recopilación de información

Recepción, catálogo y almacenamiento de información relacionada con el incidente.

Subfunción 4.3.2.2 Análisis

La gestión de incidentes depende de las actividades de análisis que se definen en la sección "Análisis".

Subfunción 4.3.2.3 Intervención

Servicios para reducir las consecuencias de un incidente y trabajar en la recuperación de las funciones de la actividad del mandante.

Subfunción 4.3.2.4 Rastreo de incidentes

Documentación de información sobre las medidas adoptadas para resolver un incidente, incluidas la información crítica recopilada, los análisis realizados, las medidas de corrección y mitigación adoptadas, y el cierre y la resolución.

Subfunción 4.3.2.5 Proceso posterior al incidente

Examen posterior para determinar las mejoras que cabe aportar a los procesos, políticas, procedimientos y recursos, y herramientas para atenuar y prevenir futuros peligros.

Función 4.3.3 Plan de comunicación

Todos los interesados y participantes deben conocer los planes más recientes y su evolución para estar al día. Es necesario implicar a la dirección para eliminar todo obstáculo que se oponga a la comunicación colaborativa abierta en caso de incidente.

Propósito
Preparar un plan de comunicación y designar a una persona de contacto que comunique a todos los interesados las informaciones actualizadas.

Resultado
Organizar comunicaciones contrastadas.

Subfunción 4.3.3.1 Publicación de información a los interesados internos

Gestión de listas utilizadas para divulgar anuncios, alertas, datos y otras publicaciones sobre la situación.

Subfunción 4.3.3.2 Buena gestión y coordinación de las relaciones públicas

Garantizar que la información se divulga a los medios de comunicación y los interesados, pero sólo por los canales autorizados de la organización. Se incluyen aquí las publicaciones en medios sociales.

Subfunción 4.3.3.3 Comunicación de las actividades de recuperación

Se comunican las actividades de recuperación a los interesados internos, directivos y equipos de gestión.

Subfunción 4.3.3.4 Obtener información posterior al incidente

El EIISP organiza reuniones de información posteriores a los incidentes para recabar información destinada a mejorar la intervención en caso de incidentes, así como las actividades del ciclo de producción segura (CPS) (por ejemplo, qué elemento del CPS podría o debería haber evitado el problema en primer lugar).

Servicio 4.4 Datos sobre vulnerabilidades

Los datos que se han de obtener son, entre otros, el volumen de problemas, la clasificación, el tiempo invertido en su solución y los productos o servicios afectados.

Propósito
Obtener periódicamente datos para el informe general.

Resultado
Determinar las esferas que se han de analizar y que necesitan recursos y mejoras.

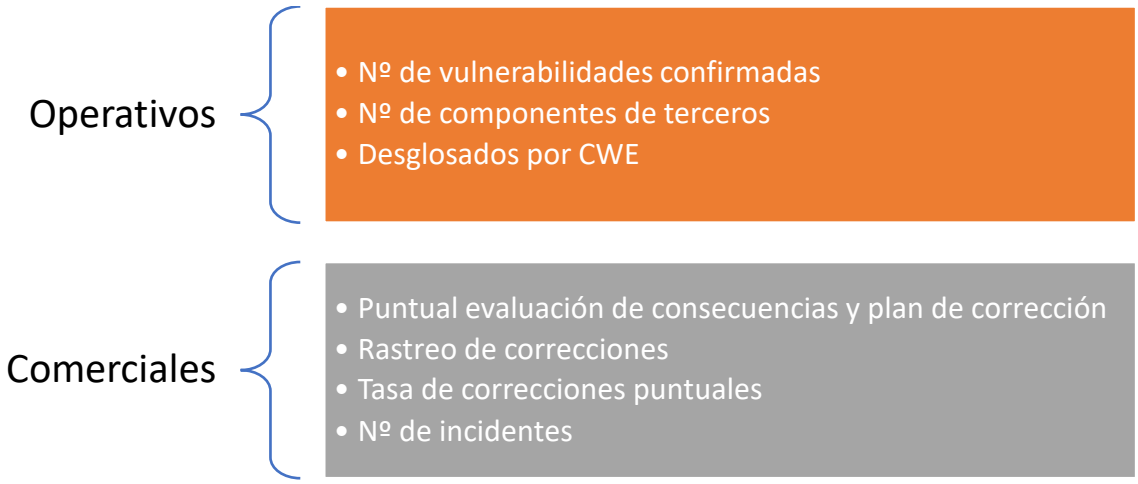


Figura 15: Datos operativos y comerciales

Función 4.4.1 Informes operativos

Los informes operativos contienen información sobre el volumen y los tipos de vulnerabilidades descubiertas y confirmadas en los distintos productos y versiones. Estos informes deben distribuirse periódicamente al EIISP y a los interesados internos.

Propósito
Obtener periódicamente datos para el informe general.

Resultado
Determinar las esferas que se han de analizar y que necesitan recursos y mejoras.

Subfunción 4.4.1.1 Relación entre el número total de vulnerabilidades comunicadas y confirmadas (por producto/unidad comercial)

Estos datos ayudan a conocer el volumen de casos tratados por el EIISP desde la perspectiva de los recursos.

Subfunción 4.4.1.2 Vulnerabilidades confirmadas totales desglosadas por componentes de terceros

Estos datos ayudan a conocer el riesgo asociado a cada componente de terceros específico.

Subfunción 4.4.1.3 Vulnerabilidades confirmadas totales desglosadas por CWE (por producto/unidad comercial)

Estos datos pueden revertirse al ciclo de producción segura e influir en la formación y capacitación.

Función 4.4.2 Informes de gestión

Los informes de gestión contienen información sobre la capacidad de respuesta de una organización a las vulnerabilidades.

Propósito
Medir el nivel de éxito de una organización a la hora de cumplir los compromisos cronológicos contraídos en los SLA. Recabar, analizar y divulgar periódicamente datos que midan el nivel de consecución de esos objetivos.

Resultado
Ilustración gráfica de los éxitos y los márgenes de mejora.

Subfunción 4.4.2.1 Puntualidad de la evaluación de consecuencias

Estos datos miden el rendimiento de los equipos de productos a la hora de realizar evaluaciones de consecuencias dentro de los plazos prescritos en los SLA.

Subfunción 4.4.2.2 Puntualidad del plan correctivo

Estos datos miden el rendimiento de los equipos de productos a la hora de presentar un plan correctivo dentro de los plazos prescritos en los SLA.

Subfunción 4.4.2.3 Rastreo de correcciones

Con estos datos se mide el rendimiento de los equipos de productos a la hora de entregar las correcciones dentro de los plazos prescritos en los SLA.

Subfunción 4.4.2.4 Tasa de corrección puntual

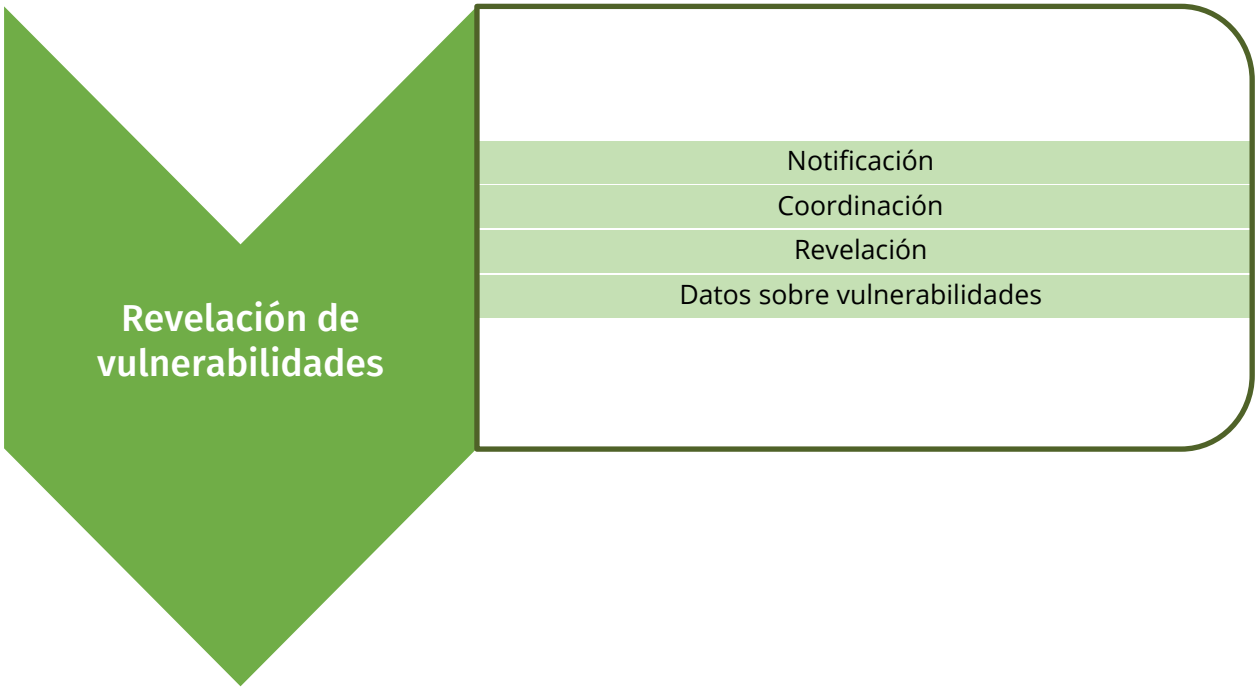
Estos datos miden la capacidad de los equipos de productos para cumplir los objetivos o acuerdos de entrega de correcciones, desde la comunicación de la vulnerabilidad a la

entrega efectiva de la corrección. Los datos pueden desglosarse por grados de gravedad o tipo de vulnerabilidad (línea de producción, tipo de vulnerabilidad).

Subfunción 4.4.2.5 Número de incidentes

Estos datos ilustran los riesgos para la organización.

Esfera de servicio 5



Es fundamental crear un entorno transparente y colaborativo donde los fabricantes, coordinadores y buscadores puedan compartir información con sus interesados y entre ellos, y negociar planes de revelación mutuamente acordados. Gracias a este tipo de asociación se podrán colmar las necesidades primarias en términos de resolución de vulnerabilidades, protección de los interesados y reconocimiento de los buscadores. Los fabricantes deben hacer pública su política de revelación de vulnerabilidades a fin de que los coordinadores, otros fabricantes y buscadores puedan consultarla.

Figura 16: Proceso de notificación de vulnerabilidades

Propósito

Ofrecer transparencia a los interesados y socios mediante la colaboración con buscadores, coordinadores y vendedores descendentes en la revelación responsable de vulnerabilidades y correcciones.

Resultado
Mayor confianza, colaboración y control de la revelación.

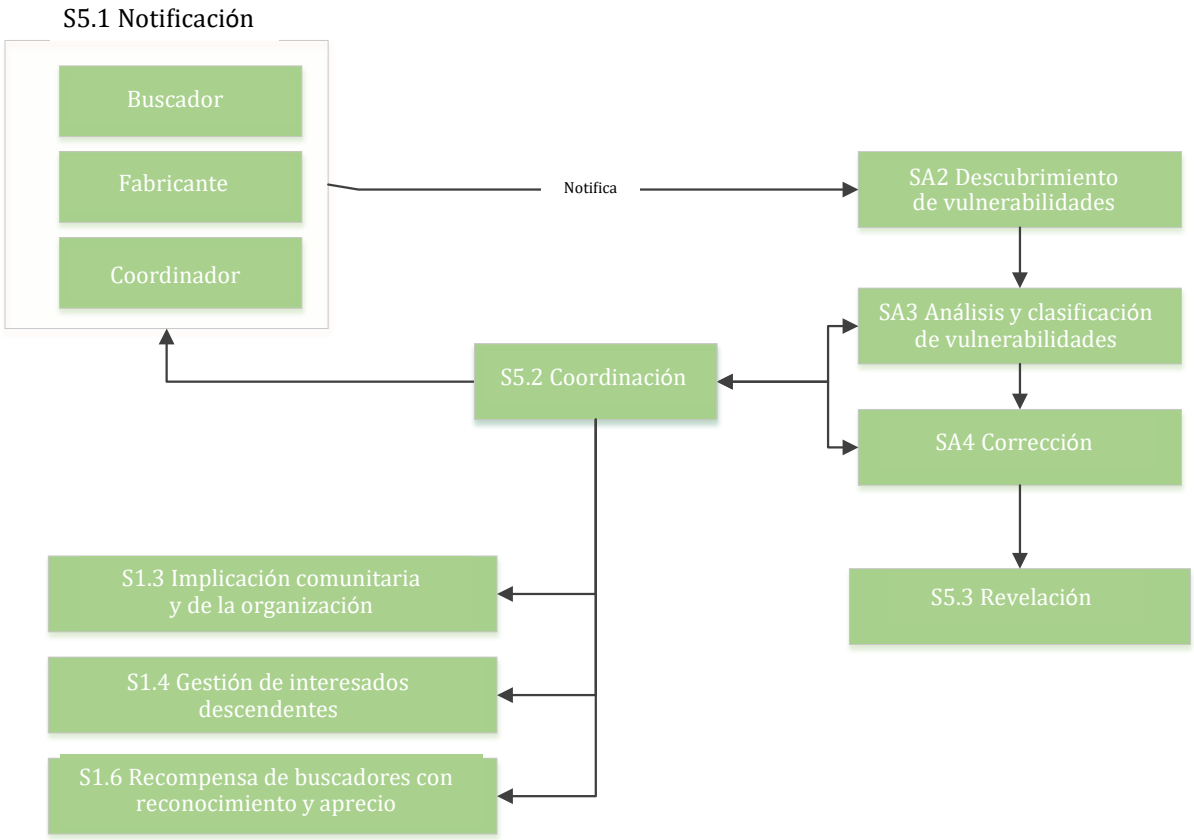


Figura 17: Ejemplo detallado de coordinación de vulnerabilidades

Servicio 5.1 Notificación

Este servicio consiste en determinar el proceso de notificación adecuado para informar puntualmente a los interesados acerca de la estrategia de mitigación, las correcciones y las soluciones alternativas a fin de que estén al día y puedan planificar sus actividades. En algunos casos pueden existir acuerdos contractuales entre fabricantes; por ejemplo, se exigirá a un fabricante ascendente que notifique al fabricante descendente las vulnerabilidades reveladas o los incidentes conocidos. El objetivo del proceso de notificación es garantizar que todos los interesados y fabricantes pueden entender y gestionar el riesgo que plantea la vulnerabilidad.

Propósito
Ofrecer transparencia a fabricantes y buscadores mediante colaboración.

Resultado
Aumentar la confianza y la colaboración con los buscadores.

Función 5.1.1 Fabricantes intermedios (fabricantes descendentes)

Un fabricante intermedio es un OEM o socio que crea y/o produce una parte, un subsistema o un *software* que se utiliza en el producto final de otro fabricante. En tales casos, el EIISP debe

concluir acuerdos para compartir la información sobre vulnerabilidades con esos fabricantes. Es necesario conocer la política de tratamiento de vulnerabilidades de los distintos fabricantes. En ocasiones las expectativas se formalizan en un acuerdo contractual. Los plazos de corrección y revelación deben negociarse lo antes posible.

Propósito
Crear un entorno colaborativo donde las expectativas de los OEM y los socios y demás fabricantes estén claras.

Resultado
Aumento de la confianza, la colaboración y el control de la revelación entre todas las partes implicadas.

Subfunción 5.1.1.1 Información del EIISP a los fabricantes intermedios

Al conocer las vulnerabilidades comunicadas por sus interesados, el EIISP debe notificarlas a los fabricantes intermedios.

Subfunción 5.1.1.2 Información de fabricantes intermedios

Cuando los fabricantes intermedios que proveen de componentes o herramientas a otro fabricante tomen conocimiento de las vulnerabilidades que se les comunican, deberán notificarlas a los EIISP de sus fabricantes.

Subfunción 5.1.1.3 Acuerdos contractuales

Los EIISP deben identificar a todos los fabricantes intermedios y considerar la posibilidad de colaborar con sus equipos jurídicos para asegurarse de que se añaden en los acuerdos contractuales cláusulas de garantía de intervención puntual en caso de vulnerabilidad.

Subfunción 5.1.1.4 Notificación del EIISP a los interesados

Los EIISP de los fabricantes podrán informar a sus interesados, en particular si el fabricante intermedio no puede corregir la vulnerabilidad o tarda un tiempo considerable en corregirla. En ocasiones los EIISP de fabricantes pueden aplicar un proceso de notificación por fases y notificar en primer lugar a los interesados que más afectados se verán por la vulnerabilidad en cuestión.

Función 5.1.2 Coordinadores

El EIISP puede solicitar a un coordinador que participe en la notificación a otros fabricantes, así como en la coordinación de los plazos de corrección que se notifican, sobre todo cuando hay múltiples fabricantes implicados. Los coordinadores, como el centro de coordinación de EIEI (EIEI/CC)[12] o los coordinadores terceros aportan valor al conseguir que múltiples organizaciones distintas se asocien y colaboren en la resolución de una vulnerabilidad.

[12] www.cert.org

Propósito
Puede pedirse a los coordinadores que intervengan y asistan a la organización del EIISP en la notificación y la colaboración con otros fabricantes en caso de vulnerabilidad.

Resultado
Aumento de la confianza, la colaboración y el control de la revelación entre todas las partes implicadas.

Subfunción 5.1.2.1 Identificación del coordinador

Documentar y conocer a los distintos coordinadores en función de la política de revelación de vulnerabilidades.

Subfunción 5.1.2.2 Implicación del coordinador

Asociación con un coordinador para garantizar la notificación a los EIISP de todos los fabricantes afectados.

Función 5.1.3 Buscador

Un buscador, como un cliente o un investigador tercero, puede notificar al EIISP una vulnerabilidad utilizando los canales documentados en *Esfera de servicio 2 Descubrimiento de vulnerabilidades*.

***Propósito**: Crear un entorno de colaboración donde las expectativas de los buscadores estén claras.*

***Resultado**: Aumento de la confianza, la colaboración y el control de la revelación con los buscadores.*

Servicio 5.2 Coordinación

Cuando proceda, el EIISP fabricante concluirá acuerdos para compartir la información sobre vulnerabilidades con los coordinadores y otros fabricantes para que conozcan la política de tratamiento de vulnerabilidades del fabricante. Los plazos de corrección y revelación deben negociarse lo antes posible.

***Propósito**: Documentar las vulnerabilidades suprimidas del producto mediante su corrección.*

***Resultado**: Claridad en cuanto a los beneficios que reporta la corrección y dónde obtenerla.*

Función 5.2.1 Coordinación bilateral

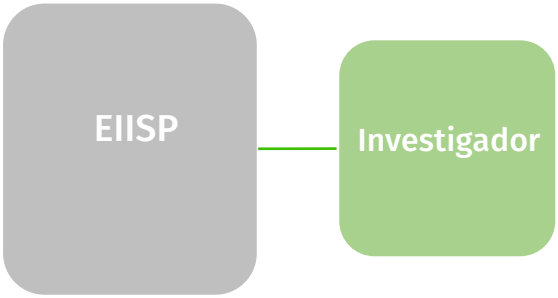


Figura 18: Coordinación bilateral

El EIISP fabricante es responsable de la comunicación con los buscadores que comunican posibles vulnerabilidades. Es importante que los fabricantes conozcan el objetivo, el programa y actitud del buscador de cara a las vulnerabilidades en general a fin de fomentar y facilitar la revelación coordinada dentro de unos plazos acordados. El EIISP debe considerar la posibilidad de reconocer a los buscadores que respetan los términos de revelación al público.

Propósito
Crear un entorno de colaboración en el que los buscadores sabrán que se les toma en serio.

Resultado
Plan de revelación negociado que recompensa los esfuerzos del buscador.

Subfunción 5.2.1.1 Recepción de informes

Acusar recibo de los informes de vulnerabilidades de buscadores terceros.

Subfunción 5.2.1.2 Actualización periódica

Facilitar periódicamente al buscador información actualizada sobre la vulnerabilidad comunicada.

Subfunción 5.2.1.3 Validación por el buscador

Entregar la corrección al buscador para que éste también pueda validarla.

Subfunción 5.2.1.4 Reconocimiento del buscador

Reconocer el valor de las contribuciones del buscador que informa sobre las vulnerabilidades. El fabricante debe verificar que la reputación del buscador es merecida.

Función 5.2.2 Coordinación entre múltiples fabricantes

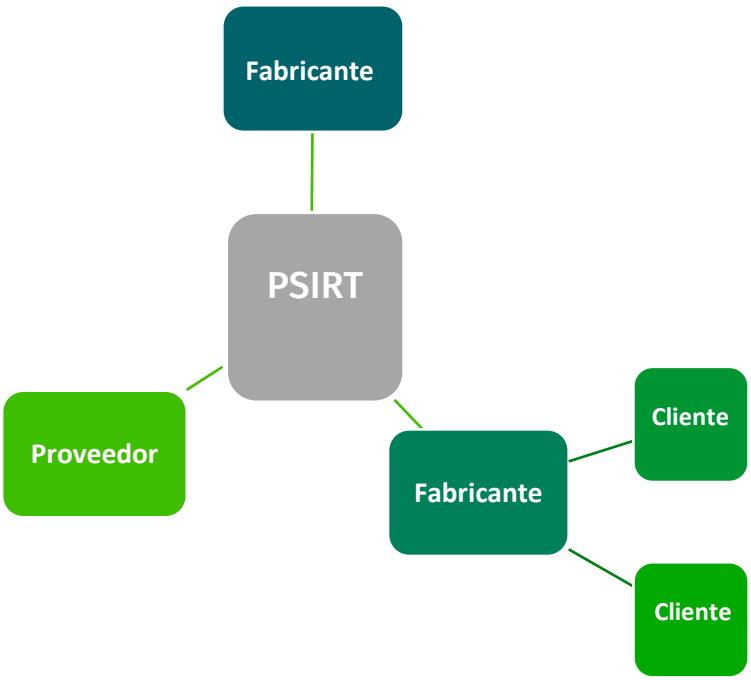


Figura 19: Coordinación entre múltiples fabricantes

Cuando proceda, el EIISP fabricante concluirá acuerdos para compartir la información sobre vulnerabilidades con los coordinadores y otros fabricantes para que conozcan la política de tratamiento de vulnerabilidades del fabricante. Los plazos de corrección y revelación deben negociarse lo antes posible.

Propósito
Ofrecer transparencia a los interesados y socios mediante la colaboración con todas las partes para revelar de manera responsable las vulnerabilidades y correcciones.

Resultado
Mayor confianza, colaboración y control de la revelación.

Interesado multipartito	Relación interna	Objeto de la coordinación
Fabricantes ascendentes	El proveedor OEM facilita la tecnología.	Para entregar una corrección se recomienda que los fabricantes ascendentes gestionen a sus interesados descendentes (véase *Esfera de servicio 1.4*).
Fabricantes descendentes	Recibe tecnología del fabricante ascendente.	Recibir notificaciones para aplicar las correcciones de seguridad. Se recomienda que los fabricantes descendentes identifiquen y colaboren con las comunidades y socios fabricantes ascendentes

Cuadro 1: Ejemplo de coordinación multipartita

Subfunción 5.2.2.1 Recepción de informes

El EIISP del fabricante acusa recibo del informe de vulnerabilidades de un fabricante o coordinador.

Subfunción 5.2.2.2 Identificación del fabricante afectado

El EIISP del fabricante o el coordinador pueden tener que identificar a los fabricantes afectados por el informe de vulnerabilidades.

Subfunción 5.2.2.3 Compartición de información sobre vulnerabilidades

El EIISP del fabricante o el coordinador comparten información sobre vulnerabilidades con los distintos fabricantes.

Subfunción 5.2.2.4 Planificación de entrega de correcciones

El EIISP del fabricante o el coordinador se asocian con los fabricantes para definir los plazos y la disponibilidad de las correcciones y cómo los fabricantes descendentes podrán recibir la corrección.

Subfunción 5.2.2.5 Validación de correcciones

El EIISP del fabricante o el coordinador validan con los fabricantes que la corrección de seguridad elimina la vulnerabilidad.

Subfunción 5.2.2.6 Coordinación de la revelación

El EIISP del fabricante o el coordinador negocian con todos los fabricantes para acordar cómo se revelará la vulnerabilidad y cuándo se hará pública.

Servicio 5.3 Revelación

Cuando se vaya a sacar una corrección de seguridad, se darán las informaciones convenientes para garantizar que los interesados y fabricantes reciben las necesarias notificaciones acerca de las correcciones. En todos los casos deberá definirse adecuadamente a quién se dirige la notificación (cada notificación puede tener un público objetivo distinto).

Propósito
Documentar los cambios de código y la publicación de correcciones de seguridad.

Resultado
Claridad en relación con las correcciones aportadas al código y dónde obtenerlas.

Función 5.3.1 Notas de versión

Las notas de versión, incluidos los archivos readme y el historial de cambio, deben incluir las referencias CVE de la corrección. En las notas de versión de detallará claramente cómo se ha corregido la vulnerabilidad.

Propósito
Indicar las correcciones incluidas en el código actualizado.

Resultado
Los interesados pueden protegerse contra la eventual exposición de las vulnerabilidades.

Subfunción 5.3.1.1 Revelación en notas de versión

Definir qué vulnerabilidades deben revelarse en las notas de versión.

Subfunción 5.3.1.1 Revisión de notas de versión

Definir el proceso de revisión.

Subfunción 5.3.1.2 Aprobación de notas de versión

Examinar y aprobar la revelación.

Función 5.3.2 Avisos de seguridad

Los fabricantes deben disponer de un mecanismo para la emisión de avisos de seguridad a los interesados en una página web pública y para revelar las vulnerabilidades corregidas.

Propósito
Crear un repositorio público de los avisos de seguridad publicados.

Resultado

Los avisos de seguridad están a disposición de los mandantes para que los examinen y tomen medidas al respecto.

Subfunción 5.3.2.1 Plantilla de aviso

Definir una plantilla de aviso de seguridad normalizada que comprenda el título, el resumen, la CVE, el estado del producto afectado y las consecuencias para el mismo, el reconocimiento, las referencias y el historial de revisión.

Subfunción 5.3.2.2 Método de entrega de avisos

Determinar el mecanismo de entrega de avisos de seguridad, por ejemplo, documento web, canal RSS o abono, entre otros.

Subfunción 5.3.2.3 Formato de los avisos

Para que los interesados y mandantes puedan procesar los avisos con herramientas automáticas, se considerará la posibilidad de publicar los avisos en formato de lectura automática, como el marco común de avisos de seguridad[13] (CSAF).

Subfunción 5.3.2.4 Desencadenantes de avisos

Definir las condiciones que desencadenarán la emisión de un aviso de seguridad. Por ejemplo, si es necesario tomar medidas para notificar a los interesados que se ha corregido un entorno anfitrión (en caso de intrusión).

Subfunción 5.3.2.5 Asignación de CVE

Determinar el proceso de asignación de un ID CVE a una vulnerabilidad.

Subfunción 5.3.2.6 Reconocimiento del buscador

Determinar si el buscador apreciaría que se le reconociese públicamente.

Subfunción 5.3.2.7 Planificación de la revelación

Definir el proceso de revisión mediante el cual se definen, entre otras cosas, quiénes son los interesados y cuándo debe procederse a la revelación.

Subfunción 5.3.2.8 Proceso de revisión de avisos

Aplicar el proceso de revisión con los interesados definidos.

[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

Función 5.3.3 Artículos fundamentados

Los fabricantes deben disponer de un mecanismo para publicar artículos fundamentados, posiblemente como acompañamiento de correcciones de seguridad de poca gravedad o que pueden servir para comunicar por qué determinadas vulnerabilidades de seguridad comunicadas se consideran falsos positivos.

Propósito
Crear un repositorio de artículos fundamentados.

Resultado
Los mandantes pueden consultar los artículos fundamentados y tomar las medidas pertinentes.

Subfunción 5.3.3.1 Publicación de artículos fundamentados

Definir qué vulnerabilidades se han de revelar en los artículos fundamentados.

Subfunción 5.3.3.2 Revisión de artículos fundamentados

Definir el proceso de revisión.

Subfunción 5.3.3.3 Aprobación de artículos fundamentados

Revisar y aprobar la publicación.

Función 5.3.4 Comunicación con interesados internos

Además de los directivos, a los que se han de notificar los planes de comunicación acerca de las vulnerabilidades, hay muchos empleados en primera línea que trabajan directamente con los interesados, cara a cara o por teléfono. Darles información confidencial sobre los próximos avisos y una lista de preguntas frecuentes contribuirá a la preparación de los que recibirán las preguntas una vez publicados esos avisos.

Propósito
Informar a los directivos, a los responsables de la comunicación y a los empleados cara al público de los próximos avisos y de las respuestas aprobadas.

Resultado
Los empleados podrán responder a las preguntas de los interesados y los medios de comunicación cuando se publique el aviso, lo que permitirá controlar el mensaje.

Subfunción 5.3.4.1 Implicación de interesados internos

Colaborar con los interesados internos para definir y/o revisar las fórmulas empleadas por sus equipos para responder a las preguntas de los clientes sobre las vulnerabilidades.

Servicio 5.4 Datos sobre vulnerabilidades

Los datos que se han de obtener son, entre otros, el volumen de problemas, la clasificación, los plazos de corrección y los productos y servicios afectados.

Propósito
Obtener periódicamente datos para los informes de gestión.

Resultado
Determinar las esferas que se han de analizar, mejorar y dotar de recursos.

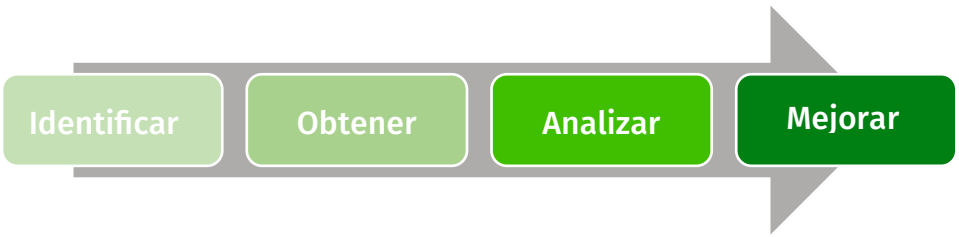


Figura 20: Procesamiento de datos sobre vulnerabilidades

Función 5.4.1 Informes operativos

Los informes operativos pueden ofrecer información adicional sobre el volumen de revelaciones publicadas y el número de visitas de las páginas. Estos informes deben distribuirse periódicamente al EIISP y a los interesados internos.

Propósito
Obtener periódicamente datos para el informe general.

Resultado
Determinar las esferas que se han de analizar y que necesitan recursos y mejoras.

Subfunción 5.4.1.1 Número de avisos de seguridad publicados

Puede darse cuenta del número de publicaciones, desglosadas por productos. Esto puede ayudar a los equipos en la asignación de recursos técnicos.

Subfunción 5.4.1.2 Número de CVE comunicados a la NVD

El número de CVE asignados puede utilizarse para convertirse en autoridad de numeración CVE (CNA).

Subfunción 5.4.1.3 Consultas de avisos de seguridad

Puede dirigir la estrategia hacia una notificación proactiva si el número de interesados que consultan los avisos es bajo.

Esfera de servicio 6

El mundo de la seguridad de los productos está en constante evolución, pues los nuevos servicios y tecnologías y su integración hacen de la formación y la capacitación una de las grandes prioridades de los profesionales de la seguridad. A medida que el *software* penetra todos los aspectos de nuestro mundo, desde los coches hasta las neveras, nunca ha sido tan importante como ahora la necesidad de que los productos sean seguros. Los EIISP desempeñan un papel clave a la hora de definir un programa formativo fuerte que dé a conocer a todos los interesados los entresijos de la producción, la validación y la entrega de productos/servicios de conformidad con las normas del mundo conectado actual.

Las necesidades de formación y capacitación pueden ser muy variables incluso dentro de una misma empresa. Las inquietudes de un creador de *firmware* y de un creador de servicios de *software* son muy distintas y con frecuencia exigen una formación muy específica y particular. En este documento se desglosan las necesidades de formación en función de cuatro tipos de interesados: EIISP, creación de productos, validación de productos y otros interesados implicados en el proceso del EIISP.

1. La **formación del EIISP** es única, pues los miembros del EIISP deben estar al día de muchos temas distintos, por ejemplo, asuntos jurídicos, comunicaciones y producción.
2. **Creación de productos** (Ingeniería y producción internas): los creadores necesitan formación en sus ámbitos específicos, por lo que la formación debe ser muy concreta. Las necesidades de un creador de *firmware* seguro, muy difícil de actualizar en la práctica, son muy distintas de las de un ingeniero de aplicaciones de escritorio.

3. **Validación de productos** (Ingeniería y producción internas): los validadores necesitan una formación constante a fin de familiarizarse con las herramientas y técnicas más modernas, como pruebas de penetración, escaneado de vulnerabilidades y examen temprano del diseño a fin de detectar los problemas antes de que sea necesario corregirlos.
4. **Todos los demás interesados**: este grupo engloba a los interesados menos técnicos que necesitan una base sólida para entender los conceptos básicos de la creación, la validación y la entrega de productos seguros, así como para reaccionar cuando uno de esos productos muestra una vulnerabilidad.

La formación en creación segura no se considera parte del programa del EIISP y se gestiona fuera del proceso del EIISP. Sin embargo, es importante que los miembros del EIISP conozcan perfectamente todos los aspectos que intervienen en la comercialización de productos seguros y, por tanto, deben asociarse con diversos equipos de producción para asegurarse de que se ofrece la formación adecuada. Es posible que en muchas organizaciones de pequeño tamaño no exista un grupo independiente responsable de que los productos se crean atendiendo prioritariamente a criterios de seguridad. En esos casos, el EIISP puede ayudar a cerrar esa brecha (este tema queda fuera del alcance del presente documento).

En cada una de las secciones siguientes se identifican los diversos grupos de interesados y se resumen los principales aspectos que pueden ayudar al EIISP a entablar diálogo sustantivo acerca de la formación y capacitación de sus interesados. Los EIISP pueden crear todo el material de formación a nivel interno, utilizar material externo o utilizar recursos de formación externos para sus interesados.

Servicio 6.1 Formación del EIISP

El personal del EIISP debe estar al día de lo que pasa en el mundo de la seguridad, incluidas las tendencias, los nuevos hallazgos y las actividades de la industria, entre otras cosas. Para alcanzar este amplio nivel de conocimiento se ha de contar con una base sólida en seguridad general demostrada por certificados en seguridad de alto nivel. Pero esos certificados son sólo una base que se ha de actualizar constantemente participando en conferencias sobre seguridad, colaborando con consorcios industriales e interesándose en la industria en su conjunto a través de blogs, prensa y publicaciones especializadas, etc. Los miembros del EIISP también tienen que mantenerse informados de la evolución constante de la legislación en materia de seguridad y privacidad.

Función 6.1.1 Formación técnica

Es importante que el personal del EIISP tenga un sólido conocimiento de los conceptos básicos de seguridad y de los productos de que se tiene que ocupar. El material formativo debe revisarse periódicamente para garantizar que, a medida que el panorama de la seguridad evoluciona, se incluyen en él las más nuevas técnicas contra las vulnerabilidades.

Propósito
Formar al personal del EIISP para que entiendan los problemas que se les comunican y puedan realizar adecuadamente la clasificación inicial antes de remitirlos a los equipos responsables de preparar, probar y publicar las correcciones.

Resultado
El personal del EIISP está suficientemente formado para realizar su trabajo.

La formación en conceptos de seguridad variará en función del tipo de productos del fabricante (por ejemplo, *hardware*, *firmware*, *software*, interconexión de redes, productos de la nube o todos ellos a la vez). A un nivel muy elevado, la formación debe comprender los temas básicos de seguridad, como los ataques comunes, la criptografía, la integridad, la disponibilidad, la autentificación, los modelos de control de acceso, el multiarrendamiento, la reglamentación y su cumplimiento, entre otros. Esta formación debe incluir también los reglamentos propios de la industria que pueden influir en las actividades del EIISP, como HIPAA para actividades verticales en la esfera de la salud y PCI DSS para las tarjetas de pago y la banca. El personal del EIISP también debe recibir formación sobre los productos a fin de entender los problemas que se comuniquen.

Función 6.1.2 Formación en comunicaciones

Dado que los buscadores externos comunican problemas al EIISP, es importante que el personal del EIISP reciba formación sobre políticas de comunicación y competencias sociales que les permitan establecer comunicaciones de manera oportuna con los buscadores externos y los interesados internos.

Propósito
Garantizar que el personal del EIISP respeta las políticas de comunicación de la organización al interactuar con entidades externas, evitando así todo problema jurídico/reglamentario que pudiese resultar de una comunicación inadecuada.

Resultado
El personal del EIISP tendrá la formación en comunicaciones suficiente para realizar su trabajo de manera clara y precisa y sin ambigüedades en la comunicación.

Función 6.1.3 Formación en procesos

Serán necesarias unas directrices procesales en las que se defina cómo se rastrearán, gestionarán y medirán los problemas comunicados. Se deberán definir las funciones de los distintos interesados implicados en el proceso de resolución de los problemas comunicados. El proceso debe comprender la respuesta puntual a los buscadores y el envío periódico de información sobre los avances de los problemas en curso. También se deberá contar con un medio bien definido y seguro para la comunicación entre los buscadores externos y el fabricante.

Propósito
Garantizar que, al gestionar incidentes de seguridad de los productos, la información fluye con facilidad para resolver oportunamente los problemas.

Resultado
El personal del EIISP recibirá la suficiente formación en materia de procesos internos para poder realizar su trabajo.

Función 6.1.4 Formación en herramientas

Subfunción 6.1.4.1 Rastreo de errores y otras herramientas de gestión para el EIISP y los ingenieros

Se ha de identificar una herramienta de rastreo de errores formalmente reconocida para cada producto (preferiblemente la misma para todos los productos) de una organización dada. En esta herramienta se han de identificar todos los errores y los errores de seguridad deben identificarse uniformemente como tales. Sólo las personas que necesitan conocer esa información deberán poder consultar y acceder a la información sobre las vulnerabilidades de seguridad de un producto. Además, la herramienta ha de cumplir los requisitos de medición de programa y ofrecer la capacidad de generación manual y automática de informes.

Propósito
Garantizar el rastreo efectivo de los problemas y la salvaguarda de la información sobre vulnerabilidades en las herramientas de rastreo certificadas y que sólo las personas autorizadas puedan acceder, rastrear y gestionar esa información.

Resultado
El personal del EIISP tendrá la formación y el conocimiento suficientes de estas herramientas para realizar su trabajo.

Subfunción 6.1.4.2 Herramientas de rastreo de terceros

Casi todos los productos contienen varios componentes de terceros (incluso de código abierto). Con frecuencia los clientes no tendrán conocimiento del *software* de terceros integrado en el producto, por lo que confiarán en que el fabricante les facilite las correcciones o la información correspondiente. Es importante identificar herramientas de rastreo de terceros internas para cubrir las dependencias de los productos del fabricante de los componentes de terceros. Se han de supervisar la base de datos nacional de vulnerabilidades (NVD), los avisos de seguridad de fabricantes terceros y otros sitios externos para rastrear las vulnerabilidades y correcciones de los componentes de terceros a fin de facilitarlas al cliente.

Propósito
Identificar herramientas para rastrear los componentes de terceros integrados en los productos a fin de rastrear y corregir las vulnerabilidades de esos componentes.

Resultado
El personal del EIISP conocerá los componentes de terceros integrados en los productos y podrá rastrearlos.

Función 6.1.5 Rastreo de todas las iniciativas de formación

El EIISP tendrá que rastrear todas las formaciones disponibles para los diversos interesados. El equipo tendrá que asegurarse de que todas esas formaciones se imparten con cierta frecuencia, dado que el panorama de la seguridad evoluciona muy rápidamente, por lo que será necesario actualizar constantemente las formaciones y procesos.

Propósito
Garantizar el seguimiento de todas las formaciones para los diversos interesados.

Resultado
El personal del EIISP sabrá que los distintos interesados han recibido formación en relación con su función en el proceso del EIISP.

Servicio 6.2 Formación del equipo de producción

Por producción segura se entienden las metodologías y medidas adoptadas a lo largo del proceso de producción específicamente diseñadas para reducir el número y la gravedad de las vulnerabilidades de los productos y servicios de *software*. Gracias a un programa estricto y a la utilización de metodologías de producción segura se pueden reducir ampliamente las vulnerabilidades antes de la comercialización de los productos, lo que resulta mucho menos oneroso que resolverlas una vez los productos en el mercado.

La producción segura empieza por los requisitos y la arquitectura del producto. Además, es fundamental evaluar la seguridad del diseño para detectar posibles vulnerabilidades antes de que el producto pase a la fase de producción.

Los programas de producción segura comprenden numerosas actividades cuyos detalles quedan fuera del alcance de este documento. Se recomienda vivamente contar con un programa independiente para gestionar adecuadamente el ciclo de producción segura. Este programa debe ajustarse a un modelo acorde con las normas industriales aceptadas. Como ejemplo de ciclo de producción segura puede citarse el modelo *Microsoft Secure Development Lifecycle*[14].

Propósito
Instar a la organización a dotarse de un programa de ciclo de producción segura (CPS) dentro del cual se forme al personal de producción en escritura de código seguro y se utilicen directrices de seguridad documentadas para crear la arquitectura o diseñar un producto.

Resultado
Los equipos de producción podrán escribir códigos seguros y comercializar productos más seguros.

La formación en producción segura no siempre se considera responsabilidad del EIISP y puede gestionarse fuera del proceso del EIISP. En cualquier caso se trata de un elemento importante para cualquier vendedor que se preocupe de la seguridad de sus productos.

Función 6.2.1 Formación en el proceso del EIISP

Todos los participantes en el proceso de producción deben entender por qué existe el proceso del EIISP, cómo funciona y lo que tienen que hacer para crear productos que lo soporten. Normalmente, una vez comercializado un producto, los equipos de producción pasan a otros proyectos y dedican un tiempo mínimo al mantenimiento. Formar a los equipos y facilitarles los métodos adecuados para almacenar información clave sobre los productos es fundamental para que el EIISP pueda resolver los problemas de vulnerabilidad de los productos. Se ha de

[14] https://www.microsoft.com/en-us/sdl/

documentar, entre otras cosas, quién fue el arquitecto de seguridad, quién lideró el proyecto y quién se ocupó de las pruebas a fin de que el EIISP pueda remitirse a las personas adecuadas para evaluar los riesgos y preparar las correcciones. En esa información se han de incluir también datos como los siguientes: qué componentes de terceros se han utilizado, cuál es el proceso de actualización de los productos, qué registros se han creado, qué excepciones de seguridad se permiten y cómo se notifica a los interesados. Esta información es también fundamental para el EIISP a la hora de resolver una vulnerabilidad de seguridad. Dado que la composición de los equipos de producción puede cambiar, es necesario que la formación se imparta periódicamente.

Propósito
Garantizar que todos los interesados entienden el proceso del EIISP y cómo se relaciona con su función en la creación de productos.

Resultado
Fomentar la cultura de la seguridad entre los creadores y una mejor cooperación a la hora de resolver vulnerabilidades.

Servicio 6.3 Formación del equipo de validación

Es necesario que los validadores se mantengan al día de las últimas herramientas y técnicas en materia de pruebas de penetración, escaneado de vulnerabilidades, *fuzzing* y pirateo ético, por ejemplo. Esta formación de los validadores pertenece al CPS y queda fuera del alcance de este documento. Sin embargo, el EIISP debe instar a la organización a disponer de un grupo dedicado a esta tarea.

Propósito
Instar a la organización a disponer de un programa CPS adecuado dentro del cual se identifiquen las herramientas de pruebas de seguridad adecuadas.

Resultado
Productos más seguros y de mayor calidad.

Al igual que la producción segura, la formación en validación de seguridad no es responsabilidad del EIISP y puede gestionarse fuera del proceso del EIISP. Sin embargo, su importancia es idéntica y debe formar parte del CPS del producto de un fabricante.

Función 6.3.1 Formación en el proceso del EIISP

Algunos miembros del equipo de validación pueden participar en las pruebas de las correcciones necesarias para solventar las vulnerabilidades de los productos. Esos miembros del equipo deben entender el proceso del EIISP, cómo funciona y cuáles son los plazos previstos, así como su función en el proceso. Es necesario que conozcan bien el ciclo de vida del producto a fin de saber cuáles son las versiones que se han de probar para las correcciones de vulnerabilidades. También tendrán que probar las soluciones alternativas, de haberlas. Será importante que prueben también las regresiones.

Propósito
Garantizar que todos los interesados entienden el proceso del EIISP y qué relación tiene con su función en la validación de productos.

***Resultado**: Fomentar una cultura de la seguridad entre los validadores y una mejor cooperación a la hora de resolver vulnerabilidades.*

Servicio 6.4 Formación continua de todos los interesados

Todos los interesados deberán recibir un cierto grado de formación e información sobre el programa EIISP. Muchos interesados participan en el proceso del EIISP de extremo a extremo. Por consiguiente, es importante identificar los diversos grupos de interesados y preparar la formación que se adapte a sus necesidades.

Propósito
Garantizar que todos los grupos de interesados reciben la formación o información básica necesaria para cumplir su papel en el programa EIISP.

Resultado
Mandantes internos bien informados que saben cómo interactuarán con el EIISP a la hora de gestionar problemas de vulnerabilidades nuevos y qué servicios les ofrecerá el EIISP en esos casos.

Función 6.4.1 Formación de la dirección

Este grupo suele participar en la definición de las políticas de la empresa en materia de comunicación, protección contra vulnerabilidades y demás. También puede ser necesaria la aprobación de la dirección a la hora de emitir avisos de seguridad, y suele necesitarse en situaciones críticas de alto riesgo, muy visibles o que implican una gran responsabilidad. También es posible que la dirección desee que se verifique periódicamente la seguridad de todos los productos. Por consiguiente, es importante que la dirección esté informada de los procesos del EIISP.

Propósito
Informar a la dirección acerca de su función en el marco del programa EIISP.

Resultado
Obtención oportuna de la necesaria aprobación de la dirección.

Función 6.4.2 Formación del equipo jurídico

El equipo jurídico participa en la definición de las políticas corporativas. Algunos problemas comunicados por los buscadores pueden plantear cuestiones de responsabilidad y necesitar de la ayuda del equipo jurídico, por lo que es importante identificar a las personas de contacto con antelación.

Propósito
Dar a conocer al equipo jurídico su función en el programa EIISP y los plazos aplicables.

Resultado
Resolución oportuna de problemas de seguridad que necesitan la aprobación del equipo jurídico.

Función 6.4.3 Formación del equipo de cumplimiento y gobernanza

Los equipos de gobernanza se ocupan de los problemas de cumplimiento de la reglamentación. Por consiguiente, es importante identificar a las personas de contacto con antelación.

Propósito
Dar a conocer al equipo de gobernanza su función en el programa EIISP.

Resultado
Resolución oportuna de vulnerabilidades de seguridad que exigen el cumplimiento de ciertas normas reglamentarias.

Función 6.4.4 Formación del equipo de comercialización

El equipo de comercialización suele intervenir cuando hay riesgos para la marca. Así, podrá ser necesario revisar los avisos de seguridad con este equipo y publicar al mismo tiempo información mercadotécnica conexa. Los equipos de comercialización también participan en la publicidad de la seguridad de los productos.

Propósito
Dar a conocer al equipo de comercialización su función en el programa EIISP e informarles de lo que se puede y no puede decir en relación con la seguridad de los productos.

Resultado
La adecuada coordinación entre el EIISP y los equipos de comercialización permitirá la armonización de la información publicada con fines comerciales y los avisos de seguridad.

Función 6.4.5 Formación del equipo de relaciones públicas

Los equipos de relaciones públicas pueden ser responsables de responder a publicaciones o blogs externos, o de responder a las preguntas de la prensa en relación con las vulnerabilidades críticas de un producto. Será necesario identificar a las personas de contacto de estos equipos para su intervención en caso necesario.

Propósito
Dar a conocer al equipo de relaciones públicas su función en el programa EIISP.

Resultado
La adecuada coordinación entre el EIISP y los equipos de relaciones públicas garantizará la imagen de seguridad exterior del fabricante.

Función 6.4.6 Formación del equipo de ventas

Podrá darse a los equipos de ventas formación sobre conceptos básicos de seguridad y comunicaciones en relación con las prácticas de seguridad. Asimismo, es muy importante que los responsables de ventas sepan qué información puede o no comunicarse a partes externas. Se recomienda que los vendedores remitan todas las preguntas y preocupaciones

en materia de seguridad de los interesados al personal del EIISP o al personal de mantenimiento, en lugar de responder a ellas directamente.

Propósito
Informar a los equipos de ventas de lo que se puede decir o no en relación con la seguridad de los productos y de adónde dirigir las preguntas cuando no puedan responderlas.

Resultado
La adecuada coordinación entre el EIISP y los equipos de ventas contribuirá a colmar las expectativas de los clientes.

Función 6.4.7 Formación del equipo de mantenimiento

Los equipos de mantenimiento deben recibir formación para tratar los informes de vulnerabilidades de seguridad remitidos por los clientes. En ocasiones, para resolver esos problemas puede ser necesaria la intervención del EIISP. Los equipos de mantenimiento deben publicar las políticas que definen la vida útil de cada producto, las versiones objeto de mantenimiento y la eventual publicación de avisos de seguridad. La mayoría de fabricantes sólo emiten avisos de seguridad para las versiones que se mantienen, motivo por el cual esas políticas son fundamentales y deben publicarse en el sitio web del fabricante para su fácil consulta por los interesados. Los EIISP suelen mantener una estrecha relación con los equipos de mantenimiento a fin de conocer el tipo de problemas comunicados por los clientes. En ocasiones los buscadores pueden ser también clientes, por lo que el tratamiento del problema puede implicar tanto al mantenimiento como al EIISP.

Propósito
Dar a conocer a los equipos de mantenimiento su función en el proceso del EIISP.

Resultado
La adecuada coordinación entre el EIISP y los equipos de mantenimiento contribuirá a colmar las expectativas de los clientes y buscadores.

Servicio 6.5 Facilitar mecanismos de retroinformación

Utilizar la información obtenida durante el análisis de las causas primeras para formar al personal y evitar vulnerabilidades similares en el futuro.

Propósito
Mejorar constantemente la formación para adaptarla al ritmo de la rápida evolución de la industria de la seguridad.

Resultado
Una formación de mayor calidad redundará en una mejor experiencia para todos los interesados.

Anexo 1: Material conexo

- [15]Architecture Content Framework
- [16]ISO 31000:2009 Risk management – Principles and guidelines
- ISO/CEI 27000/2018 Information technology – Security techniques – Information security management systems
- [17]ISO/CEI 30111:2013 Information technology – Security techniques – Vulnerability handling processes
- [18]ISO/CEI 29147:2014 Information technology – Security techniques – Vulnerability disclosure
- [19]Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure
- Guía y normas de los Fundamentos para la dirección de proyectos (PMBBOK)

[15] http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html
[16] https://www.iso.org/iso-31000-risk-management.html
[17] https://www.iso.org/obp/ui/#iso:std:53231:en
[18] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en
[19] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRSTMultiparty-Vulnerability-Coordination-v1.0.pdf

Anexo 2: Agradecimientos

- Barbara Cosgriff, MetLife
- Beverly Finch, Lenovo
- Carl Denis, Siemens
- Chris Robinson, Red Hat
- Jeff Hahn, Honeywell
- Jerry Bryant, Intel
- Josh Dembling, Intel
- Jean-Robert Hountomey, Broadcom
- Kevin Ryan, NetApp
- Langley Rock, Red Hat
- Lisa Bradley, Dell Technologies
- Peter Allor, Red Hat
- Reshma Banerjee, Oracle
- Rupert Wimmer, Siemens
- Shawn Richardson, NVIDIA
- Steve Brukbacher, Johnson Controls
- Tania Ward, Dell Technologies
- Vic Chung, SAP

Anexo 3: Cuadros e ilustraciones

Anexo 4: Ventajas e inconvenientes de los modelos orgánicos de EIISP

Modelo	Descripción	Ventajas	Inconvenient
Distribuid	Un equipo operativo del EIISP reducido distribuye el trabajo a los representantes del EIISP en las distintas esferas funcionales (por ejemplo, mantenimiento, ingeniería, gestión de productos).	▪ Ideal para las grandes empresas con carteras de productos amplias y diversificadas. ▪ Amortización del costo del EIISP. ▪ El trabajo se distribuye por funciones. ▪ Adaptable al crecimiento de la cartera.	▪ La organización del EIISP tiene un cierto grado de autoridad para imponer políticas y orientaciones. ▪ Con frecuencia el EIISP carece de control directo de los recursos que solucionan las vulnerabilidades y, por tanto, ejerce menos control. ▪ Las diferentes áreas de producción pueden situar sus intereses por encima de las actividades del EIISP.
Centralizado	Organización del EIISP más grande, directamente implicada en todas las actividades del EIISP (por ejemplo, gestión de programas, clasificación, identificación, corrección y comunicación) para todas las áreas de producción distintas.	▪ Ideal para empresas pequeñas con carteras de productos más pequeñas. ▪ Grupo central de expertos en seguridad de productos altamente competentes. ▪ La organización del EIISP toma todas las decisiones acerca del presupuesto, las políticas y los recursos del EIISP. ▪ Mejor control y responsabilidad sobre las actividades operativas del EIISP.	▪ No se adapta bien al crecimiento de las carteras de productos. ▪ Las decisiones importantes se han de tomar con la cooperación o aprobación de distintos directores funcionales. ▪ Resulta caro mantener un equipo central con competencias especializadas.
Híbrido	Combinación de las características de los modelos centralizado y distribuido.		

Cuadro 2: Ventajas e inconvenientes de los modelos orgánicos de EIISP

Anexo 5: Tipos de equipos de intervención en caso de incidentes

- **EIISI nacional (Equipo de intervención en caso de incidentes de seguridad informática)** – Entidad constituida por una autoridad nacional para coordinar incidentes de ciberseguridad a nivel nacional. Por lo general entre sus mandantes se encuentran todos los organismos y departamentos gubernamentales, las fuerzas del orden público y la sociedad civil. También suele ser la autoridad para interactuar con los EIISI nacionales de otros países, así como con actores regionales e internacionales.
- **EIISI sectorial/infraestructura fundamental** – Encargado de supervisar, gestionar e intervenir en caso de incidentes de ciberseguridad relativos a un sector determinado (por ejemplo, energía, telecomunicaciones o finanzas).
- **EIISI empresarial (organizativo)** – Suele ser un equipo encargado de supervisar, gestionar e intervenir en caso de incidentes de ciberseguridad que afectan a las infraestructuras y servicios TIC internos de una organización determinada.
- **EIISI regional/multipartito** – Equipo o matriz de equipos encargados de supervisar, gestionar e intervenir en caso de incidentes de ciberseguridad relativos a una región determinada o a un número de organizaciones.
- **Equipo de intervención en caso de incidentes de seguridad de productos (EIISP)** – Equipo dentro de una entidad comercial (normalmente un operador) que gestiona la recepción, investigación y la notificación interna o pública, de información de seguridad sobre vulnerabilidades relativas a productos o servicios comercializados por esa organización.

Glosario

- **Acciones** – Lista del modo de actuar en diferentes niveles de detalle/madurez.
- **Capacidad** – Actividad cuantificable que se realiza con arreglo a los roles y responsabilidades de una organización. A los efectos del marco de servicios SIRT, las capacidades pueden definirse como servicios más amplios o como las funciones, tareas o acciones necesarias.
- **Volumen de capacidad** – Número de veces que una organización puede ejecutar una determinada capacidad antes de agotar los recursos de algún modo.
- **Exposición común a la vulnerabilidad (CVE**) – Lista de entradas con un número de identificación, una descripción y, al menos, una referencia pública de las vulnerabilidades públicamente conocidas.
- **Sistema común de puntuación de vulnerabilidades (CVSS)**[20] – Puntuación numérica que indica la gravedad de una vulnerabilidad.
- **Lista de puntos débiles comunes (CWE)**[21] – Lista formal de tipos de puntos débiles de *software* creada para:
  - servir de lenguaje común para describir los puntos débiles de seguridad de *software* en los ámbitos de la arquitectura, el diseño o el código;
  - servir de referencia para medir la eficacia de las herramientas de seguridad de *software* cuyo objetivo es eliminar esos puntos débiles;
  - servir de norma básica para la identificación, la mitigación y la prevención de puntos débiles.
- **Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPPA)**[22] – Ley estadounidense diseñada para la protección de la confidencialidad de los expedientes médicos de los pacientes y demás información facilitada a los planes sanitarios, los médicos, los hospitales y otros profesionales de la salud.
- **Indicadores fundamentales de rendimiento**[23] – Valor mensurable que demuestra la efectividad con que una empresa alcanza sus objetivos clave. Las organizaciones utilizan IFR a múltiples niveles para evaluar su capacidad de alcanzar 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.
- **Norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS)**[24] – Norma de seguridad de la información que promueve la seguridad de los datos del titular de la tarjeta en todo el mundo.
- **Tasks** – Lista de acciones que deben realizarse para realizar la tarea.

[20] https://www.first.org/cvss/
[21] https://cwe.mitre.org/about/index.html
[22] https://www.medicinenet.com/script/main/art.asp?articlekey=31785
[23] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator
[24] https://www.pcisecuritystandards.org/pci_security/