Marco de servicios del CSIRT de Gobierno

1.- Objetivo

El marco de servicios es un documento conceptual que describe de manera estructurada una serie de servicios de seguridad informática y funciones conexas que ofrece el CSIRT de Gobierno en caso de incidentes de seguridad informática y otros equipos que prestan servicios relacionados con la gestión de incidentes.

2.- Contexto

A) Gestión de eventos de seguridad de la información

La cual tiene por objeto identificar los incidentes de seguridad de la información a partir de la correlación y el análisis de los eventos de seguridad de muy diversos eventos y fuentes de datos contextuales, esta tarea, es realizada por el equipo SOC en la modalidad 7*24.

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

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

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

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

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

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

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

B) Gestión de incidentes de seguridad de la información

Este ámbito de servicio constituye el núcleo del CSIRT y consiste en servicios que son esenciales para ayudar a las instituciones durante un ataque o incidente. CSIRT deben estar preparados para ayudar y apoyar. Gracias a esta posición y experiencia únicas, son capaces no sólo de recopilar y evaluar informes de incidentes de seguridad de la información, sino también de analizar los datos relevantes y realizar un análisis técnico detallado del propio incidente y de cualquier dispositivo utilizado. A partir de este análisis, se pueden recomendar medidas de mitigación y de recuperación del incidente, y se ayudar a las instituciones a aplicar las recomendaciones

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

- Aceptación del informe de incidentes de seguridad de la información.
- Análisis de incidentes de seguridad de la información.
- Análisis de dispositivos y pruebas forenses.
- Mitigación y recuperación.
- Coordinación de incidentes de seguridad de la información.
- Ayuda en la gestión de crisis.

B.1) Aceptación del informe de incidentes de seguridad de la información

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

Descripción: Para el CSIRT, la tarea más importante es la aceptación de los informes sobre los eventos de seguridad de la información y los posibles incidentes de seguridad de la información que afecten a las redes, dispositivos, componentes, usuarios, organizaciones o la infraestructura –a los que se hace referencia como "víctimas"– en el conjunto de mandantes.

Para el registro de eventos, el CSIRT de Gobierno pone a disposición de las instituciones tres formas de contacto, con tal de notificar los incidentes de seguridad de la información con mayor eficacia. Para tener una referencia le recomendamos revisar la Guía de Notificación de Incidentes realizada por CSIRT, la cual la podrá encontrar en el siguiente link: https://www.csirt.gob.cl/media/2021/10/Guia-de-notificacion-ciberincidentes.pdf.

Formulario de registro de incidente en el sitio web: www.csirt.gob.cl

Correo electrónico: soc@interior.gob.cl

Numero de emergencia de registro de incidentes: 1510

B.2) Análisis de incidentes de seguridad de la información

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

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

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

- Clasificación de incidentes de seguridad de la información (prioridades y clasificación).
- Recopilación de información.
- Coordinación de análisis detallados.
- Análisis de causas fundamentales del incidente de seguridad de la información.
- Correlación entre incidentes.

B.3) Análisis de los artefactos y de pruebas forenses

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

Descripción: Los servicios relacionados con la comprensión de las capacidades y la intención de los artefactos (por ejemplo, malware, ataques, volcados de memoria volátil o copias de disco, códigos de aplicaciones, registros, documentos), los mecanismos utilizados, su propagación, detección, mitigación y su desarme o neutralización. Esto se aplica a todos los formatos y fuentes: hardware, firmware, memoria, software, etc. Todo artefacto o prueba debe ser preservado y recopilado sin alteración alguna, y mantenerse aislado.

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

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

B.4) Mitigación y recuperación

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

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

Se considera que las siguientes funciones forman parte de la implementación de este servicio: establecimiento de un plan de respuesta;

- Medidas ad hoc y contención
- Restauración de sistemas.
- Ayuda a otras entidades de seguridad de la información.

B.5) Coordinación de incidentes de seguridad de la información

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

Descripción: Es fundamental para todos los interesados y las organizaciones afectadas que se les notifique y mantenga informados sobre los pormenores y las actividades en curso en relación con un incidente de seguridad de la información. Dado que algunas actividades imprescindibles para la mitigación y recuperación satisfactorias pueden requerir la aprobación de la administración, es indispensable establecer funciones adecuadas de tramitación y notificación antes de poder gestionar eficaz y eficientemente cualquier incidente de seguridad de la información.

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

- Distribución de notificaciones.
- Distribución de información pertinente.
- Coordinación de actividades.
- Notificación.
- Comunicación a los medios.

B.6) Ayuda en la gestión de la crisis

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

Descripción: Si bien los incidentes de seguridad de la información de hoy en día raramente constituyen una crisis organizacional o nacional, en realidad tienen el potencial para ello. Pero la respuesta a una crisis suele asociarse a una emergencia que amenaza el bienestar de las personas y de la sociedad en general, o al menos la existencia de una organización. Conforme a lo dispuesto en la gestión de crisis, un alto cargo asumirá la responsabilidad de una crisis, alterando así la jerarquía habitual durante la emergencia. Dado que los sistemas y redes pueden contribuir a las emergencias o deben estar disponibles para responder a una situación de crisis, el CSIRT es un recurso fundamental para la gestión de esas situaciones y aportará su valiosa experiencia, pero también se ha de contar con los servicios y redes de puntos de contacto establecidos.

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

- Distribución de información a las instituciones.
- Informe sobre el estado de la seguridad de la información.
- Comunicación de decisiones estratégicas.

B.7) Gestión de vulnerabilidades

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

Se considera que los siguientes servicios se ofrecen en este ámbito de servicios: descubrimiento/investigación de vulnerabilidades;

- Admisión de informes de vulnerabilidades.
- Análisis de vulnerabilidades.
- Coordinación de vulnerabilidades.
- Divulgación de vulnerabilidades.
- Respuesta a vulnerabilidades.

B.8) Descubrimiento/investigación de vulnerabilidades

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

Descripción: El descubrimiento de una nueva vulnerabilidad es el primer paso necesario para iniciar el ciclo de vida de la gestión general de vulnerabilidades. Este servicio incluye aquellas funciones y actividades que el CSIRT puede realizar activamente a través de su propia investigación u otros servicios para descubrir una nueva vulnerabilidad.

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

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

B.9) Análisis de vulnerabilidades

Finalidad: Analizar y comprender las vulnerabilidades confirmadas.

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

vulnerabilidad se producen con otros participantes en un proceso coordinado de divulgación de la vulnerabilidad (CVD)

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

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

B.10) Coordinación de vulnerabilidades

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

Descripción: La gestión de la mayoría de las vulnerabilidades implica notificar, colaborar y coordinar el intercambio de información relevante con múltiples partes, tales como los inspectores/informadores de vulnerabilidades, los proveedores afectados, los programadores, los EIISP u otros expertos de confianza

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

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

B.11) Divulgación de vulnerabilidades

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

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

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

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

B.12 Respuesta a vulnerabilidades

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

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

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

- detección/exploración de vulnerabilidades;
- reparación de vulnerabilidades

B.12) Transferencia de conocimientos

Por la naturaleza de sus servicios, el CSIRT, está en una posición única para recopilar datos pertinentes, realizar análisis detallados e identificar amenazas, tendencias y riesgos, así como para crear las prácticas idóneas operativas actuales que ayuden a las organizaciones a detectar, prevenir y responder a los incidentes de seguridad. La transferencia de estos conocimientos a las instituciones es fundamental para mejorar la seguridad cibernética en general. Se considera que este ámbito de servicio en particular presta los siguientes servicios:

- Concientización y sensibilización;
- formación y educación;
- asesoramiento técnico y de políticas;
- asesoramiento legal

B12.1) Concientización y sensibilización

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

Resultado: Se logra que los mandantes sean conscientes de:

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

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

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

B12.2) Formación y educación

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

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

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

B12.3) Asesoramiento técnico y de políticas

Finalidad: Garantizar que las políticas y procedimientos de las instituciones incluyan consideraciones adecuadas de gestión de incidentes y, en última instancia, les permitan gestionar mejor los riesgos y amenazas

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

- ayuda en la gestión de riesgos;
- evaluar la madurez de las instituciones
- ayuda en la planificación de la continuidad de las actividades y la recuperación en caso de catástrofe;
- ayuda en materia de política mediante el traspaso de matrices de políticas;
- asesoramiento técnico.

B13.4) Asesoramiento legal

Finalidad: Entregar una guía y traspaso de conocimiento, cuando los incidentes de seguridad revistas los caracteres de delito, así como la prevención de ilícitos a través de la baja o revocación de inscripción de dominios que puedan usarse con fines fraudulentos

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

- Notificación de inscripción dominios en Nic Chile
- Asesoría jurídica para la revocación temprana
- Asesoría en la baja de sitios fraudulentos
- Asesoría legal en la denuncia y querella por infracción a la ley 19.223

Control de Cambio

Versión	Fecha	Autor	Cambio Realizado	Revisado por	Aprobado por
V1	3 de agosto de 2021	Equipo CSIRT		Katherina Canales	Carlos Landeros

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.19 17:03:50 -03'00'