Estableciendo un CSIRT

Martijn van der Heide

Traducción al Español:
Ernesto Pérez Estévez y Paul F. Bernal Barzallo
CSIRT CEDIA
https://csirt.cedia.org.ec

Version 1.3.1-es (Setiembre 2020)

Tabla de Contenidos

Introducción

Con Internet siempre en expansión y el hecho de que cada vez más organizaciones que son críticas para el funcionamiento de las naciones requieren Internet estos días, la estabilidad y la disponibilidad se vuelven aún más importantes.

La Infraestructura Crítica (ej: Sectores financieros, de Energía, Transporte o Gobierno) depende cada vez más de las posibilidades de los ciudadanos para acceder a sus servicios a través de Internet. Al mismo tiempo, estos servicios requieren cada vez más de Internet para proveerse de servicios. Además: procesos primarios de muchas organizaciones se han vuelto dependientes de la disponibilidad de Internet.

En la actualidad una falla de Internet de varias horas es inaceptable y una falla suficientemente larga puede realmente desestabilizar la economía. Organizaciones que usan tiendas virtuales enfrentan severos impactos incluso por pequeñas fallas.

Si vemos reportes noticiosos, incluso una falla de Facebook de 15 minutos se vuelven titulares a nivel mundial. No sólo fallas, también se reportan diariamente filtraciones de información a nivel mundial, robo o destrucción de información de usuarios y de propiedad intelectual como una forma de vandalismo o de espionaje corporativo en muchos casos.

Los incidentes cuestan, son caros. Hay un costo directo en cuanto a pérdida de ingresos y ganancias así como también costos relacionados con la contención y solución de un incidente, pero también enfrentamos costos indirectos relacionados con daño a las marcas, pérdida de clientes, reclamos por parte de los usuarios o incluso multas de parte de entes reguladores. Existen varios casos documentados en los cuales los incidentes de seguridad han traído consigo la quiebra de organizaciones porque no se han podido recuperar de estos.

Cada vez que se tiene un incidente de seguridad, una respuesta rápida y adecuada es la clave. Y es aquí donde los CSIRTs entra en la ecuación.

Un CSIRT es un equipo de expertos en seguridad de TI que responde a amenazas o incidentes de seguridad de la información. Los CSIRT tienen la capacidad y competencia para detectar y manejar estos incidentes y/o amenazas así como de ayudar a sus miembros a recuperarse de estos ataques.

De forma proactiva un CSIRT puede ofrecer diversos servicios con la finalidad de mitigar vulnerabilidades y riesgos, hacer conciencia y educar a sus miembros con el desarrollo y mejora de los servicios de seguridad de ellos.

Público Objetivo

Este manual se creó para organizaciones que quieren aprender más sobre equipos CSIRT y cómo comenzar su propio CSIRT.
Describe tanto el proceso de crear un CSIRT y los requerimientos para esto. Cuando ha sido posible se dan ejemplos para mostrar cómo se puede llevar a cabo cada paso.
El público objetivo son aquellas personas a nivel gerencial, pero este manual puede ser utilizado directamente por el staff de operaciones y también como una guía de referencia.

Terminología

Tenemos varios términos asociados con los equipos de seguridad los cuales veremos mientras investigamos sobre esta área en Internet. Trataremos de explicar los más comunes aquí.

CERT, o Computer Emergency Response Team
"CERT" es una marca registrada del Centro de Coordinación CERT (CERT/CC)[1], que es parte del Software Engineering Institute (SEI) de la Universidad Carnegie Mellon (CMU), EEUU.
Este fue el primero grupo de respuesta a incidentes en ser creado, en respuesta a una falla masiva causada en la institución por parte del gusano Morris[2] en 1988.
Si un equipo desea utilizar el término "CERT" como parte de su nombre, se requiere la firma de un acuerdo de uso con el registrante de la marca.[3]

CSIRT, o Computer Security Incident Response Team
Es una forma genérica de describir a un equipo de respuesta a incidentes. Su función es idéntica a la de un CERT pero, como se indicó anteriormente, el término CERT es una marca registrada. En este manual utilizaremos el término CSIRT.

ISAC, o Information Sharing and Analysis Center
Es una plataforma de cooperación para equipos de seguridad en el mismo sector o con un objetivo común. Este puede ofrecer muchos de los servicios de un CSIRT pero no hace manejo de incidentes.

SOC, o Security Operating Center
Es un área física o una ubicación dentro de un edificio donde se realiza monitoreo en tiempo real y el despacho y coordinación de incidentes, es similar a cómo los ISP tienen sus NOCs (Network Operating Centers) pero en este caso el SOC es para eventos de seguridad.
Normalmente sólo CSIRTs avanzados u organizaciones muy grandes con muchos activos de TI ubicados en diversos lugares son los que necesitan de un SOC.

No hay una distinción visible entre las actividades de un CSIRT y las de un SOC, existe mucho solapamiento entre las funciones de ambos; además, un CSIRT puede estar localizado dentro de un SOC mientras otras organizaciones utilizan al SOC como primera línea de su CSIRT.

Cualquiera sea el término utilizado, y cualquiera sea el nombre que se le dará al team (si es que se le da alguno), lo más importante es tener la competencia para hacerlo.

Estructura de este manual

El capítulo 1 proveerá una visión estructurada para guiar en el ciclo de vida y madurez del equipo.
Los capítulos 2-4 describirán los diversos pasos que se requerirán para llegar a planificar, obtener aprobación de gerencia y comenzar el equipo CSIRT.
Aunque es mejor que tengamos un involucramiento de parte de la gerencia durante el proceso, escogimos agregar la aprobación definitiva en la segunda fase, pues encontramos que es normal que gerencia requiera una propuesta clara y completa antes de dedicarse a tiempo completo a la idea.
El capítulo 5 describe los servicios más importantes de un equipo, el manejo de incidentes.

---

[1] CERT/CC: <https://www.cert.org/>
[2] The Morris Worm: <https://en.wikipedia.org/wiki/Morris_worm>
[3] Mayor información y el proceso para aplicar a una licencia de uso pueden ser encontrados en su sitio web: <https://www.cert.org/incident-management/csirt-development/cert-authorized.cfm>

El capítulo 6 detalla los últimos pasos: agregar servicios adicionales al catálogo de servicios del CSIRT.

Nota legal

Este manual ha sido desarrollado con el objetivo de apoyar a CSIRTs existentes y CSIRTs futuros en su implementación y operación durante su fase de inicio así como durante la vida del equipo. El contenido está basado en el conocimiento colectivo y la experiencia de la comunidad de CSIRTs y no representa solamente la visión de ThaiCERT y ETDA. Puede no describir el estado del arte en esta materia y podrá ser actualizado de tiempo en tiempo.

Se han realizado citas a terceros. ThaiCERT no es responsable del contenido de fuentes externas a las que hace referencia este manual, incluidos sitios web, ni de su disponibilidad.

Donde se mencionan productos específicos, esto no significa que ThaiCERT apoya o promueve estos, sino que sirven de ejemplos solamente.

Este manual persigue solamente objetivos educativos e informativos. Ni ThaiCERT ni ninguna persona actuando en su nombre es responsable por el uso que se le pueda dar a la información contenida en este manual. Toda la información contenida es provista tal cual sin ningún tipo de garantía. ThaiCERT/ETDA no promete ni ofrece resultados específicos, efectos ni consecuencias del uso de la información aquí contenida.

Reconocimientos

ThaiCERT quisiera agradecer a todas las instituciones e individuos que contribuyeron a este manual. En especial, un agradecimiento especial a:

CERT/CC y especialmente al equipo de desarrollo de CSIRT, cuya Descripción del Servicio ha sido íntegramente utilizada en el capítulo 6.
ENISA, por su conocimiento sobre el personal, las leyes y los reglamentos.
El equipo de TRANSITS por sus sugerencias en el proceso de manejo de incidentes.
A todos los que amablemente apoyaron con la revisión por pares de este manual.

Nota de los traductores

Este manual ha sido traducido en Enero del 2020 por el equipo CSIRT del CEDIA, la Red Avanzada del Ecuador, con el mero interés de aportar con documentación en Español para la formación y operación de equipos de respuesta en la región de latinoamérica y España.
En caso de encontrarse inconsistencias o fallas gramaticales, de concepto y ortográficas en la traducción al Español, rogamos se contacte a csirt -arroba- cedia.org.ec con información del particular.

[4] Creative Commons License: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Revisiones del documento

Version	Date	Remarks
1.0	June 2016	First publication
1.1	July 2016	Small number of changes from peer-review
1.2	November 2017	Brought up-to-date plus expanded on team maturity (new paragraph 1.1)
1.2-es_EC	Enero 2020	Traducción al Español de la versión 1.2
1.3-ec_EC	Julio 2020	Primera publicación al Español
1.3.1-es_EC	Setiembre 2020	Correcciones menores a la versión Español.

1. Gestión del ciclo de vida del equipo

Implementar un equipo CSIRT tiene varias facetas y factores a considerar e implementar. Es recomendable utilizar un enfoque de gestión de proyectos e implementar el ciclo de Deming (Planificar-Hacer-Verificar-Actuar, PHVA)[5] para la mejora continua.

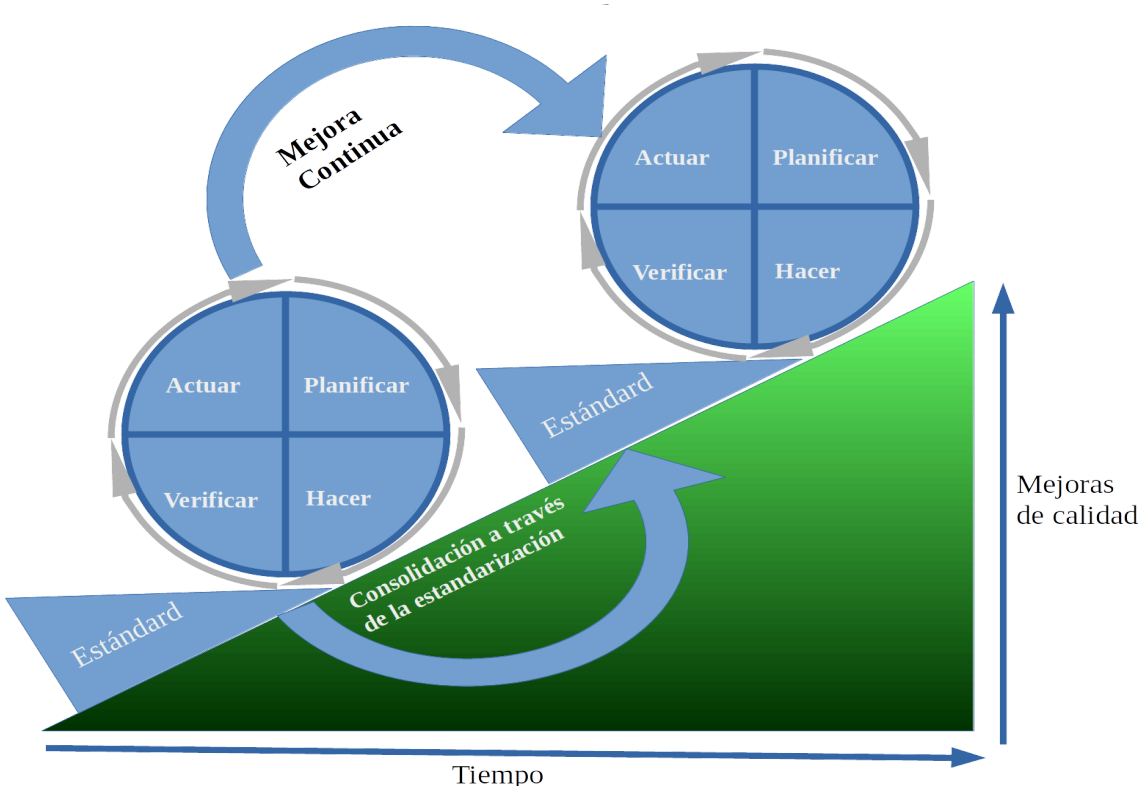

Figure 1: Ilustración del ciclo de Deming (Ciclo PHVA). Mejoras continuas a la calidad se logran iterando en el ciclo y consolidando el progreso logrado a través de la estandarización (Johannes Vietze)

El equipo de manejo del proyecto debería, idealmente, incluir en rol consultivo a un auspiciante ejecutivo, que sea familiar con la alta gerencia de la organización, los objetivos del negocio y la estrategia, y que pueda ayudar a obtener apoyo para los planes de formación del equipo CSIRT. Existen casos de estudio sobre la formación de un equipo CSIRT los cuales describen el camino que han seguido con el objetivo de apoyar a futuros teams en su creación, como por ejemplo:

AusCERT[6]
Una institución financiera[7]
CERT Polska[8]

[5] Ciclo de Deming: <https://es.wikipedia.org/wiki/Ciclo_de_Deming>
[6] AusCERT: <https://www.auscert.org.au/render.html?it=2252>
[7] Financial Institution: <http://www.cert.org/incident-management/publications/case-studies/afi-case-study.cfm>
[8] CERT Polska: <https://www.terena.org/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>

Como referencia adicional, KPN (Royal Dutch Telecom) ha publicado en línea su Marco de ciberseguridad[9], el cual puede ser utilizado también como punto de inicio.

PLANIFICAR

Definir el Marco del CSIRT

Se describe en el capítulo 2, además del Apéndice A: Template del marco de un CSIRT.

Definir presupuesto

Definir un presupuesto plurianual, diferenciar entre costos operativos y costos de inversión

No sobrecargar los gastos ni rellenar el presupuesto.

Ser tan sucinto como sea posible y considere tantos los tangibles como intangibles.

Crear un plan de negocio

Estudie ejemplos y sitios de apoyo en planes de negocio.

Su auspiciante ejecutivo seguramente le podrá apoyar en esta parte.

El plan de negocio debe reflejar los objetivos del CSIRT para la organización y cómo estos objetivos trabajan en conjunción con el presupuesto.

Hable sobre el retorno de la inversión (ROI).

Presente su presupuesto y plan

Como se indica en el capítulo 3.

Investigue de forma tal que en este punto sea capaz de defender su presupuesto y la necesidad de cada punto del plan.

Presente el plan, primeramente, a su auspiciante ejecutivo de forma tal que pueda recibir retroalimentación de una fuente que le apoya en el proyecto.

Entonces preséntelo a la directiva, la cual es la responsable de aprobar sus planes y financiamiento.

HACER

Implemente lo planificado

Tal y como se describe en el capítulo 4.

- Cree una información general de las fuentes de información.
- Cree una política de manejo de incidentes.
- Cree una política de manejo e intercambio de información.
- Evalúe la base instalada de la Comunidad objetivo.
- Comunique de la existencia de su CSIRT.
- Construya una red de confianza, asista a conferencias y seminarios.
- Practique el proceso.

Realice las operaciones rutinarias para el manejo de incidentes (capítulo 5) y otros servicios fundamentales (capítulo 6).

VERIFICAR

Analice el desempeño del equipo

Enfóquese en flujos, procesos y tareas importantes

- Aquellos que se realizan frecuentemente.
- Los que tienen una ejecución inconsistente.
- Aquellos que podamos mejorar porque tenemos el control.

Usa métricas y medidas apropiadas

- Recuerde: “tenemos lo que podemos medir”

[9] KPN (Royal Dutch Telecom): <https://github.com/KPN-CISO/kpn-security-policy>

- Las métricas tienen que finalizar con incentivos apropiados

Involucre a los miembros del equipo

- La inclusión y el involucramiento nos llevan a compromisos compartidos por todos
- Comparta lo que ellos hacen bien y también en lo que pueden mejorar.
- Si este existe: Trabaje con el departamento de aseguramiento de la calidad (QA),
- Considere usar un consultante externo y facilitador.

Entreviste a su Comunidad objetivo

- Qué está haciendo bien el CSIRT
- En qué áreas puede mejorar

Gestión general de la calidad

- ¿El team trabaja de acuerdo a procesos y estándares?
- ¿Se ha documentado todo?
- ¿Todos conocen dónde puede encontrarse la documentación?
- ¿Se crean minutas de las reuniones? ¿Están estas minutas disponibles para referencia futura?
- ¿Cómo se trabaja en equipo y cómo se mantienen actualizados sobre incidentes en curso?
- ¿Quién asistió a cuáles entrenamientos, conferencias y seminarios?

ACTUAR

Decida qué mejoras o adiciones realizar

Como resultado de la fase VERIFICAR, se pueden conocer qué mejoras realizar a las operaciones.

A medida que el equipo madura, pueden irse necesitando o deseando servicios adicionales, tales como se describe en el capítulo 6.

Comience una nueva fase PLANIFICAR con el objetivo de implementar estas mejoras y comenzar un nuevo ciclo de mejora continua.

Una vez establecido el equipo, el ciclo PHVA se sugiere se realice anualmente, coincidiendo con el año fiscal de la organización con la finalidad de asegurar que los requerimientos del CSIRT sean incluidos en el presupuesto del siguiente año.

1.1 Midiendo y mejorando la madurez

Una forma de ver la selección de servicios es de acuerdo al modelo de madurez del CSIRT, este puede ir de un modelo estrictamente reactivo hasta la implementación de servicios proactivos y de manejo de la calidad. Este esquema ha sido ideado por ThaiCERT.

En este manual, el CSIRT más simple que describimos es una organización de nivel 2 (Básico).

Nivel de MAdurez	Descripción
1. Introductorio	El CSIRT existe como un Punto de Contacto (POC) para coordinación y resolución de incidentes. Tiene sus reglas y regulaciones para notificar a las autoridades relevantes.
2. Básico	Igual a 1, adicionando un proceso para manejar nuevas amenazas. Se utiliza un sistema de tickets para manejar los incidentes reportados y se proveen avisos para la organización.

3. Activo	Igual a 2, adicionando herramientas de análisis de amenazas y procedimientos para la clasificación y el manejo de incidentes.
4. Proactivo	Igual a 3, adicionando diseminación de información de seguridad, herramientas para verificar y mantener el estado de la seguridad y planificación de entrenamientos a miembros del equipo.
5. Comprensivo	Igual a 4, pero con monitoreo en tiempo real de incidentes y amenazas. Se definen y comparten a lo interno y terceros instrucciones para nuevas amenazas y formas de prevenir incidentes con la finalidad de generar conciencia.

Las iniciativas de madurez de un CSIRT hacen referencia a los cinco pilares de madurez de un CSIRT:

Bases
Plan de negocio, entender restricciones legales
Organización
Mandato y otras estructuras organizacionales internas dentro de la organización y la coordinación con otros CSIRT
Humano
Personal del equipo, estructura, experiencia, código de conducta y opciones de entrenamiento
Herramientas
Todo lo que se requiera para realizar las tareas antes mencionadas
Procesos
Para manejo de amenazas e incidentes o la interacción con los medios

Trusted Introducer desarrolló un estándar para el modelo de madurez de un CSIRT basándose en 3 niveles[10]:

1. Listado
2. Acreditado
3. Certificado

El proceso de certificación se basa en SIM3 tal y como explicamos en el siguiente párrafo.

ThaiCERT fue el primer team no europeo en ser acreditado en el 2015.

1.1.1 SIM3: El Modelo de Manejo de Madurez de Incidentes de Seguridad

Este modelo fue desarrollado con la finalidad de permitir la medición del nivel de madurez de un equipo de seguridad o respuesta a incidentes utilizando cuatro áreas: organización, aspectos humanos, herramientas y procesos. Es usado como apoyo en el marco de certificación de Trusted Introducer y además está siendo adoptado por varias organizaciones de miembros como FIRST y la Nippon CSIRT Association (NCA).

El modelo de madurez SIM3[11] se basa en tres elementos básicos:

1. Parámetros de madurez
2. Cuadrantes de madurez
3. Niveles de madurez

[10] Proceso del Trusted Introducer: <https://www.trusted-introducer.org/processes/overview.html>
[11] SIM3 model: <https://www.trusted-introducer.org/SIM3-Reference-Model.pdf>

Los parámetros son las cantidades que se usan para medir la madurez – existen unas 40 que se detallan posteriormente. Cada parámetro pertenece a un de los 4 cuadrantes – los cuadrantes son entonces las 4 principales categorías de los parámetros:

O – Organización (11)
H – Humano (7)
T – Herramientas (Tools) (10)
P – Procesos (17)

Estos 4 cuadrantes han sido escogidos de tal forma que estos son mutuamente independientes dentro de lo posible.

Lo que realmente se mide son los Niveles de cada Parámetro. Se deseó y encontró una simplicidad a través de un conjunto único de niveles, válidos para todos los parámetros en todos los cuadrantes:

0 = no disponible / indefinido / desconocido
1 = implícito (conocido/considerado pero no ha sido escrito, “en la cabeza”)
2 = explícito interno (escrito pero no formalizado)
3 = explícito formalizado (sellado, aprobado, publicado)
4 = sujeto a procesos de control / auditado / puesto en vigor)

1.1.2 Autoevaluación del nivel de madurez del CSIRT

Existen auto-evaluaciones en línea, basadas o similares a SIM3:
GCCS and NCSC-NL[12].
ENISA[13].

[12] CSIRT Maturity Quick Scan: <https://check.ncsc.nl/>
[13] CSIRT Maturity - Self-assessment Survey: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey>

2. Redactando el marco de trabajo del CSIRT

El marco de trabajo del CSIRT describe en detalle qué hará el CSIRT, para quién, y qué recursos se requerirán para entregar estos servicios.
Aunque cada CSIRT es diferente de los demás, existen varios elementos que aplican a cada equipo. Un template de estos elementos se proveen en el Apéndice A: Template del marco de trabajo del CSIRT.
Seguiremos las mejoras prácticas internacionalmente aceptadas, con la finalidad de hacer fácil la posibilidad de que posteriormente nos podamos incorporar a iniciativas internacionales de cooperación; sus procesos de aplicación como miembros normalmente requieren los mismos elementos que serán trabajados aquí, de esta forma, al tenerlos ya disponibles, el proceso de incorporación será más fácil.
Debido a su alcance tan completo, el marco de trabajo puede ser utilizado para anunciar el CSIRT a la Comunidad objetivo y al mundo (ver también 4.5)
Siempre que sea posible, usaremos ThaiCERT de ejemplo para cada elemento.

2.1 Misión

La misión del team debe ser documentada. En ella se explica el propósito y función del CSIRT de una forma clara y debe contener un bosquejo de los objetivos fundamentales del equipo.
Es una muy buena práctica el hacer que la misión sea compacta (unas 2 a 3 oraciones) pero no muy corta, pues se tiene que evitar ambigüedad ya que la misión será la misma durante un par de años. La misión describe el objetivo principal del equipo en el futuro.

ThaiCERT es el CERT nacional de Tailandia, su misión es hacer al ciberespacio y las transacciones electrónicas más seguras actuando como punto de contacto para incidentes de seguridad informática de la comunidad de Internet de Tailandia.

2.2 Comunidad objetivo

La Comunidad objetivo, conocida en Inglés como constituency es quiénes reciben los servicios del CSIRT.
El entender quién es la Comunidad objetivo del CSIRT ayuda al equipo a determinar cuáles son las necesidades que ellos tienen, qué activos necesitan ser protegidos y cuál va a ser la interacción con el CSIRT.
Cada equipo debe tener una Comunidad objetivo claramente definida. De existir solapamiento con algún otro equipo esto debe ser dado a conocer a la Comunidad objetivo para que tengan claro qué servicio solicitar a cada equipo.
Podemos verificar la Comunidad objetivo del CSIRT a través de charters, misión, documentos de operaciones o cualquier documento similar, o documentos que describan el propósito y función del CSIRT.
ENISA[14] define los siguientes 'sectores' en los que un CSIRT trabaja:

Sector	Enfocado en	Comunidad objetivo
CSIRT Académico	Instituciones académicas y educativas, tales como universidades o institutos de investigación así como sistemas relacionados con la conectividad a Internet orientadas a la academia.	Staff universitario y estudiantes.

[14] De ENISA "A step-by-step approach on how to set up a CSIRT", page 8

CSIRT Comercial	Servicios comerciales. Puede ser una organización independiente, un ISP o similar.	Usuarios de pago.
CSIRT de Infraestructura crítica	Protección de infraestructura crítica y/o Protección de información y protección de infraestructura. Cubre la parte de TI de la infraestructura crítica de un país.	Gobierno, sectores con o en el área de infraestructura crítica y ciudadanía.
CSIRT del Gobierno	Sirve al gobierno en sí	Agencias gubernamentales.
CSIRT Interno	Sirve a la propia organización.	Staff interno y departamento de TI.
CSIRT Fuerzas armadas	Organizaciones militares con responsabilidades en infraestructura de TI	Staff de instituciones militares o relacionadas con lo militar como por ejemplo el ministerio del área.
CSIRT Nacional	Se enfoca en lo nacional, considerado el punto de contacto central del país.	No tiene Comunidad objetivo directa aunque en algunas ocasiones el CERT nacional se combina con el CERT gubernamental.
CSIRT sector PYMEs	CSIRT organizado con la finalidad de proveer sus servicios a sus miembros o grupo de interés.	Las PYMEs y su staff.
CSIRT de fabricantes/PSIRT	Orientado a productos específicos de un fabricante, usualmente se orienta a solucionar vulnerabilidades de sus productos o apoyar en soluciones de mitigación ante un ataque. PSIRT es una forma común de llamarles: Product Security Incident Response Team.	Fabricantes, dueños de un producto.

ThaiCERT es el CERT nacional de Tailandia, además de ser el CSIRT gubernamental; por tanto su Comunidad objetivo está compuesta por todas las personas, redes y organizaciones en Tailandia.

2.3 Autoridad

La autoridad de un equipo indica lo que éste está autorizado a hacer. Puede variar desde un rol meramente de apoyo o ayuda hasta una autoridad completa con la finalidad de deshabilitar servicios vulnerables o comprometidos.
En sentido general, se sugiere que un CSIRT sea solamente responsable por los aspectos técnicos y no en aspectos regulatorios o administrativos que busquen reprimir o castigar, esto es importante pues la Comunidad objetivo podría dejar de reportar incidentes por miedo a ser castigados o reprimidos.

ThaiCERT coordina los incidentes de seguridad relacionados con sus miembros y no tiene otro mandato adicional.

2.4 Responsabilidad

Es lo que se espera que un CSIRT haga con sus miembros para cumplir con su función.
De forma general, esto incluye los servicios típicos del catálogo de servicios del CSIRT (le describiremos en el capítulo 6), pero el CSIRT puede tener funciones adicionales tales como relaciones específicas y responsabilidades con reguladores o fuerzas del orden.

Cuando deban agregarse estas funciones, se debe tener un especial cuidado que no ocurran conflictos de intereses, como por ejemplo cuando a un CSIRT se le dan tareas operativas cuando a la vez tiene como rol el supervisar esas mismas tareas.
En el caso de CSIRTs Nacionales y Gubernamentales, esta responsabilidad usualmente está definida en forma de Ley.

ThaiCERT maneja todo tipo de incidentes de seguridad informática. Además, ThaiCERT provee recomendaciones técnicas y operativas así como avisos, concienciación, entrenamiento y consultoría.

2.5 Estructura organizacional

A este punto también se le conoce como Afiliación o Auspiciante.
Indica la posición del CSIRT dentro de la organización o la Comunidad objetivo.
Muchos equipos nacionales están ubicados dentro de organizaciones gubernamentales, mientras otros pueden estar asociados a una empresa comercial, Red Nacional de Investigación (NREN) o Universidad.

2.5.1 Modelo de negocio independiente

En este modelo, el CSIRT es una organización independiente, con su propia estructura de dirección, empleados y equipo de apoyo. Este modelo puede ser aplicable a CSIRT comerciales.

2.5.2 Modelo incrustado (embebido)

Para CSIRTs internos es normal ubicarlos dentro del departamento de TI. Esto tiene sentido pues mucho de lo que el CSIRT hará está relacionado directamente con los sistemas de TI de la organización. En organizaciones muy grandes este no puede ser el lugar adecuado; un CSIRT busca proteger todos los activos de información de la compañía, no sólo de TI.
Si el CSIRT es ubicado “muy abajo” en la estructura organizacional, puede ser simplemente considerado como “el juguete de TI” y carecer de apoyo del resto de la organización. De la misma forma, si es ubicado muy “arriba”, los empleados pueden verle como la torre de marfil e ignorarlo en su conjunto.
En la actualidad se está evidenciando una lenta tendencia de ubicar a los CSIRTs más arriba con la finalidad de servir de mejora manera a la organización.
El CSIRT debe poderse encontrar en el organigrama de la organización o en algún tipo de anuncio por parte de la alta directiva.
Donde quiera que sea que esté ubicado un CSIRT, es crucial mantenerse en continuo contacto con los departamentos.

Existen algunos posibles modelos para organizar físicamente un CSIRT en dependencia de la estructura de la organización:

- Centralizado: todos los miembros del equipo del CSIRT están ubicados en la misma oficina.
- Distribuído: los miembros del CSIRT están situados en más de un lugar, por ejemplo si se tienen diversas ubicaciones en la organización. Este requiere alguna coordinación para trabajar en conjunto en el día a día.
- Distribuído en zonas horarias: para multinacionales. Esta es una versión avanzada del modelo distribuído, llamados a veces ‘siguiendo al sol’. En este modelo, la oficina operacional del CSIRT cambia a medida que avanza el día en una zona horaria. Para cada oficina operacional, las horas de trabajo pueden ser horas regulares de trabajo, luego de lo cual la oficina en otro país toma el mando.

2.5.3 Modelo campus

Como sugiere su nombre, este modelo se adopta normalmente por parte de CSIRTs académicos o de investigación, aunque también aplica a CSIRTs del sector de las Fuerzas Armadas y a CSIRT de PYMEs. En este caso, los miembros (universidades o empresas) pueden o no tener su propio CSIRT, en dependencia del tamaño y presupuesto, y un CSIRT madre o central se constituye para coordinar los esfuerzos del sector y actuar como punto de contacto hacia el mundo exterior.
Este CSIRT central puede ser una organización independiente o estar embebido en una.

Para los miembros sin su propio CSIRT dedicado, el CSIRT central puede proveer todos los servicios de un CSIRT para ellos.

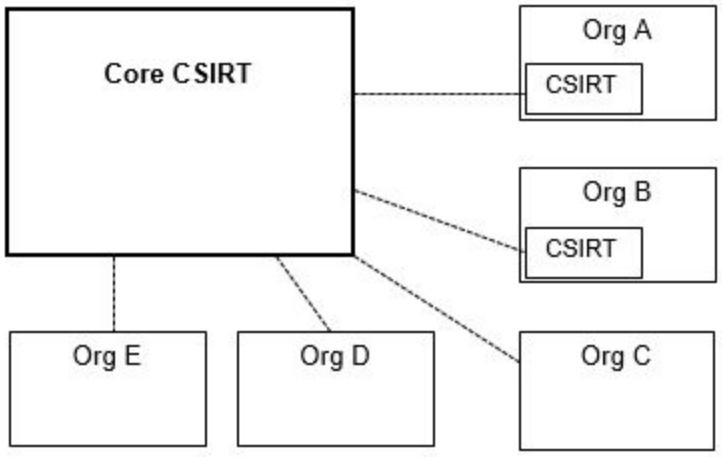

Figura 2: Estructura organizacional del modelo campus

ThaiCERT es parte del gobierno Tailandés y opera desde una oficina de una de sus agencias. Como tal, ThaiCERT es un equipo centralizado-embebido.

2.6 Disponibilidad

La disponibilidad de los servicios de un CSIRT dependen de las horas de trabajo de la organización donde éste se ubique.
Excepto que un CSIRT esté disponible 24x7, se deben hacer provisiones para receptar reportes de incidentes fuera de las horas de oficina. Esto puede ser tan simple como que todos los correos recibidos sean revisados la siguiente jornada laboral, otra forma es tener un técnico del equipo de guardia para monitorear reportes enviados y decidir si este puede esperar hasta que comience la jornada laboral o se requiere acción inmediata.

Es importante considerar el ambiente de trabajo de la organización cuando se vaya a determinar su horario de operación. Por ejemplo, si el departamento de TI está solamente disponible durante horario de oficina, podría no tener mucho sentido que el CSIRT opere 24x7 pues los problemas no podrán ser resueltos fuera del horario de oficina.

Tenga en cuenta que el tener personal atendiendo fuera de horario de oficina puede hacer que la organización tenga costos extras a pagar por concepto de horarios nocturnos, horas extras u otras causales de ley.

ThaiCERT estaba disponible solamente en horario de oficina hasta inicios del 2015, con un número de emergencia para caso de requerirse contacto fuera de este horario. Actualmente está disponible 24x7.

2.7 Servicios fundamentales

Existen muchos servicios que un CSIRT puede ofrecer, pero en un principio no es necesario ofrecer más que uno o dos de estos. Hablaremos sobre los servicios en el capítulo 6.
Para ser apropiadamente llamado un equipo CSIRT, la respuesta a incidentes es un servicio requerido. Hablaremos sobre esto en el capítulo 5.,
Un servicio normalmente requerido es el de Anuncios de seguridad.

ThaiCERT ofrece muchos de los servicios cubiertos en el capítulo 6.

2.8 Requerimientos de personal

2.8.1 Cantidad

No existe un cálculo exacto de la cantidad de personal técnico necesario para mantener un equipo CSIRT, cada CSIRT es diferente, trabaja en ambientes diferentes y tiene diferente cantidad de Comunidad objetivo.
Sin embargo, si partimos de una experiencia colectiva por parte de la comunidad de CSIRTs, los siguientes valores han probado ser una buena aproximación:

Para poder entregar 2 servicios centrales: Respuesta a Incidentes y Anuncios, un mínimo de **4 empleados a tiempo completo** son sugeridos.

Para un CSIRT con mayor cantidad de servicios, que opere en horario de oficina y mantenga sus propios sistemas se sugiere un valor **entre 6 y 8 empleados a tiempo completo**.

Para una operación 24x7 (3 turnos diarios), el mínimo recomendado es de 12 empleados a tiempo completo.

Estos números incluye redundancia para personal que sale de vacaciones o por enfermedad.

El staff de ThaiCERT es de 30 empleados.

2.8.2 Competencias

A continuación haremos una pequeña panorámica de las competencias esenciales que se requieren para el equipo técnico del CSIRT, tal y como sugiere ENISA[15]. Se podrían requerir certificaciones y diplomas para avalar estas competencias.
En dependencia de los servicios que se van a entregar se podrían requerir habilidades o competencias adicionales a los especialistas.

A continuación algunos puntos que deben considerarse en sentido general para el staff:
Competencias personales

Flexible, creativo y con espíritu de equipo
Sólidas habilidades analíticas
Capacidad de explicar asuntos técnicos con palabras fáciles

[15] De ENISA “A step-by-step approach on how to set up a CSIRT”, pág. 25

Disposición a mantener la confidencialidad y trabajar de forma procedimental
Buenas habilidades organizacionales
Resistente al stress
Sólidas habilidades comunicativas y de escritura
Abierto de mente y con deseos de aprender

Competencias técnicas

Amplio conocimiento de tecnologías de internet y protocolos
Conocimiento de SO Linux y Unix (en dependencia del equipamiento de la Comunidad objetivo)
Conocimientos sobre SO Windows (en dependencia del equipamiento de la Comunidad objetivo)
Conocimientos de equipamiento de infraestructura de red (Router, switches, DNS, Proxy, Mail, etc.)
Conocimiento de aplicaciones de Internet (SMTP, HTTP(s), FTP, telnet, SSH, etc.)
Conocimiento de amenazas de seguridad (DDoS, Phishing, Desfiguración de sitios web, sniffing, etc.)
Conocimiento de evaluación de riesgos e implementaciones prácticas

Competencias adicionales

Disposición para trabajar 24x7 o en turnos de guardia (en dependencia del modelo de servicio)
Distancia máxima dispuesto a viajar (en caso de emergencia; tiempo máximo de viaje)
Nivel de educación
Experiencia de trabajo en el campo de seguridad de TI

2.8.3 Código de conducta/ética

Un código de conducta o de ética es un conjunto de reglas o guías para staff del CSIRT que describe cómo se debe comportar profesionalmente durante su jornada laboral y, potencialmente también, fuera del horario de oficina. El comportamiento fuera de la oficina es muy relevante, porque se espera de parte del personal del CSIRT que se comporten responsablemente en privado así como en ambientes de TI y seguridad.
Un buen ejemplo del código de conducta es el “CSIRT Code of Practice” de Trusted Introducer.[16]

Debemos asegurar que el staff es confiable y evitar contratar a (ex-)crackers. Al CSIRT le tomará al menos un año generar confianza a su Comunidad objetivo y a sus pares por lo que no se puede arriesgar perder esta confianza repentinamente. Realizar una depuración al momento de contratar a sus empleados es una buena práctica.

ThaiCERT usa el “CSIRT Code of Practice” de Trusted Introducer.

2.8.4 Entrenamiento

Un plan de entrenamiento del equipo incluye dos fases o entrenamientos: entrenamiento interno para el staff que recién ingresa que le permite aprender sobre cómo opera el CSIRT, y un entrenamiento con terceros con miras a mejorar continuamente las habilidades y mantenerse al día con los nuevos desarrollos en la tecnología (incluídos también las nuevas amenazas y métodos de ataque).

Se puede obtener entrenamiento externo de alta calidad para su CSIRT en:

[16] Trusted Introducer CSIRT Code of Practice: <https://www.trusted-introducer.org/CCoPv21.pdf>

TRANSITS[17]
CERT/CC[18]
SANS Institute[19]
FIRST[20]

si es posible, asegúrese de que también se reserve presupuesto para asistir a conferencias y seminarios como parte del entrenamiento contínuo. (ver 4.6).

ThaiCERT practica todo lo anterior.

2.9 Infraestructura y herramientas

Las instalaciones del CSIRT y la infraestructura de red y telecomunicaciones deben ser diseñadas con gran cuidado para no solamente proteger la información sensitiva recolectada por el CSIRT sino además para proteger al staff del CSIRT.
Las áreas de almacenamiento de la información y de trabajo del equipo deben ser construidas y protegidas de la misma forma y cumplir los mismos requerimientos que un datacentro.

Consideraciones sobre la seguridad física

Ubicar los servidores del CSIRT y repositorios de datos en locales seguros o en el Centro de operaciones de seguridad (SOC) Secured rooms or security operations center (SOC).
Deben tenerse espacios seguros y a prueba de sonidos para la discusión de actividades e investigaciones del CSIRT.
La documentación no electrónica y notas físicas debe almacenarse en un depósito seguro que no pueda ser accedido por personas no autorizadas.
Los documentos físicos que ya no sean necesarios deben ser destruidos mediante una trituradora o herramientas que los vuelvan inutilizables (ej: pulso electromagnético).
El personal del CSIRT debe estar separado físicamente de otras partes de la organización, debe mantenerse algún tipo de control de acceso.
Debe mantenerse una política para el acceso de invitados a las instalaciones si es que no existe dentro de la política de control de acceso.

Consideraciones sobre el equipamiento de TI

Mecanismos de comunicación seguros tales como teléfonos seguros, faxes o correo electrónico.
Sistemas endurecidos, incluidas las computadoras de escritorio.
La red del CSIRT debe estar separada de la red de la oficina.
Espacio para re-instalar rápidamente sistemas que han estado fuera del área segura o usados para análisis de malware.

Consideraciones sobre herramientas específicas para el CSIRT

Sistema de tickets.
Base de datos de contactos de los equipo del CSIRT, miembros (constituency) y otros Puntos de contacto (POC) de Interés.
Cualquier otro material requerido para entregar servicios de importancia al team.

[17] TRANSITS: <https://www.terena.org/activities/transits/>
[18] CERT/CC: <http://cert.org/training/>
[19] SANS Institute: <https://www.sans.org/>
[20] FIRST: <https://www.first.org/>

En Apéndice C: Herramientas de seguridad se mencionan herramientas que los CSIRT usan frecuentemente.

Algunos servicios del CSIRT, tales como forensia digital, pueden tener requerimientos de TI o físicos específicos.

ThaiCERT usa todo lo anterior.

2.10 Relaciones internas y externas

Con la finalidad de obtener apoyo y reconocimiento de su organización, es importante construir una buena relación de trabajo. Cuando ocurren incidentes, necesitarás de otros para resolver el problema o para realizar consultas sobre posibles acciones. Relacionarse con ellos hará que este proceso sea mucho más rápido y fluído.
Las relaciones con los departamentos de operaciones (IT, network) son de gran ayuda pero además con otros como el de seguridad física, comunicaciones, legal y recursos humanos.

Relaciones con terceros en su comunidad pueden rendir un buen beneficio, por ejemplo con su CSIRT nacional, fuerzas del orden o el ente regulador. Si existen CSIRTs por sectores o ISAC en su sector[21], debería considerar afiliarse a ellos.

Ver 4.6 para conocer ejemplos de iniciativas de colaboración internacional que pueden beneficiar a su equipo.

ThaiCERT mantiene todas las relaciones anteriores.

2.11 Modelo de financiamiento

Para asegurar estabilidad a largo plazo, el CSIRT requiere el diseño de un modelo de financiamiento que provea ingresos que garanticen la operación continua del equipo y la provisión continua de servicios del CSIRT a sus miembros.
El modelo de financiamiento debe cubrir no solamente inversiones iniciales (CAPEX) sino además costos operacionales recurrentes (OPEX) para cubrir pagos a personal, instalaciones, licencias de software y otros costos requeridos para la entrega de servicios y su apropiado mantenimiento.

El modelo de financiamiento puede ser:

- Un centro de costo dentro de la organización (la cual cubre los gastos y no recibe ingresos por su operación), o
- El equipo puede ser financiado de forma total o parcial por subsidios, tener en cuenta entonces:
  - ¿Quién otorgará los subsidios?
  - ¿Cuál es el propósito del subsidio?
  - ¿De qué valor serán los subsidios? ¿Cuánto tiempo de operación cubrirá?
  - ¿Cuán confiable o segura es la fuente de financiamiento?
  - ¿Cuánto tiempo lleva esta fuente de financiamiento activa?
- El equipo debe detallar el subsidio, incluir quién lo entregará, la fuente de esos ingresos, el propósito y la duración de este.
- El equipo puede también vender sus servicios ya sea de forma interna o externa (a través de un cargo o costo a sus clientes internos o externos), o

[21] Ver ThaiCERT: “Establishing a Sector-based ISAC”

Financiado a través de un consorcio de organizaciones tales como universidades o redes de investigación.

o una combinación de las fuentes anteriormente mencionadas.

ThaiCERT es financiado completamente por el gobierno y además provee diversos servicios especializados por un costo.

3. Obtener la aprobación de gerencia

El apoyo al CSIRT debe provenir de los más altos niveles gerenciales de la organización (de preferencia de la junta directiva si la empresa es comercial, o por parte del ministerio o gabinete para un CSIRT gubernamental). Esto es importante por las siguientes razones:

- Para asegurar que las políticas a nivel organizacionales sean implementadas y de obligatorio cumplimiento.
- Para asegurar apoyo en caso de que tengan que tomarse acciones críticas o que incurran en altos costos.
- Para asegurar la continuidad de las operaciones durante reorganizaciones o cortes de presupuesto.

Cuando se presenten los planes para la implementación del CSIRT, tenga en cuenta que gerencia ve de forma diferente a TI y que hablan un idioma diferente del de las personas técnicas. Para convencer a la alta gerencia de que un CSIRT puede ayudarles en los objetivos del negocio hacen falta argumentos de negocio en vez de argumentos técnicos.

Estos argumentos pueden ser:

- Requerimientos legales o contractuales que exigen la implementación de ciertos niveles de seguridad de la información.
- Tener un CSIRT entrenado y equipado puede ayudar a reducir las pérdidas por caídas o fallas en el servicio producto de incidentes informáticos pues la organización podrá contener o recuperarse de forma más expedita, esto es: el CSIRT puede ahorrar dinero.
- Servicios preventivos pueden reducir vulnerabilidades y amenazas antes de que estos sean explotados.
- Centralizar la seguridad de la información en un CSIRT ahorrará el hecho de que cada departamento tenga que duplicar los esfuerzos de seguridad y puede mejorar la línea base de seguridad de la organización como un todo.
- En dependencia del sector, el tener un CSIRT puede ser una ventaja competitiva.
- Desde el punto de vista de las relaciones públicas, el tener un CSIRT muestra un compromiso con la seguridad (“Ustedes están seguros con nosotros”).
- “Nuestra competencia ya lo hace.”

3.1 Acordar una estructura de reportes para mantener a involucrados e interesados

Usualmente la misma estructura de reportes utilizada para cualquier otro departamento dentro de la organización será suficiente, por ejemplo mediante reuniones regulares además de reportes trimestrales y anuales.
Sin embargo es importante tener en mente que el CSIRT es usualmente un centro de costos mientras pueda ahorrarle dinero a la organización. Por lo tanto, si es posible, debemos agregar valores que permitan visualizar el ahorro que representó a la organización para mostrar cómo se contribuye al resultado financiero.

Para la transparencia gubernamental, ThaiCERT publica estadísticas mensuales sobre incidentes en el sitio web y además publica un detallado reporte anual en forma electrónica y en impresos.

4. Planificar el equipo y ambiente de trabajo

4.1 Crear una descripción general de las fuentes de información

Crear y mantener una lista de todas las fuentes que se usará

- Para detectar automáticamente potenciales incidentes
- Para ser alertados de los incidentes por parte de terceros (ej. e-mail, teléfono, formulario web).
- Para obtener información sobre amenazas y vulnerabilidades.
- Para comunicarse directamente con los miembros durante un incidente (lista de puntos de contacto).
- Para comunicaciones generales con la Comunidad objetivo (concienciación, relaciones públicas).

4.2 Crear una política de manejo de incidentes

La política de manejo de incidentes debe definir quién tiene la responsabilidad para manejar qué tipo de incidente de seguridad y quién puede ser llamado para apoyar en la implementación de la respuesta en las otras áreas de la organización.
Esto incluye:

- Los tipos de incidentes que caen dentro de la jurisdicción o experticia del CSIRT
- Quién maneja el análisis y la respuesta
- Qué acciones deben tomarse con los entes de justicia, si se requiere
- Qué hacer con los reportes y actividades fuera del alcance del CSIRT

La política debe delinear el proceso a seguir a la hora de manejar un incidente. Debe incluir:

- Tiempos de respuesta
- Métodos de escalamiento
- Cómo clasificar y priorizar los incidentes
- Cómo se rastrean y guardan los incidentes
- Cuándo y cómo se cierran los incidentes
- Cómo buscar apoyo para el análisis o la implementación de las medidas de mitigación o estrategias de recuperación.

En el capítulo 5 tendremos una visión más completa del proceso de respuesta a incidentes.

4.3 Crear una política de manejo e intercambio de información

La clasificación de la información describe la categorización o clasificación de la información incluyendo distinciones entre la información sensitiva, confidencial o pública y cómo cada una es manejada durante el almacenamiento, tránsito, acceso, etc.
Estas clasificaciones deben aplicarse a la información en cualquier medio, ya sea electrónico o físico.
Un sistema de clasificación frecuentemente usado es el Traffic Light Protocol (TLP).[22]

La política debe incluir cuál tipo de información debe mantenerse solamente dentro de las instalaciones del CSIRT y cómo la información debe ser manejada en laptops y otros dispositivos móviles. Esta debe además detallar qué tipo de información puede o no ser discutida a través de dispositivos móviles o no

[22] Traffic Light Protocol: <https://www.us-cert.gov/tlp>

asegurados así como cuál información debe ser almacenada y discutida de forma segura así como también la información que se puede compartir con personas no autorizadas.
La política debe definir la forma en que la información recibida de otros CSIRT debe ser manejada, protegida y compartida dentro del CSIRT y dentro de la organización.

4.3.1 Leyes y regulaciones

Como cualquier organización, el CSIRT se rige por leyes y acuerdos internacionales.
Los estándares no son de obligatorio cumplimiento pero pueden ser dispuestos o recomendados por leyes y regulaciones. De la misma forma, los contratos comerciales con los clientes pueden requerir la implementación de estándares específicos.

A continuación una pequeña lista de posibles leyes y políticas relativas al CSIRT[23]:

Nacionales

- Leyes sobre TI, telecomunicaciones y medios
- Leyes sobre la protección de datos y privacidad
- Leyes y regulaciones sobre retención de datos
- Legislación sobre finanzas, contabilidad y manejo corporativo
- Códigos de conducta para gobernanza y gobernanza de TI
- Para Tailandia: Computer Crimes Act and Electronic Transactions Act (article 35)[24]

Internacional

- Acuerdo de Basilea II (en especial lo relacionado con el manejo del riesgo operacional)
- Convención sobre el cibercrimen del Consejo de Europa
- Convención sobre los derechos humanos del Consejo de Europa (art. 8 de la privacidad)
- Junta de Normas Internacionales de Contabilidad (IAS; en cierta medida requieren controles de TI)

Estándares

- British Standard BS 7799 (Seguridad de la Información)
- International Standards ISO2700x (Sistema de Gestión de Seguridad de la Información)
- German IT-Grundschutzbuch, French EBIOS y otras variantes nacionales

Hay que tener en cuenta que los aspectos legales no solamente aplican a la información que se maneja localmente, además aplica a cualquier intercambio de información con pares extranjeros.
Notar además que las leyes y regulaciones pueden limitar el tipo de acciones que son permitidas durante la respuesta a un incidente (ej: sniffers de tráfico para analizar un ataque pueden no ser permitidos por razones de privacidad).

Algunos países tienen leyes que requieren notificar al ente regulador en caso de que ocurra una duga de datos. Una vez el CSIRT entra en operación, este proceso de notificación puede ser incorporado a sus procesos (como parte de sus responsabilidades, ver 2.4).

---

[23] De ENISA “A step-by-step approach on how to set up a CSIRT”, page 28
[24] Para guías de implementación del Electronic Transactions Act, ver “Information Technology Law” del ETDA’s ICT Law Center

Para finalizar, Internet está en un continuo y rápido crecimiento y las leyes normalmente están yendo detrás de la tecnología. Como resultado, actualmente no hay leyes en varias áreas, no todas las leyes han sido probadas en la corte e incluso algunas leyes pueden entrar en conflicto con otras.

Para determinar si su CSIRT está cumpliendo con las legislaciones nacionales e internacionales sugerimos busque ayuda legal y verifique que su organización pueda cumplir con lo que usted tiene planificado hacer.

4.3.2 Comunicaciones seguras con PGP

Como PGP o GPG son recomendados como forma de comunicación segura en la comunidad de CSIRTs (y requerido para la mayoría de las Comunidad objetivo), se debe describir y detallar cómo se usa PGP en el equipo CSIRT.
Aunque es solamente una recomendación, se vuelve obligatorio y usted desea pertenecer a organizaciones como FIRST o Trusted Introducer.

Consideraciones generales sobre la políticas de claves:

- ¿Quién debe tener claves? (managers, equipo de respuesta, etc.)
- Cómo se crearán, gestionarán, distribuirán y archivarán las claves
- Problemas comunes con las claves, tales como:
  - Quién creará las claves
  - Qué tipo de clave deberá crearse
  - Cuál será el tamaño de la clave
  - Expiración de las claves
  - Se requerirá de certificado de revocación
  - Dónde se almacenarán las claves y sus revocaciones
  - Quién necesitará firmar una clave
  - Políticas de claves incluyendo custodia de la clave
  - Quién gestiona las claves y políticas relacionadas así como procedimientos para la gestión de las claves.

4.4 Evaluar la base instalada de la membresía

Crear y mantener una visión general de los productos de software y hardware (y sus versiones) comúnmente utilizadas en la Comunidad objetivo, para poder ofrecer asesoría específica.

Alternativamente, si el CSIRT proporciona un servicio de notificaciones, se podría pedir a la Comunidad objetivo que se suscriba a los avisos para los productos que utilizan, de una lista de todos los productos posibles (para que mantengan efectivamente su propia descripción general del producto).

4.5 Comunicar la existencia del CSIRT

Una vez establecido, es importante informar regularmente a la comunidad que el equipo existe, cómo interactuar con él y qué se puede esperar del mismo.

En particular, si un CSIRT tiene la intención de servir como un punto de contacto único para los informes de incidentes de seguridad para su Comunidad objetivo, debe asegurarse de que todos los interesados sepan informar incidentes directamente al CSIRT. Del mismo modo, otras partes que puedan necesitar el apoyo de un constituyente (por ejemplo, durante un incidente) deben saber del CSIRT y de las interacciones que pueden esperar de él.

Una forma común de publicitar al centro es publicando un documento que describa el CSIRT y sus servicios, en la intranet (para equipos internos) o en Internet, por ejemplo, utilizando la plantilla RFC 2350 [25].

Independientemente de la relación (autoridad) del CSIRT con su membresía, debe hacer más que simplemente definir y publicitar la Comunidad objetivo a la que dice servir. No puede funcionar de manera efectiva sin ganar y mantener su confianza y respeto.

Esta confianza debe ganarse y cultivarse. A medida que el equipo gana la confianza y el respeto de su Comunidad objetivo declarada, más elementos de la Comunidad objetivo declarada comenzarán a reconocer y apoyar al equipo.

Se pueden publicar boletines informativos regulares sobre los incidentes manejados o, sobre una base más ad-hoc, temas para crear conciencia o compartir las lecciones aprendidas de amenazas o incidentes particularmente interesantes.

4.6 Construir una red de confianza, ir a conferencias y seminarios

Tenga en cuenta que cada organización enfrenta muchas veces las mismas amenazas y seguramente aprendió de esos incidentes. Al compartir experiencias y lecciones aprendidas, todos tenemos el beneficio de las Mejores Prácticas para mejorar la seguridad y mitigar amenazas e incidentes.

En estos días, los incidentes rara vez involucran solo 1 organización. En muchos casos, el atacante se encuentra en otro lugar, a menudo en un país diferente. Peor aún, un ataque puede involucrar muchas fuentes a la vez (ataques DDoS).

Para resolver tales incidentes, el equipo necesitará trabajar en conjunto con otros equipos, típicamente con los equipos donde se origina el ataque.

Hay varias organizaciones donde los equipos de CSIRT colaboran y se ayudan entre sí con capacitación, conocimiento y resolución de incidentes. Algunos ejemplos son FIRST (Forum of Incident Response and Security Teams)[26] donde varios cientos de equipos CSIRT en todo el mundo son miembros, APCERT (Asia Pacific CERT)[27] para CSIRT nacionales en la región de Asia Pacífico, Trusted Introducer[28] para todos los equipos CSIRT en Europa, o AfricaCERT[29] para equipos CSIRT en África.

Convertirse en miembro de tales organizaciones es muy beneficioso.

Esas organizaciones, así como varios otros equipos individuales más grandes de CSIRT, organizan regularmente conferencias y seminarios a los que se puede asistir para capacitación y como una oportunidad para establecer contactos con otros equipos de CSIRT y construir relaciones.

[25] RFC2350: <https://www.ietf.org/rfc/rfc2350.txt>
[26] FIRST: <http://www.first.org/>
[27] APCERT: <http://www.apcert.org/>
[28] Trusted Introducer: <https://www.trusted-introducer.org/>
[29] AfricaCERT: <http://www.africacert.org/>

4.7 Practicar los Procesos

Dado que los incidentes más grandes no ocurren con frecuencia, el equipo puede no tener suficiente experiencia con el proceso y los procedimientos involucrados. Además, los procedimientos pueden no funcionar bien o no cubrir todos los aspectos. Esto puede causar demoras innecesarias cuando se produce dicho incidente.
Una de las formas prácticas de entrenar y mejorar los procedimientos es mediante un ejercicio de mesa, simulando y resolviendo un incidente a través de un juego de roles.
ENISA ofrece gratuitamente, una gran cantidad de opciones de capacitación de procesos en línea.[30]

[30] Material de entrenamiento en línea de ENISA:
<https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>

5. Proceso de manejo de un incidente

La descripción en este capítulo es el proceso y el flujo de trabajo completos para un servicio básico de manejo de incidentes.
Cada uno de los pasos del flujo de trabajo se explicará en los siguientes párrafos.
Se proporcionará una selección de herramientas en el Apéndice C: Herramientas de seguridad

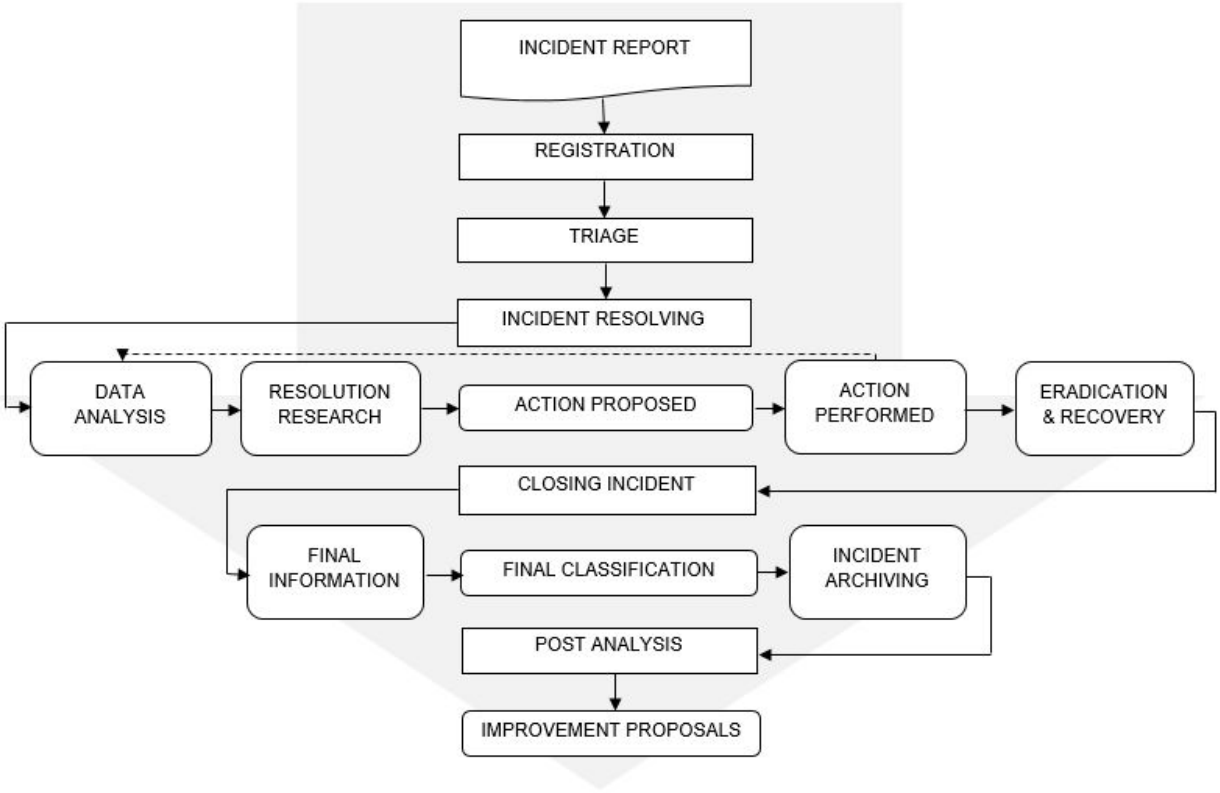

Figura 3: El flujo de trabajo del proceso de manejo de incidentes

5.1 Reporte de incidentes

5.1.1 Notificación

Los informes de incidentes pueden provenir de varias fuentes, ya sea por observaciones propias (monitoreo) o por notificaciones de otras fuentes.
Apéndice B: El formulario de ejemplo de Informe de incidentes, contiene una plantilla con todos los elementos de información que idealmente se deberían recibir en una notificación.

Para contacto directo, un equipo de CSIRT podría tener publicadas facilidades como:

- E-mail
- Teléfono
- Formulario web de contacto
- Redes sociales

Hay que tener cuidado de no crear un solo punto de falla al elegir las facilidades. Casi todas las opciones anteriores requieren acceso a Internet (y si se usa VoIP para los servicios telefónicos, todas ellas), por lo que una interrupción de Internet puede hacer que el equipo sea inaccesible. Se debe pensar en una instalación de respaldo.

Otras fuentes pueden incluir

- Eventos informados por la propia red de monitoreo
- Membresías a listas de correo de proveedores o grupos de seguridad
- Suscripciones a feeds automáticos, consulte el Apéndice D: Recursos de información
- Radio, televisión y periódico

5.1.2 Registro

Todas las notificaciones deben registrarse en un ticket. Este ticket se usará durante todo el proceso de manejo de incidentes.
A cada ticket se le debe asignar un número único, que es el número de referencia utilizado para todas las comunicaciones relacionadas con este incidente.

Muchos sistemas de tickets pueden configurarse para leer automáticamente una cuenta de correo electrónico. Todo el correo electrónico enviado a esa cuenta creará automáticamente un nuevo ticket (para nuevos incidentes) o agregará la comunicación a un ticket existente (si el número del ticket está incluido en el asunto del correo electrónico).

Es importante gestionar todos los incidentes desde un solo lugar (el CSIRT), incluso si la resolución del incidente real tiene lugar en otro sitio. Esto es necesario porque las notificaciones adicionales podrían estar relacionadas con tickets existentes, por ejemplo, un brote de virus podría provocar incidentes en varios departamentos, mientras que en realidad son todos el mismo incidente.
El registro central también permitirá reutilizar las comunicaciones y mitigaciones conocidas.

Los sistemas de tickets de uso común (gratuitos) de los CSIRT son RTIR (Request Tracker for Incident Response)[31] y OTRS (Open Technology Real Services)[32].

ThaiCERT usa RTIR como sistema de tickets.

5.2 Triage

Este es uno de los pasos más importantes en el proceso de manejo de incidentes, ya que este es el punto donde se toman las decisiones críticas.
Primero, se necesita verificación; ¿Es esto realmente un incidente? ¿Cuán confiable es la fuente de donde vino el informe?

Una vez que se ha establecido que efectivamente está ocurriendo un incidente:

- ¿Está este incidente en el alcance del CSIRT? ¿Pertenece a la Comunidad objetivo y es el CSIRT responsable de este tipo de incidente?
- ¿Cuál es el impacto?
- ¿Hay posible daño colateral?

[31] RTIR: <https://bestpractical.com/>
[32] OTRS: <https://www.otrs.com/>

¿Qué tan urgente es? ¿Puede el daño aumentar con el tiempo? ¿Se puede propagar a otros componentes?

Responder al notificador

Confirmar la recepción del informe.
Explicar cómo se realizará el procesamiento y qué se puede esperar.
Sugerir qué hacer mientras tanto, hasta que se resuelva el incidente

Las plantillas de respuesta pueden ser muy útiles y ahorrar tiempo.

5.2.1 Clasificación de Incidentes

Clasificar el incidente. Puede que no haya suficiente información disponible en este momento para clasificar con confianza, pero esto puede corregirse fácilmente más adelante.

La clasificación puede ayudar a determinar la gravedad y la prioridad y los recursos necesarios para manejar el incidente más adelante.

Ejemplo de gravedad y prioridad, tal como lo utilizan algunos gobiernos y grandes empresas:

Grupo	Severidad	Ejemplos
Rojo	Muy Alta	DDoS, sitio de phishing
Ambar	Alta	Troyano, acceso no autorizado
Amarillo	Normal	Spam, temas de copyright

Prioridad	Gobierno	SLA cliente	Otros
Rojo	1	1	2
Ambar	2	1	3
Amarillo	3	2	3

También provee una función estadística muy útil, permitiendo al CSIRT

reconocer tendencias en tipos de incidentes
proveer estadísticas/gráficos para gestión
compararlos con otros equipos de CSIRT

Algunas taxonomías comúnmente usadas (clasificaciones)[33] son:

Common Language for Incident Response (de CERT/CC)
eCSIRT.net taxonomy (desarrollada durante el proyecto eCSIRT.net)
Auto-definida por el equipo
Aunque definir una taxonomía propia podría encajar mejor en la organización, compararla con otros equipos podría ser complicado.
Además, hay que asegurarse de no crear una taxonomía demasiado compleja (ejm: un tipo de incidente diferente para cada tipo de malware); aunque esto podría crear una muy detallada visión de los tipos de incidentes manejados, también significa que se invertirá mucho tiempo en la determinación del tipo correcto, en lugar de resolver el incidente a mano.

ThaiCERT usa la taxonomía eCSIRT.net y publica estadísticas por mes de incidentes en el sitio web[34]. Un gráfico de ejemplo de los incidentes manejados en 2015:

[33] Full descriptions of these taxonomies can be found at <https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies>

[34] Estadísticas mensuales de ThaiCERT: <https://www.thaicert.or.th/statistics/statistics-en.html>

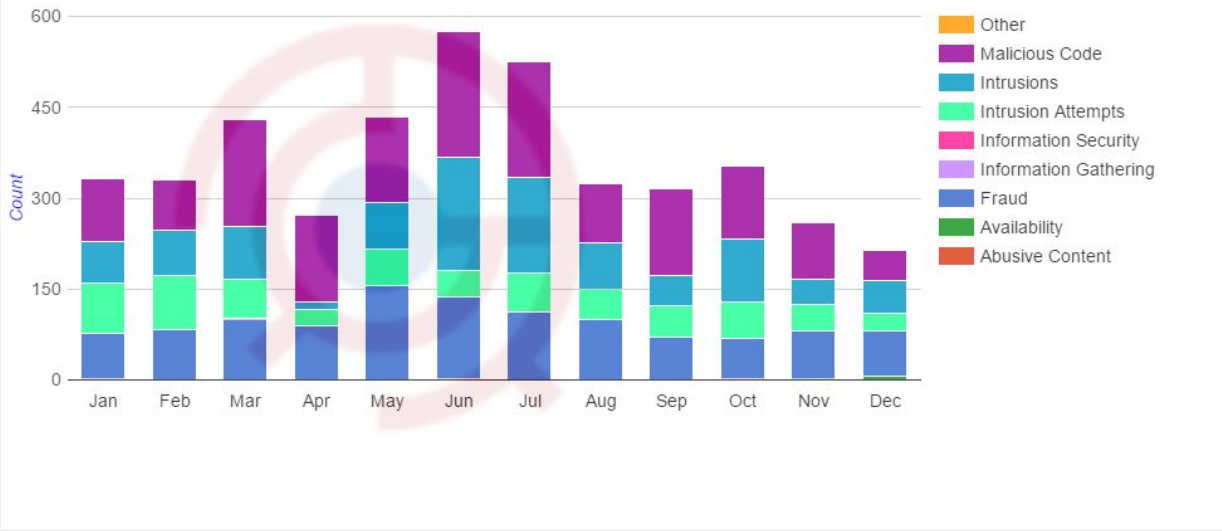

Figure 4: Estadísticas mensuales de incidentes de ThaiCERT

El paso final del triage es asignar uno o más responsables a este incidente, quienes ejecutarán las siguientes acciones.

5.3 Resolución de incidentes

5.3.1 Análisis de datos

En este paso trataremos de buscar tanta información como sea posible con la finalidad de obtener una visión más completa del incidente y su causa.

Recolectar datos del reporte y del entorno del sistema (o sistemas) afectado(s):

- Información de contacto detallada
- Descripción detallada del incidente
- Clasificación del incidente sugerida por quien lo reporta
- Sistemas operativos y disposición de la red
- Hora exacta y zona horaria del lugar del incidente
- Configuración de los sistemas de seguridad
- Severidad del incidente
- Archivos de log incluídos en el reporte

Existen varios repositorios donde podemos encontrar datos relacionados sobre el incidente:

- Netflow
- Logs de los routers
- Logs de servidores Proxy
- Logs de aplicaciones web
- Logs de servidores de correo
- Logs de DHCP
- Logs de servidores de autenticación
- Otras bases relacionadas con el incidente
- Equipos de seguridad como firewalls o logs de sistemas IDS

Podría requerirse información de terceros, cuando la fuente del ataque está fuera de nuestra membresía.

- Identifique a quién necesita contactar
- Notifíquese
- Solicítele, de forma amable, la información que le pueda ayudar

Aunque es importante obtener tanto detalle como sea posible, sea pragmático y no espere mucho por datos de terceros, el incidente puede continuar en curso y cualquier demora puede incrementar el problema o dar oportunidad al intruso para borrar sus trazas.
De forma general, el 20% de los datos pueden darnos el 80% del conocimiento necesario para encontrar una solución

5.3.2 Investigar formas de solución

Esta fase consiste en encontrar la mejor solución de un conjunto de posibles soluciones, basándonos en la información recopilada de la fase anterior.
Puede lograrse pensando o hablando sobre las observaciones y conclusiones obtenidas al momento, quizá comparando características de configuración de sistemas o instalaciones ya conocidas (ya sea que estén en uso o que su implementación sea positiva para este incidente).
Para incidentes más complicados, una buena alternativa es tener sesiones de lluvias de ideas.

5.3.3 Propuesta de acción

En dependencia de la complejidad del incidente, una o más acciones pueden ser requeridas para mitigar el incidente.
Debemos mantener nuestra audiencia en mente cuando estemos proponiendo acciones - los técnicos entenderán de soluciones técnicas, pero si, por ejemplo, se requiriera la adquisición de servicios adicionales o sea necesaria una medida financieramente costosa, sugerimos ajustar nuestro lenguaje para que pueda ser entendido por gerencia o financiero.

Las acciones pueden incluir

- Apagar un servicio
- Realizar un escaneo para buscar malware
- Parchear un sistema
- Endurecer un un sistema
- Aislar o enjaular un sistema o servicio
- Auditar un sistema
- Recolectar información adicional (quizá contratando a un tercero)
- Comprar un servicio (ej: protección anti DDOS)
- Escalar a un nivel gerencial más alto o buscar consejo legal
- Involucrar a Comunicaciones corporativas o a Relaciones públicas
- Involucrar a agencias de cumplimiento de la ley para realizar una investigación criminal
- Si el sistema o aplicación se provee por parte de un tercero (ej: basado en la nube, Github, Pastebin, redes sociales), se requiere enviarles una alerta y trabajar con ellos.

5.3.4 Acción realizada

Verificar la acción tomada:

- ¿Es el destino del ataque alcanzable, como se supone que debería ser?
- ¿La acción resolvió realmente el problema?

¿Se está filtrando apropiadamente el tráfico?

Si el objetivo del ataque sigue siendo vulnerable y/o la solución propuesta no resuelve el incidente por completo, repita los pasos anteriores para encontrar otras soluciones.

5.3.5 Erradicación y recuperación

Luego de que el incidente haya sido resuelto, el sistema puede ser limpiado y regresado a producción.
Hay que notar que algunas acciones podrían requerir más tiempo luego de que el incidente haya sido resuelto, por ejemplo, podría proceder una investigación penal.
Si los departamentos de Comunicación Corporativa o Relaciones Públicas han sido involucrados en el incidente, hay que asegurarse de que disponen de la información para actualizar sus comunicados.

5.4 Cerrando el Incidente

Debe existir una política muy clara de cómo y cuándo se puede proceder a cerrar un incidente. Esto porque el tiempo que un incidente permanece abierto puede ser utilizado como métrica de desempeño.
Algunos equipos escogen nunca cerrar los incidentes (pues puede llegar nueva información, aunque la mayoría de los sistemas de tickets permiten la re-apertura), algunas deciden que un incidente puede ser cerrado cuando está técnicamente resuelto, otros equipos cerrarán el incidente solamente después de que se han realizado acciones de seguimiento.

5.4.1 Información final

Asegúrese que toda la documentación de respaldo está incluida en el ticket.
Este es el momento de informar a las partes interesadas.

- Una breve descripción de lo que sucedió
- El resultado del trabajo de mitigación
- Hallazgos y recomendaciones

5.4.2 Clasificación final

Ahora que tenemos toda la información disponible sobre el incidente, es una buena práctica el verificar (y corregir si es necesario), la clasificación.
Si la clasificación original ha sido muy diferente de la que actualmente conocemos, quizá la función de triage puede beneficiarse de información adicional para mejorar la clasificación.

5.4.3 Archivo del incidente

El incidente ahora puede ser cerrado y archivado.

Se sugiere que los tickets cerrados permanezcan accesibles al equipo a través de un sistema que permita la búsqueda. Incidentes similares pueden ocurrir nuevamente y el poder consultar los pasos adoptados en incidentes similares puede ahorrar una enorme cantidad de tiempo.

5.5 Análisis ex-post

Se pueden aprender varias cosas de un incidente, con el objetivo de prevenir que estos vuelvan a suceder en el futuro o para mitigarlos rápidamente.

Ejemplos de lecciones aprendidas y propuestas de mejora:

- Adiciones o clarificaciones en la política de seguridad
- Mejoras en la arquitectura de red

- Mejoras en los mecanismos de detección
- Herramientas que pudieron haber mejorado el análisis
- Nuevos tipos de ataques

Los equipos CSIRT pueden compartir sus lecciones aprendidas con la comunidad de seguridad de forma tal que otros equipos puedan beneficiarse del conocimiento adquirido por estos (ver 4.6).

6. Agregar servicios según se requieran

A continuación tenemos una lista completa de servicios de CSIRT como los ha definido CERT/CC[35]:

Servicios Reactivos	Servicios Proactivos	Calidad de servicios de gestión de la seguridad
Alertas **Gestión de Incidentes** **Análisis** **Respuesta in situ** **Soporte de respuesta** **Coordinación de respuesta** Manejo de Vulnerabilidades Análisis Respuesta Coordinación de respuesta Gestión de Artefactos Analysis Respuesta Coordinación de respuesta	**Anuncios** Vigilancia Tecnológica Auditorías de seguridad o evaluaciones Configuración y Mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras Desarrollo de herramientas de seguridad Servicios de detección de intrusos Diseminación de Información relacionada con la seguridad	Análisis de riesgos Continuidad del negocio y plan de recuperación ante desastres Consultorías de seguridad Concienciación sobre seguridad Educación/Entrenamiento Evaluación de productos o certificación de estos

Los servicios marcados en **negritas** son los servicios mínimos que debe ofrecer un CSIRT al comenzar.

Luego de iniciado se pueden agregar otros servicios según se vaya requiriendo.
Los servicios deben seleccionarse cuidadosamente con el objetivo de dar un mejor servicio a la membresía con el presupuesto disponible, cada servicio adicional va a tener un impacto sobre los recursos requeridos, habilidades y convenios que se deban manejar por parte del CSIRT. Es preferible ofrecer menos servicios con alta calidad que ofrecer muchos servicios con baja calidad.

Además de proveer un servicio por el CSIRT mismo, algunos servicios se pueden tercerizar a otros equipos u organizaciones especializadas. Esto es una buena alternativa ante servicios que son muy caros y raramente necesarios como por ejemplo forensia digital.
El CSIRT puede seguir siendo el punto de contacto al adquirir un servicio de terceros.

Tengamos en cuenta que *ningún* CSIRT ofrece *todos* los servicios anteriormente listados.

[35] Del "Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd edition", pág 25

6.1 Descripción de los servicios[36]

6.1.1 Servicios Reactivos

Los servicios reactivos están diseñados para responder a las solicitudes de apoyo, reporte de incidentes de la membresía del CSIRT, y cualquier amenaza o ataque contra los sistemas del CSIRT. Algunos servicios se inician a través de una notificación de un tercero o mediante el monitoreo de logs y alertas de IDS.

Alertas y Avisos

Este servicio busca diseminar información que describe ataques, vulnerabilidades, alertas de intrusión, virus, o información engañosa. Provee recomendaciones sobre acciones a tomar a corto plazo para tratar de mitigar o resolver los problemas que provoca esta actividad. La alerta, aviso o información se envía como una reacción al problema que está sucediendo con la finalidad de notificar a los miembros de la actividad y proveerles guías que les ayuden a proteger sus equipos o sistemas que puedan ser afectados. La información puede haber sido generada por el mismo CSIRT o puede ser redistribuida de otros CSIRTs, fabricantes o expertos de seguridad, o de otros miembros del CSIRT.

Manejo de Incidentes

El manejo de incidentes consiste en recibir, realizar el triaje, responder a solicitudes y reportes, así como analizar incidentes y eventos. Específicamente se pueden realizar las siguientes actividades:

tomar acción para proteger sistemas y redes afectadas o amenazadas por intrusos
proveer soluciones y estrategias de mitigación ante alertas o avisos de relevancia
buscar actividad de intrusos en otras partes de la red
filtrado de tráfico de red
reconstruir sistemas
parchear o reparar sistemas
desarrollar estrategias para responder o mitigar la intrusión.

En vista de que las actividades de manejo de incidentes son implementadas de formas diferentes por cada CSIRT, este servicio se categoriza basada en el tipo de actividad que se desarrolla y el tipo de apoyo que se da:

Análisis de Incidentes

Existen varios niveles de análisis de incidentes y muchos sub-servicios. Fundamentalmente el análisis de incidentes consiste en examinar toda la información y evidencia disponible o artefactos relacionados con un incidente o evento. El propósito del análisis es identificar el alcance del incidente, y del daño causado por este, la naturaleza del incidente y estrategias de respuesta o de mitigación disponibles. El CSIRT puede usar los resultados del análisis de vulnerabilidades y de artefactos (descritas más abajo) para entender y proveer un análisis más actualizado y completo de lo que ha sucedido a un sistema específico.

El CSIRT correlaciona actividad entre incidentes con la finalidad de determinar cualquier interrelación, tendencias, patrones, o características propias de un intruso. Dos sub-servicios que pueden ser ofrecidos como parte de análisis de incidentes, en dependencia de la misión, objetivos y procesos del CSIRT son:

Recolección de evidencia forense

[36] From "Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd edition", page 25-34

Es la recolección, preservación, documentación y análisis de evidencia de un sistema comprometido para determinar los cambios realizados a este y para apoyar en la reconstrucción de los eventos que condujeron al ataque. Esta recolección de información y evidencia debe ser realizada de una forma que se documente una posible cadena de custodia que pueda ser admitida como evidencia por la justicia. Las tareas que usualmente se realizan durante la recolección de evidencia forense incluyen (pero no se limitan a) realizar una copia fiel bit a bit de los discos duros de los sistemas afectados; buscar cambios realizados al sistema tales como nuevos programas, archivos, servicios y usuarios; buscar procesos corriendo y puertos abiertos y; verificar troyanos y toolkits. El equipo de trabajo del CSIRT que realice estas acciones deben además estar preparados para actuar como perito judicial en procedimientos legales.

Trazas o búsqueda de trazas

Es el buscar el origen de un intruso o identificar los sistemas a los cuales un intruso ha tenido acceso. Dentro de esta actividad se puede además buscar trazas o tracear cómo el intruso entró al sistema o redes afectadas, qué sistemas fueron utilizados para obtener acceso, dónde se originó el ataque y, qué otros sistemas y redes fueron usados como parte del ataque. Puede además intentar determinarse la identidad del intruso. Este trabajo puede ser realizado independientemente aunque normalmente se busca colaboración con personal judicial o policiales, ISP y otras organizaciones involucradas.

Respuesta a incidentes in-situ

El CSIRT provee apoyo directo, en sitio, para apoyar a los miembros en la recuperación de un incidente. El CSIRT mismo analiza presencialmente los sistemas afectados y conduce labores de reparación y recuperación de los sistemas afectados en vez de solamente proveer apoyo telefónico o por email (ver más adelante). Este servicio incluye todas las acciones tomadas a nivel local que sean necesarias si se sospecha que un incidente ha ocurrido o está ocurriendo. Si el CSIRT no está ubicado en el sitio afectado, miembros del equipo viajarán al sitio y realizarán la labor de respuesta. En algunos casos puede existir un equipo ya en sitio que provea la respuesta a incidentes como parte de su labor rutinaria. Esto es especialmente cierto si el manejo de incidentes se provee como parte de las funciones del sistema, redes, o administrador de seguridad como parte o en nombre de un CSIRT ya establecido.

Apoyo a la respuesta a incidentes

El CSIRT apoya y guía a las víctimas de un ataque con la finalidad de que se puedan recuperar de un incidente. Esto vía email, teléfono o documentación. Puede incluir asistencia técnica en la interpretación de información recolectada, proveer información de contacto o guías para mitigar o recuperarse del incidente. No incluye acciones respuestas directas en sitio. El CSIRT provee guía, apoyo, remoto de forma tal que el personal del sitio pueda realizar la recuperación ellos mismos.

Coordinación de respuesta a incidentes

El CSIRT coordina los esfuerzos de respuesta entre las partes involucradas en un incidente. Usualmente incluye la víctima del ataque, otros sitios involucrados en el ataque, y cualquier otro sitio del que se requiera apoyo durante el análisis del ataque. Puede incluir a partes que provean apoyo de TI a la víctima tales como ISP, otros CSIRT, y administradores de sistemas y redes en el sitio. El trabajo de coordinación puede incluir el recolectar información de contacto, notificar a sitios de su posible involucramiento en el ataque (como víctima o como fuente del ataque), recolectar estadísticas sobre el número de sitios involucrados, así como facilitar el intercambio de información y análisis. Parte del trabajo de coordinación puede incluir notificaciones y colaboración con asesoría legal de una

organización, recursos humanos o relaciones públicas. Puede incluir relaciones con agencias de justicia o policiales.
Este servicio no incluye respuesta directa en sitio.

Manejo de vulnerabilidades

El manejo de vulnerabilidades incluye el recibir información y reportes sobre vulnerabilidades de Software y Hardware; analizar la naturaleza, mecánica utilizada y efectos de las vulnerabilidades; así como desarrollar estrategias de respuesta para detectar y reparar estas vulnerabilidades. Como las actividades de manejo de vulnerabilidades se implementan en diversas formas para cada CSIRT, este servicio se categoriza basado en el tipo de actividades que se desarrollan y el tipo de apoyo que se da:

Análisis de vulnerabilidades

El CSIRT realiza análisis técnico y examen de las vulnerabilidades en hardware o software. Esto incluye la verificación de vulnerabilidades sospechosas y examen técnico de software o hardware para determinar dónde está ubicada y cómo puede ser explotada. El análisis de vulnerabilidades puede incluir revisión del código fuente, usar un debugger para determinar dónde ha ocurrido la vulnerabilidad o tratar de reproducir el problema en un sistema de prueba.

Respuesta a vulnerabilidades

Este servicio consiste en determinar la respuesta adecuada para mitigar o reparar una vulnerabilidad. Puede incluir investigar o desarrollar parques, actualizaciones o soluciones alternativas. Puede además incluir el notificar a terceros de las estrategias de mitigación mediante la distribución de información con publicaciones de notas o alertas. Este servicio puede incluir también el proceso de respuesta mediante la implementación de parcheado, actualizaciones o soluciones alternativas.

Coordinación en la respuesta a vulnerabilidades

El CSIRT notifica a las diversas partes de la empresa o membresía sobre la vulnerabilidad y comparte información sobre cómo arreglar o mitigar la vulnerabilidad. El CSIRT verifica que la estrategia de respuesta a la vulnerabilidad ha sido aplicada exitosamente. Este servicio puede involucrar comunicaciones con fabricantes, otros CSIRTs, expertos técnicos, membresía e individuos o grupos que inicialmente descubrieron o reportaron la vulnerabilidad. Las actividades incluyen facilitar el análisis de la vulnerabilidad o reporte de vulnerabilidad; coordinar la publicación de documentos, parches o soluciones alternativas; y sintetizar los análisis técnicos realizados por terceros. Este servicio puede incluir además el mantener un archivo público o privado, o base de conocimientos con información sobre la vulnerabilidad y las estrategias de respuesta correspondientes.

Manejo de artefactos

Un artefacto es cualquier archivo u objeto encontrado en un sistema que pueda estar involucrado en sondeos o ataques a un sistema o red o que está siendo utilizado para saltarse medidas de seguridad implementadas. Los artefactos pueden incluir, pero no están limitados a: virus, troyanos, gusanos, scripts de exploits y toolkits. El manejo de artefactos consiste en recibir información sobre copias de artefactos que están siendo usados en ataques, reconocimiento y otras actividades no autorizadas o disruptivas. Una vez se recibe, el artefacto es revisado. Esto incluye analizar la naturaleza, mecánica, versió y uso del artefacto; así como desarrollar (o sugerir) estrategias de respuesta para detectar, remover y defenderse contra este. Puesto que las actividades de manejo de artefactos se desarrollan de diversas formas en dependencia del CSIRT, este servicio se puede categorizar basado en el tipo de actividades que se realizan y el tipo de apoyo que se ofrece:

Análisis de artefactos
El CSIRT realiza un examen técnico y análisis de cualquier artefacto que se encuentre en un sistema. El análisis a realizar puede incluir el identificar el tipo de archivo y estructura del artefacto, comparar un artefacto recién descubierto con otros artefactos o versiones ya existentes para buscar similitudes y diferencias, o realizar ingeniería reversa o desensamblado de código para determinar el propósito y función del artefacto.

Respuesta a artefactos
Este servicio consiste en determinar las acciones apropiadas para detectar y remover artefactos de un sistema, así como acciones para prevenir que artefactos sean instalados. Esto puede incluir crear firmas que puedan ser agregadas a antivirus o IDS.

Coordinación en la respuesta a artefactos
Este servicio consiste en compartir y sintetizar resultados de análisis y estrategias de respuestas sobre un artefacto con otros investigadores, CSIRTs, fabricantes, y otros expertos en seguridad. Las actividades incluyen notificar a terceros y sintetizar análisis técnicos de diversas fuentes. Las actividades pueden además incluir el mantener un archivo público o para los miembros sobre artefactos conocidos y su impacto y estrategias de respuestas correspondientes.

6.1.2 Servicios proactivos

Los servicios proactivos están diseñados para mejorar la infraestructura y procesos de seguridad de los miembros antes de que ocurra un incidente o evento, o que este sea detectado. Los objetivos principales son el reducir la ocurrencia de incidentes así como reducir su impacto y alcance cuando ocurran.

Anuncios
Incluye, pero no se limita a, alertas de intrusión, avisos de vulnerabilidades y avisos de seguridad. Estos avisos informan a los miembros sobre nuevos desarrollos en el mediano a largo plazo tales como nuevas vulnerabilidades encontradas y sobre herramientas de seguridad.
Los anuncios permiten a los miembros proteger sus sistemas y redes contra nuevos problemas encontrados antes de que estos puedan ser explotados.

Vigilancia tecnológica
El CSIRT monitorea y observa nuevos desarrollos tecnológicos, actividades de intrusos y tendencias con el objetivo de ayudar a la identificación de amenazas futuras. Los tópicos pueden ser expandidos para incluir acciones legales o legislativas, amenazas políticas o sociales así como tecnologías emergentes. Este servicio incluye la lectura de listas de seguridad, sitios web de seguridad y artículos de actualidad en revistas y periódicos en los campos de ciencia, tecnología, política y gobierno para extraer información relevante a la seguridad de los sistemas y redes de los miembros. Puede incluir comunicaciones con terceros que sean autoridades en estos campos para garantizar que se obtenga la mejor y más precisa información.
El resultado de este servicio puede ser algún tipo de anuncio, guías o recomendaciones enfocadas a problemas de seguridad en el mediano-largo plazo.

Auditoría o evaluaciones de seguridad
Este servicio provee una revisión detallada y análisis de la infraestructura de seguridad de una organización, basándose en los requerimientos definidos por la organización o por estándares de la

industria. Puede además incluir una revisión de las prácticas de seguridad de la organización. Existen diversos tipos de auditorías o revisiones que pueden proveerse, tales como:

Revisión de la infraestructura: Revisión manual de configuraciones de hardware o software, routers, firewalls, servidores y dispositivos de escritorio para asegurar que estén alineados con las mejores prácticas de seguridad de la organización o la industria y sus configuraciones estándares
Revisión de mejores prácticas: Entrevistas con empleados y administradores de redes y sistemas para determinar si sus prácticas de seguridad están acordes con la política de seguridad de la organización o estándares de la industria
Escaneos: Usando buscadores de vulnerabilidades o escáneres de virus, determinar qué sistemas o redes son vulnerables.
Pruebas de penetración: Probar la seguridad de un sitio atacando a propósito sus sistemas y redes.

Antes de realizar estas pruebas es importante obtener aprobación de las partes interesadas. Algunas de estas prácticas pueden estar prohibidas por políticas organizacionales.
Al proveer este servicio se puede incluir el desarrollo de un conjunto de prácticas contra las cuales las pruebas o evaluaciones se realizan, así como el desarrollar un conjunto de habilidades o requerimientos de certificación para el staff que realice estas pruebas, evaluaciones, auditorías o revisiones. Este servicio puede ser tercerizado con la expertise apropiada en realizar estas actividades.

Configuración y mantenimiento de herramientas de seguridad, aplicaciones, infraestructuras y servicios

Este servicio identifica o provee guías sobre cómo configurar y mantener de forma segura herramientas y aplicaciones y la infraestructura informática usada por la membresía del CSIRT o el CSIRT en sí mismo. Además de proveer guías, el CSIRT puede realizar actualizaciones de configuración y mantenimiento de herramientas de seguridad y servicios como IDS, sistemas de monitoreo y escaneo de redes, filtros, wrappers, firewall, VPN, o mecanismos de autenticación. El CSIRT puede incluso proveer estos servicios como parte de su función principal. El CSIRT puede además configurar y mantener servidores, equipos de escritorio, laptops, tabletas, teléfonos inteligentes y otros servicios inalámbricos de acuerdo con sus guías de seguridad. Este servicio incluye el escalar a gerencia cualquier problema con las configuraciones o el uso de herramientas y aplicaciones que el CSIRT crea que puedan dejar a la organización en un estado vulnerable a un ataque.

Desarrollo de herramientas de seguridad

Este servicio incluye el desarrollo de cualquier herramienta nueva, específica para los miembros que sea requerida o de interés para estos o el CSIRT. Esto puede incluir, por ejemplo, el desarrollo de parches de seguridad para software a la medida usado por los miembros, o distribuciones de seguridad aseguradas que puedan ser utilizadas para reconstruir equipos comprometidos. Además puede incluir el desarrollo de herramientas o scripts que extiendan la funcionalidad de herramientas de seguridad existentes tales como nuevos plugins para un escáner de vulnerabilidades, scripts que faciliten el uso de tecnologías de cifrado, sistema de distribución automatizados de parches, etc.

Servicios de detección de intrusiones

CSIRTs que realizan este servicio, revisan los logs de IDS, analizan e inicial el proceso de respuesta ante cualquier evento que se enmarque dentro de límites pre-establecidos, o reenvían esta alerta, de

acuerdo a estrategias de escalamiento o acuerdos de nivel de servicios pre-establecidos. La detección y análisis de intrusiones de logs de seguridad puede ser una tarea extenuante-no solamente el determinar dónde ubicar los sensores, sino en recolectar y analizar inmensas cantidades de datos capturados. En muchos casos se requiere el uso de herramientas especializadas o una alta expertise para sintetizar e interpretar la información identificando falsas alarmas, ataques, o eventos de red y para implementar estrategias para eliminar o minimizar estos eventos. Algunas organizaciones escogen tercerizar esta actividad a terceros que tienen mayor experiencia en manejar este tipo de servicios tales como proveedores de servicios de seguridad manejados.

Diseminación de información relacionada con seguridad

Este servicio provee a los miembros de una colección de información comprensiva y fácil de buscar que apoya en el mejoramiento de la seguridad. Esta información puede incluir:

información de contacto y formas de reportes al CSIRT
archivos de alertas, advertencias y otros anuncios
documentación sobre mejores prácticas
orientación general sobre seguridad informática
políticas, procedimientos y checklists
desarrollo de parches y distribución de información
enlaces a fabricantes y proveedores
estadísticas actuales y tendencias en el reporte de incidentes
otra información que pueda mejorar las prácticas de seguridad en general

Esta información puede estar publicada por el CSIRT o por cualquier otra dependencia de la organización (TI, Talento humano, Relaciones con medios), y puede incluir información de fuentes externas tales como otros CSIRTs, fabricantes y expertos de seguridad.

6.1.3 Servicios de gestión de la calidad de la seguridad

Los servicios que caen en esta categoría no son únicos al manejo de incidentes o a CSIRTs en particular. Existen servicios ya establecidos y bien conocidos diseñados en aras de mejorar la seguridad en general de la organización. Al aprovechar la experiencia ganada en la provisión de servicios reactivos y proactivos descritos anteriormente, un CSIRT puede ofrecer perspectivas muy interesantes y propias a estos servicios de gestión de la calidad de la seguridad que, de otra forma, podrían no estar disponibles. Estos servicios están diseñados para incorporar retroalimentación y lecciones aprendidas basadas en el conocimiento obtenido durante la respuesta a incidentes, vulnerabilidades y ataques. Alimentar estas experiencias en los servicios tradicionales ya establecidos (ver abajo) como parte del proceso de gestión de la calidad puede mejorar a largo plazo los esfuerzos de seguridad de una organización. En dependencia de la estructura organizacional y responsabilidades, un CSIRT puede proveer estos servicios o participar como parte de un equipo de seguridad más grande dentro de la organización
Las siguientes descripciones explican cómo la experiencia de un CSIRT puede beneficiar a cada uno de estos servicios de gestión de la calidad de la seguridad:

Análisis de riesgos

Los CSIRTs pueden agregar valor a las evaluaciones y análisis de riesgos. Esto puede mejorar la capacidad de la organización para evaluar amenazas reales, proveer evaluaciones cualitativas y cuantitativas de los riesgos de los activos de información, y evaluar estrategias de protección y respuesta. Los CSIRTs que proveen estos servicios conducirán o apoyarán con actividades de análisis de riesgos de seguridad para nuevos sistemas y procesos de negocios o evaluar amenazas y ataques contra activos y sistemas de los miembros del CSIRT.

Continuidad del negocio y plan de recuperación ante desastres

Basados en ocurrencias pasadas y en predicciones futuras de tendencias de seguridad, muchos más incidentes tendrán potencial para degradar seriamente las operaciones de los negocios. Por tanto, los esfuerzos de planificación deben considerar la experiencia del CSIRT y recomendaciones para determinar cómo se debe responder de una mejorar manera a estos incidentes para asegurar la continuidad de las operaciones del negocio. Los CSIRT que realizan estos servicios están involucrados en la planificación de la continuidad del negocio y plan de recuperación ante eventos relacionados con seguridad informática, amenazas y ataques.

Consultoría en seguridad

Los CSIRTs pueden proveer avisos y guías sobre mejores prácticas de seguridad para implementar en los negocios de los miembros. Un CSIRT que provea este servicio apoya en la preparación de recomendaciones o identificación de requerimientos para la compra, instalación o aseguramiento de nuevos sistemas, dispositivos de red, aplicaciones de software, o procesos de negocios empresariales. Este servicio incluye la provisión de guías y apoyo en el desarrollo de políticas de seguridad organizacionales o de los miembros. Puede además brindar testimonios o apoyo al legislativo y otros cuerpos gubernamentales en caso de ser requerido.

Concienciación

CSIRTs pueden identificar dónde es que los miembros requieren de mayor información y apoyo en la aplicación o cumplimiento de mejores prácticas o políticas organizacionales. Incrementar los niveles de concienciación de la membresía no solamente mejora su comprensión de los problemas de seguridad sino que además les ayuda a desarrollar sus actividades diarias de una mejora manera. Esto puede reducir la ocurrencia de ataques e incrementar la probabilidad de que los miembros puedan detectar y reportar ataques, ayudando por tanto a disminuir los tiempos de recuperación y eliminando o minimizando pérdidas.

Los CSIRTs que realizan este tipo de servicio buscan oportunidades para incrementar la concienciación en seguridad mediante la creación de artículos, pósters, noticias, sitios web y otros recursos informativos que expliquen las mejores prácticas de seguridad y provean apoyo sobre precauciones a tomar.

Las actividades pueden incluir además reuniones programadas y seminarios para mantener a los miembros al día con los procedimientos de seguridad que se desarrollan y potenciales amenazas a los sistemas de las organizaciones.

Entrenamiento/Capacitación

Este servicio consiste en proveer información a los miembros sobre problemas de seguridad a través de seminarios, talleres, cursos y tutoriales. Los tópicos pueden incluir lineamientos para reportar incidentes, métodos de respuesta adecuados, herramientas de respuesta a incidentes, métodos de prevención de incidentes, y cualquier otra información necesaria para proteger, reportar y responder a incidentes de seguridad informáticos.

Evaluación o certificación de productos

En este servicio un CSIRT conduce evaluaciones de producto para herramientas, aplicaciones u otros servicios con la finalidad de garantizar la seguridad de los productos y su alineación con prácticas de seguridad de la organización o del CSIRT. Las herramientas y aplicaciones revisadas pueden ser en software libre o productos comerciales. Este servicio se puede proveer como una evaluación o a través de un programa de certificación, en dependencia de los estándares que se apliquen por la organización o el CSIRT.

Apéndice A: Template del marco de trabajo del CSIRT

FRAMEWORK de un CSIRT
Nombre del equipo: Misión: Membresía: Autoridad: Responsabilidad: Estructura organizacional: Disponibilidad: Servicios: Staff: Infraestructura y herramientas: Relaciones internas y con terceros: Modelo de financiamiento:

Apéndice B: Formulario de reporte de incidentes (ejemplo)

FORMULARIO DE REPORTE DE INCIDENTE

Por favor rellene este formulario y envíelo a: …….
Lines marked with * are required.

Nombre y Organización

1. Nombre*:
2. Organización*:
3. Tipo de sector:
4. País*:
5. Ciudad:
6. E-Mail*:
7. Teléfono*:
8. Otra información:

Equipo(s) afectado(s)

9. Número de equipos:
10. Hostname e IP*:
11. Funciones de este(os) equipo(s)*:
12. Zona horaria:
13. Hardware:
14. Sistema Operativo:
15. Software afectado:
16. Archivos afectados:
17. Protocolo/Puerto:

Incidente

18. Número de referencia del incidente #:
19. Tipo de incidente:
20. Inicio del incidente:
21. ¿Incidente en curso?: SÍ NO
22. Hora y forma en que se descubrió:
23. Vulnerabilidades conocidas:
24. Archivos sospechosos:
25. Contramedidas:
26. Descripción detallada*:

Apéndice C: Herramientas de seguridad

Existen muchas herramientas disponibles para apoyar a los equipos de CSIRT en su trabajo, muchas de ellas son de uso abierto.

Tenga en cuenta que la mayoría de los archivos de logs se almacenan en texto claro y pueden ser leídos fácilmente mediante el uso de herramientas en línea de comando de Unix/Linux tales como *sed, awk y grep*. Estas mismas herramientas pueden ser utilizadas para normalizar archivos de logs provenientes de diversas fuentes o convertirlos en diferentes formatos para permitir el uso de herramientas más avanzadas.

A continuación una selección de herramientas normalmente utilizadas en este trabajo:

Herramientas de consulta de dominios e IP	
DomainTools	<https://www.domaintools.com/>
Domain Dossier	<http://centralops.net/co/DomainDossier.aspx>
IP to ASN Mapping	<http://www.team-cymru.org/IP-ASN-mapping.html>
GeoLite2	<http://dev.maxmind.com/geoip/geoip2/geolite2/>
RIPEstat	<https://stat.ripe.net/>
Herramientas de análisis de E-mail	
Google Apps Messageheader	<https://toolbox.googleapps.com/apps/messageheader/>
MXToolbox	<http://mxtoolbox.com/EmailHeaders.aspx>
Herramientas de monitoreo de red	
nfdump	<http://nfdump.sourceforge.net/>
nfsen	<http://nfsen.sourceforge.net/>
Herramientas de auditoría	
nmap	<https://nmap.org/>
AutoScan-Network	<http://autoscan-network.com/>
Wireshark	<https://www.wireshark.org/>
AbuseHelper	<https://github.com/abusesa/abusehelper>
Herramientas de evaluación de vulnerabilidades	
Nessus	<http://www.tenable.com/products/nessus-vulnerability-scanner>
Metasploit	<https://www.metasploit.com/>
Vega	<https://subgraph.com/vega/index.en.html>
OWASP ZAP	<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>
SQLcheck	<http://www.softpedia.com/get/Internet/Servers/Database-Utils/SQL-Check.shtml>
Burp Suite	<https://portswigger.net/burp/>

Kali	<https://www.kali.org/>
Herramientas de detección de intrusiones	
Snort	<https://www.snort.org/>
Tripwire	<https://sourceforge.net/projects/tripwire/>
Herramientas de forensia	
Sleuth Kit	<http://www.sleuthkit.org/>
Autopsy	<http://www.sleuthkit.org/autopsy/>
Tcpxtract	<http://tcpxtract.sourceforge.net/>
EnCase	<https://www.guidancesoftware.com/encase-forensic>
FTK, Forensic Toolkit	<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
Herramientas de análisis de malware	
VirusTotal	<https://www.virustotal.com/>
Malware Domain List	<http://www.malwaredomainlist.com/>
Malware Hash Registry	<http://www.team-cymru.org/MHR.html>
MISP, Malware Information Sharing Platform	<https://mispriv.circl.lu/>
AlienVault Open Threat Exchange	<https://otx.alienvault.com/>
Malwr	<https://malwr.com/>
Hybrid Analysis	<https://www.hybrid-analysis.com/>
Honeypots	
honeyd	<http://www.honeyd.org/index.php>
Herramientas WiFi	
inSSIDer	<http://www.metageek.com/products/inssider/>
Acrylic WiFi Scanner	<https://www.acrylicwifi.com/en/wlan-software/wlan-scanner-acrylic-wifi-free/>
SIEM	
Splunk	<http://www.splunk.com/>
Herramientas de cifrado	
GnuPG	<https://www.gnupg.org/>
VeraCrypt	<https://veracrypt.codeplex.com/>
Herramientas para rastreo de incidentes	
RTIR	<https://bestpractical.com/>
OTRS	<https://www.otrs.com/>
Bases de datos	

SQLite	<https://www.sqlite.org/>
MySQL	<https://www.mysql.com/>
PostgreSQL	<https://www.postgresql.org/>

Apéndice D: Fuentes de información

Para notificar incidentes, existen varias fuentes automatizadas provistas por la comunidad de seguridad a las que nos podemos suscribir, muchas de ellas sin costo. Las aquí listadas son usualmente utilizadas por muchos equipos:

Notificaciones de Incidentes		
APWG, Anti-Phishing Working Group	<http://apwg.org/>	Phishing
PhishTank	<http://www.phishtank.com>	Phishing
Dark-H	<http://dark-h.org>	Desfiguraciones de sitios web
Mirror-Zone	<http://mirror-zone.org>	Desfiguraciones de sitios web
Zone-H	<http://zone-h.org>	Desfiguraciones de sitios web
Zone-HC	<http://zone-hc.com>	Desfiguraciones de sitios web
Shadowserver	<https://www.shadowserver.org>	Botnet Open DNS resolver Open proxy server etc.
Team Cymru	<http://www.team-cymru.org/services.html>	Botnet Fuerza bruta DDoS Malware URL Open DNS resolver Open proxy server Phishing Escaneos

Para encontrar información sobre un equipo CSIRT cuya membresía esté involucrada en un incidente, los siguientes sitios pueden ser consultados:

Información de contacto (equipos CSIRT))	
FIRST, Forum of Incident Response and Security Teams	<https://www.first.org/>
APCERT, Asia Pacific CERT	<http://www.apcert.org/>
Trusted Introducer	<https://www.trusted-introducer.org/>
AfricaCERT	<http://www.africacert.org>
Latin American CSIRTs	<http://www.lacnic.net/en/web/lacnic/csirts>
OIC-CERT, Organisation of the Islamic Cooperation CERT	<http://www.oic-cert.org/>
NatCSIRT, National CSIRTs	<http://www.cert.org/incident-management/national-csirts/national-csirts.cfm>