



Creación de Equipos de Respuesta a Incidentes de Seguridad en Cómputo

Juan Carlos Guel López
Departamento de Seguridad en Cómputo
UNAM-CERT

Un poco del Instructor

- Ligado al campo de la Seguridad en Cómputo desde 1997
- En 1999 dirige el Área de Seguridad de la UNAM
- En 2000 funda el Departamento de Seguridad de la UNAM
- En 2000-2001 funda el UNAM-CERT avalado por FIRST
- Fundador de la iniciativa de la Red Nacional de Seguridad en Computo desde 2002. (agrupa 144 Universidades de México)
- Desde 1999 coordina el evento “Seguridad en Computo México” y DISC “Día Internacional de la Seguridad en Computo”
- Actualmente Chair del grupo de Seguridad de RedCLARA (Mas de 800 Universidades de AL)
- Miembro del Antiphishing Working Group.
- Ha impartido diversos cursos, talleres y tutoriales en diversos eventos.
- Ha colaborado en diversos proyectos en diversos sectores Publico, privado y participado en diversos procesos electorales.



Índice

1. Introducción
2. Estableciendo el CSIRT
3. Involucrando a la Organización
4. Financiamiento del CSIRT
5. Servicios del CSIRT
6. Flujo de Información en el CSIRT
7. Modelos de CSIRT
8. Recursos Humanos e Infraestructura
9. Implementación y Operación del CSIRT
10. Conclusiones



Introducción

- Crear un CSIRT dentro de una organización es un proceso que involucra un cambio estructural, organizacional y desde luego requiere de mucho esfuerzo y compromiso a todos los niveles.
- Sin duda un CSIRT viene a darle un gran valor a la organización ya que provee un punto de contacto único para afrontar, resolver y proponer en el campo de las nuevas tecnologías



Objetivos iniciales

- Entender los métodos para:
 - Establecer una visión de la forma en la que su CSIRT operará.
 - Delinear el marco de operación de su CSIRT; misión, autoridad, alcance y tipo de constitución dentro de su organización.
 - Determinar el modelo organizacional adecuado para el nuevo CSIRT.
 - Definir diferentes niveles de servicios proporcionados por su CSIRT.



Perfil de los ajustes

- Individuos encargados de la creación de un CSIRT:
 - Directores Generales.
 - Jefes de Seguridad.
 - Administradores.
 - Líderes de proyecto.
 - Miembros de equipos de proyecto.



Etapas en el desarrollo de un CSIRT

- Etapa 1. Educando a la organización.
- Etapa 2. Planificando el esfuerzo.
- Etapa 3. Implementación inicial.
- Etapa 4. Fase operacional.
- Etapa 5. Estrecha colaboración.



No existe una receta única

- No existe una única receta para la creación de un CSIRT, está depende de tus:
 - Necesidades y requerimientos.
 - Misión y objetivos.
 - Disponibilidad de recursos y soporte.



Presentaciones

- Preséntación de Cada Uno:
 - Nombre y puesto.
 - Organización.
 - Experiencia.
 - Progreso en la implementación y creación de un CSIRT.
 - Manejo de incidentes previos.
 - Preguntas.



Propósitos

- Definir la naturaleza y propósito del CSIRT.
- Discutir el porqué las organizaciones necesitan de los CSIRT.



¿Por qué estamos aquí?

- Las redes de computadoras han revolucionado la forma en que se llevan a cabo los negocios, a la vez que han introducido riesgos potenciales.
- Los cambios en la manera en cómo la sociedad hace uso de la tecnología trae consigo nuevas posibilidades de intrusión.
- En la mayoría de los casos los administradores de las redes o sistemas no cuenta con la gente ni la experiencia para defenderse en contra de los ataques y reducir los daños.



¿Qué es lo que se puede hacer?

- Como defensa en contra de las amenazas de seguridad en Internet, las organizaciones pueden:
 - Mantenerse al día con los últimos parches de los sistemas operativos y las actualizaciones los productos.
 - Instalar defensas perimetrales e internas como ruteadores, firewalls, scanners, y sistemas detectores de intrusos.
 - Actualizar y extender políticas y procedimientos de seguridad.
 - Lanzar alertas de seguridad, capacitar a los empleados, clientes y miembros de la organización y de la constitución en cuestiones básicas de seguridad.

¿Qué es un CSIRT?

- Son las siglas de Computer Security Incident Response Team, es una Organización o Equipo que provee servicios y soporte, en un entorno definido (constitución), para prevenir, manejar y responder a los incidentes de seguridad computacional.



¿Por qué un CSIRT?

•Reactivo

- Un esfuerzo de respuesta concentrado.
- Respuesta mas rápida y estandarizada.
- Coordinación con otras comunidades de seguridad.

•Proactivo

- Permite que los objetivos de las organizaciones se lleven a cabo.
- Servicios de valor agregado a procesos de negocio.
- Asistencia en el desarrollo de evaluaciones de vulnerabilidades y establecimiento de políticas de seguridad.



¿Qué es lo que hace un CSIRT?

- En general un CSIRT:

- Proporciona un punto único de contacto para el reporte de los problemas locales y de su rango de acción.
- Asiste a la organización y en general a la comunidad de cómputo en la prevención y manejo de incidentes de seguridad en cómputo.
- Comparte información y experiencias con el CSIRT/CC, otros equipos de respuesta y otros sitios y organizaciones adecuados.



¿Qué es un Incidente de Seguridad ?

- Un CSIRT requiere establecer criterios que definan, no sólo cómo está constituido un incidente de seguridad, sino también el cómo manejarlo.
 - ¿Cuál es la definición de un incidente de seguridad en tu organización?
 - ¿Cuáles los elementos críticos que deben ser protegidos en tu organización?



Ejemplos de CSIRT's

CERT Coordination Center (CERT/CC)

<http://www.cert.org/>

Forum of Incident Response and Security Teams (FIRST)

<http://www.first.org/>

Australian Computer Emergency Response Team (AusCERT)

<http://www.auscert.org.au/>

German Research Network (DFN-RT)

<http://www.cert.dfn.de/>

Japan Computer Emergency Response Team Coordination Center (JPCERT)

<http://www.jpCERT.or.jp/>

Department of Defense CERT(DOD-CERT)

<http://www.cert.mil/>





Estableciendo el CSIRT

Puntos clave

- Los cambios en la forma de uso de la tecnología en la sociedad, han abierto la puerta para nuevas oportunidades de intrusión.
- La creación de un CSIRT es uno de los pasos que las organizaciones pueden tomar para proveer una estrategia más rápida de respuesta.
- Los CSIRT vienen en todas las variedades, pero la misión y los objetivos de un CSIRT siempre deben de concordar con los objetivos de la organización o de su rango de acción.



Propósito

Estableciendo el Contexto

- Identificar las acciones y decisiones claves que deben de considerarse en la planeación e implementación de un CSIRT.
- Encontrar los elementos, decisiones y acciones críticas de su organización.



Imagina...

- ... que el sistema más crítico para tu organización ha sido comprometido, modificado o se ha accedido a información clasificada.



Pregúntate

- ¿Cómo respondería tu organización a este tipo de incidente si se presentara en este momento?
 - ¿Quién respondería?
 - ¿Quién debería responder?
 - ¿Quién más necesitaría verse involucrado?
 - ¿Cuál debería ser la respuesta?
 - ¿Quién toma estas decisiones?
 - ¿Cómo desearías que tu organización respondiera?



¿Qué hemos aprendido?

- ¿Qué es lo que se sabe de manejo de incidentes en tu organización?
- ¿Qué es lo que no se sabe del manejo de incidentes en tu organización ?
- ¿Qué es lo que necesitas saber?
- ¿Quién más necesita involucrarse para obtener las respuestas?
- ¿Qué necesita cambiarse en el modo actual en que tu organización provee o no una respuesta?
- ¿Cómo cambiaría un CSIRT la forma de responder?
- ¿Qué es lo que quieres que tu CSIRT haga?



Identificación de decisiones y elementos clave

- Haz una lista de elementos clave y decisiones que pienses deberían ser tomadas en cuenta para diseñar y crear de manera exitosa un CSIRT.
 - En general.
 - Para tu organización.



Decisiones y elementos clave

- ¿Cuál es tu rango de acción?
- ¿Cuál es su misión?
- ¿Cómo operará el CSIRT?
- ¿Qué autoridad tiene el CSIRT?
- ¿Cómo será fundado el CSIRT?
- ¿Qué servicios proveerá?
- ¿Ante quién responderá o se reportará el CSIRT ?
- ¿Qué tipo de actividad debe de ser reportada al CSIRT?
- ¿Dónde estará físicamente el CSIRT?
- ¿El equipo estará centralizado o distribuido?



Más decisiones y elementos clave

- ¿Qué tipo de personal se requiere?
- ¿Cuánto personal debe tener?
- ¿El personal realizará alguna otra labor o sólo trabajo relacionado al CSIRT?
- ¿Qué tipo de equipo debe ser adquirido?
- ¿Cómo debe ser configurada la infraestructura del CSIRT?
- ¿Qué políticas y procedimientos de operación estándar serán necesarios?
- ¿Quién ayudará a diseñar e implementar el CSIRT?
- ¿Cómo deben de ser comunicados la misión y los servicios que se proporcionarán?



El beneficio de los escenarios

- Crear posibles escenarios pueden ayudar a tu equipo de desarrollo de proyecto CSIRT en:
 - Ayudar a estimular sus pensamientos acerca de los procesos específicos de tu organización.
 - Ayudar a ordenar los objetivos organizacionales del CSIRT.
 - Identificar los procesos de negocios que deberían de ser modificados para implementar de manera exitosa el CSIRT.



Puntos clave

- Los escenarios de la vida real pueden ser de utilidad para detectar nuevos elementos que deberían tomarse en cuenta.
- Se requiere identificar qué es lo que se sabe y qué no.
- La creación del CSIRT tal vez traiga consigo la re-evaluación de los procesos de negocios.



Involucrando a la Organización en la creación del CSIRT



Propósito

- Ayudarte a definir el marco de trabajo para tu CSIRT.
- Establecer la importancia de una visión global de tu CSIRT.
- Revisar declaraciones de las misiones de los existentes CSIRT's y fundar estrategias.
- Discutir ideas para planear y diseñar la estrategia del CSIRT.



Creando un CSIRT ejecutivo

- Para ser efectivo, un CSIRT requiere de cuatro elementos:
 - Un marco de trabajo operacional.
 - Un servicio y políticas de marco de trabajo.
 - Asegurar la calidad del marco de trabajo.
 - La capacidad de adaptarse a un ambiente cambiante a perfiles de amenazas cambiantes.



Pasos básicos de la implementación

- Reunir información.
- Identificar la constitución del CSIRT.
- Determinar la misión del CSIRT.
- Determinar el rango y los niveles de servicios del CSIRT.
- Determinar la estructura de reporte, autoridad y modelo organizacional del CSIRT.
- Financiamiento seguro para las operaciones del CSIRT.
- Identificar y adquirir equipos, personal y recursos de infraestructura.
- Crear un plan, obtener realimentación sobre el plan.



Establecer un proyecto de equipo

La información clave reunida incluye:

- ¿Cuáles son los puntos críticos que deben de ser protegidos?
- ¿Qué tipo de incidentes reportados con mayor frecuencia?
- ¿Qué problemas de seguridad existen?
- ¿Qué tipo de respuesta se requiere?
- ¿Qué procesos se requieren?
- ¿Quién desempeñará cada tarea?



Todo depende de:

- Una implementación exitosa dependerá de:
 - Desarrollar una visión global de los requerimientos de la organización.
 - La claridad de esa visión.
 - Obtener recursos disponibles incluyendo personal, experiencia y financiamiento.
 - Comunicar su visión y estrategia.
 - Construir una reputación de confiabilidad de tu equipo.



Tratando con restricciones

- Las restricciones pueden incluir:
 - Presupuesto.
 - Falta de financiamiento.
 - Dispersión geográfica de la organización.
 - Desacuerdos organizacionales o facciones.
 - Falta de entendimiento en la administración.
 - Falta de experiencia del personal.
 - Carencia de una visión clara o falta de consenso en la organización.
 - Falta de comunicación.
 - Marco de tiempo establecido.



Aprendiendo de otros

- Revisando los CSIRT existentes

- Constitución.
- Misión.
- Financiamiento.



Misión de CERT/CC

- El CERT/CC se caracteriza por trabajar con la comunidad de Internet en la detección y resolución de los incidentes de seguridad computacional así como dar los pasos para prevenir futuros incidentes.



Misión del AusCERT

- La misión del AusCERT es proporcionar soporte y mejorar el conocimiento de la comunidad. La representación y comunicación considerando la seguridad computacional, tanto lógica como internacional, siendo la fuente principal más confiable e imparcial sobre asuntos de seguridad.



Misión del JPCERT

- JPCERT es un punto central para la coordinación, de forma independiente de actividades de expertos en los sitios donde se ensanchan las brechas de con esos expertos capaces de dar soporte tecnológico a los sitios afectados, con lo cual se facilita la cooperación de necesaria para resolver los problemas de seguridad.
- JPCERT/CC no es, sin embargo, un servicio de mantenimiento o consulta. La responsabilidad de solucionar los problemas de seguridad descansa directamente el los usuarios; JPCERT/CC juega un rol de soporte, ofreciendo asistencia en el aspecto técnico.



Misión de Mi CSIRT

- Direccionar la seguridad en cómputo en mi corporación a los usuarios locales de Internet, asesoría y repuesta a posibles ataques de internet.
- <http://www.mycert.my/what.html>



Misión de SingCERT

- “SingCERT” es un centro para la respuesta a incidentes de seguridad en Singapur.

- Misión:

- Un punto de contacto.
- Facilita la resolución de amenazas de seguridad.
- Provee servicios de valor agregado.
- Incrementa la competitividad nacional en seguridad en IT.



Misión de CanCERT

- La misión del CanCERT es convertirse en el centro más confiable para la recolección y diseminación de información relacionada a las amenazas sobre las redes de computadoras, vulnerabilidades, incidentes y respuestas para incidentes del gobierno canadiense, negocios y organizaciones académicas.
- CanCERT provee un soporte confiable de seguridad para la administración de redes de computadoras del gobierno canadiense, negocios y organizaciones académicas.
- <http://www.cancert.ca/>



Misión del CERT NASK

- Proveer un único y confiable punto de contacto en Polonia para los clientes de la comunidad de NASK y otras redes en dicho país para tratar con problemas e incidentes de seguridad en sus redes, así como buscar la forma de prevenirlos.
 - Responder a los incidentes de seguridad en las redes conectadas a NASK y redes conectadas a otros proveedores polacos.
 - Reportar incidentes de seguridad.
 - Proveer información de seguridad y alertas de posibles ataques.
 - Cooperación con otros equipos de respuesta a incidentes a través de todo el mundo.



IBM - ERS

- IBM-ERS es un contratista comercial de servicios, que provee servicios de manejo y respuesta de incidentes, probando mensual y semanalmente vulnerabilidades, detección de intrusos en tiempo real.



Listas de los CSIRT's

- Se pueden encontrar ligas a diferentes equipos de CSIRT en las siguientes páginas:
- **FIRST:**
 - <http://www.first.org/about/organization/teams/index.html>
 - <http://www.first.org/members/map/>
- **TERENA:**
 - <http://www.ti.terena.nl/teams/index.html>



Identifica tu constitución

- Tu constitución quizás sea definida por ti, dependiendo de tu proyecto.
- Si tu constitución no está aún definida, necesitarás determinar la forma que ésta tomará.
- ¿Qué elementos deberían ser tomados en cuenta antes y después de identificar tu constitución?



Determinar tu Misión

- Tu misión debe ser definida en los estatutos de la misión de tu CSIRT.
- El RFC 2350 establece que su misión debe ser:
 - Explicar el propósito de tu equipo.
 - Resaltar los objetivos y metas centrales del equipo.



RFC 2350 Expectations for Computer Security Incident Response

- This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.
- The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs).
- <http://www.faqs.org/rfcs/rfc2350.html>



Puntos clave

- Debes tener una visión clara de como estará estructurado tu CSIRT antes de que puedas planear los detalles de la operación.
- La misión de tu CSIRT debe soportar las metas y objetivos de la constitución.



Financiamiento del CSIRT



Obtener financiamiento para tu CSIRT

- Existen varias estrategias para financiar tu CSIRT:
 - Suscripción de membresía.
 - Servicios con honorarios base.
 - Contratación de servicios.
 - Patrocinio gubernamental.
 - Patrocinio académico o de investigación.
 - Patrocinio por parte de un consorcio.
 - Una combinación de cualquiera de los de arriba.



Prepárate

- Tu fuente de financiamiento puede cambiar
 - Las fuentes iniciales de financiamiento pueden ser limitadas.
 - Prepárate para buscar nuevas fuentes de financiamiento.
 - Muchos de los CSIRT tienen que enfrentar este mismo tipo de retos.



Definición de Servicios del CSIRT



Propósito

- Rangos y niveles de servicios.
- Describir el tipo de servicios que un CSIRT debe ofrecer.
- Proporcionar información y ayuda para decidir qué servicios serían los adecuados para tu CSIRT.
- Ayudar a entender los elementos que necesitas tomar en cuenta, cuando selecciones los niveles de servicios de tu CSIRT.



¿Qué rango de servicios?

- ¿Qué rango de servicios debe ofrecer el CSIRT?
 - Reactivos.
 - Proactivos.
- ¿Qué tópicos asocian a proporcionar y elegir los servicios de un CSIRT?



Rango de servicios

- **Servicios Obligatorios:**
 - Manejo de incidentes.
- **Servicios comunes del CSIRT:**
 - Alertas y anuncios.
 - Respuesta y análisis de vulnerabilidades.
 - Análisis de artefactos.
 - Educación y capacitación.
 - Auditoria y pruebas de penetración.
 - Análisis de riesgo.
 - Desarrollo de productos de seguridad.
 - Colaboración.
 - Coordinación.



Manejo de incidentes

- Proporciona mecanismos de reporte de incidentes.
- Mantiene los datos de los incidentes en lugar seguro.
- Entiende la amenaza, naturaleza y alcance de su actividad.
- Identifica nuevos tipos de métodos de ataque.
- Proporciona soporte técnico para respuesta de incidentes de seguridad.
- Facilita la comunicación entre los sitios y equipos de respuesta.



Avisos y anuncios

- Publicar y distribuir información al público en general o a una constitución definida.
 - Analizar y desarrollar avisos y anuncios.
 - Retransmitir avisos de otros equipos.



Manejo de vulnerabilidades

- Analizar y verificar el problema.
- Analizar y sugerir soluciones viables.
- Coordinarse con otros reporteros de vulnerabilidades y otros expertos de confianza.
- Mantener la información de las vulnerabilidades en un lugar seguro.



Detección de intrusos

- Revisar las alertas de los sistemas de detección de intrusiones (IDS).
- Analizar patrones a través de la organización.
- Sintetizar la información para obtener una visión general de la actividad del incidente.
- Actualizar y mantener las firmas de los IDS.
- Revisar y monitorear el ambiente de red existente para establecer una línea base de actividad de la red, para tener un punto de comparación en contra de potenciales anomalías.
- Mantener registros para usar durante la investigación y recuperación de actividades.



Otros

- Inculcar una cultura de la seguridad y capacitación.
- Visores de la tecnología.
- Desarrollo de productos de seguridad.



Selección de servicios

- Cada Equipo necesita determinar:
 - Qué rango de servicios proporcionará.
 - Qué nivel de soporte dará a cada uno de los servicios.



Definir tus servicios

- Por cada servicio que tu CSIRT proporciona, necesitas definir claramente:
 - Conjunto de expectativas acerca de cómo el servicio ha de operar.
 - Establecer un horario de disponibilidad para los servicios.
 - Definir las políticas y procedimientos relacionados con los servicios que se proporcionan.
 - Definir claramente los roles y responsabilidades.
 - Paso por paso las instrucciones para desarrollar el servicio.



Definiciones internas de los servicios

- Título del servicio.
- Qué es lo que el servicio hace.
- Quién proporciona el servicio.
- Quién es el respaldo para el servicio si el primario no está disponible.
- Horas en las que el servicio deberá ser ofrecido.
- El flujo de información de adentro y hacia afuera del servicio .
- Equipo, herramientas, políticas y procedimientos que se utilizarán para proveer el servicio.
- La prioridad del servicio el relación a otros servicios.
- Líneas claras de división de responsabilidades y escala de toma de decisiones.



Definiciones externas de los servicios

- Título.
- Qué es lo que cubre y no cubre el servicio.
- Quién debería o no usar el servicio.
- Horas de operación.
- Cualquier requerimiento especial para el acceso, como:
 - Cuotas
 - Subscripciones.
 - Filiaciones.



Nivel de servicios

- Para cada servicio que tu CSIRT ofrezca, necesitas definir claramente:
 - Cuantos recursos serán asignados para el servicio.
 - La extensión y profundidad con la que los servicios serán proporcionados.



Anunciar los niveles de servicios

- Siempre asegúrate de anunciar cada nuevo servicio que quieras que tu constitución utilice:
 - Métodos de difusión:
 - Poner la información en sitios de web.
 - Correo electrónico a los miembros de la constitución.
 - Crear volantes y material de difusión.
 - Pensar en como obtener retroalimentación sobre nuevos servicios y actividades.



Políticas y procedimientos

- Todos los proyectos y funciones del CSIRT deben soportados por políticas y procedimientos bien definidos.
- Estos ofrecen la guía para:
 - Responsabilidades y roles.
 - Prioridades.
 - Nivel de decisión.
 - La naturaleza de las respuestas dadas.
 - Nuevos miembros del personal de CSIRT.



Ejemplos de políticas

- Política de seguridad.
- Política de ambiente de reporte abierto.
- Política de reporte de incidentes.
- Política de manejo de incidentes.
- Política de comunicación externa.
- Política de relaciones públicas.
- Política de distribución de la información.
- Política de errores humanos.
- Política de educación y capacitación.



Ejemplos de procedimientos

- Procedimientos de operación estándar.
- Aceptación y seguimiento de reportes de incidentes.
- Manejo de incidentes y vulnerabilidades.
- Configuración de las redes y sistemas del CSIRT.
- Monitoreo de redes y sistemas y detección de intrusos.
- Respaldo y almacenamiento de los datos de los incidentes.
- Procesos de notificación (cómo es empaquetada, distribuida y archivada la información etc.).



Puntos clave

- Ser selectivos en relación a los servicios que proporcionarás a tu constitución.
- Difundir y anunciar los servicios que proporcionas y asegurarse de que el CSIRT sea capaz de darles soporte.
- Desarrollar políticas y procedimientos que permitan al personal del CSIRT proporcionar los servicios de manera efectiva y eficiente.



Reportes e Información de un CSIRT



Propósito

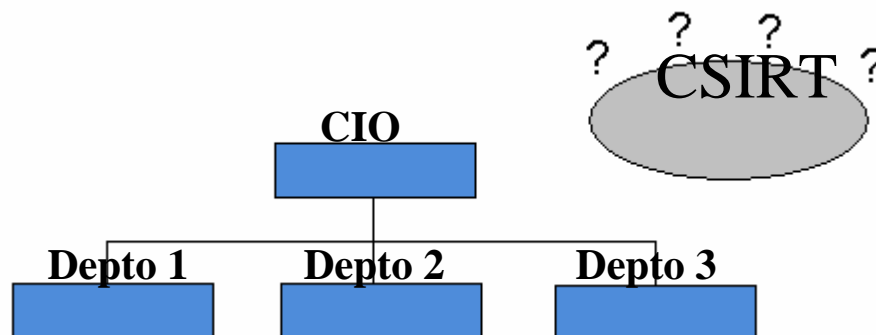
- Discutir la estructura de reporte del CSIRT.
- Resaltar la importancia del flujo de información a través de el CSIRT.
- Discutir varios tipos de autoridad que un CSIRT debe tener.
- Revisar modelos organizacionales alternativos de CSIRT y pruebas estructuras organizacionales.
- Discutir tópicos concernientes a el tamaño del CSIRT.



Estructura del reporte

Algunas preguntas...

- ¿Cuál es el lugar del CSIRT dentro de tu organización?
- ¿Ante quién reporta el CSIRT?
- ¿Qué autoridad tiene el CSIRT?



Flujo de información

- ¿Cuáles son los lineamientos de tus reportes?
- ¿Qué información es la que se reporta?
- ¿A dónde se reporta esta información?
- ¿Cómo se reporta la información?
- ¿Cómo se maneja la información?
- ¿Qué políticas y procedimientos de manejo de información son necesarios?



Autoridad CSIRT

• ¿Cuál será la autoridad del CSIRT?

• Completa.

• Compartida.

• Sin autoridad.

• Otra.



¿Qué es lo que se está reportando?

- Reportes de Vulnerabilidades.

- Alertas IDS.

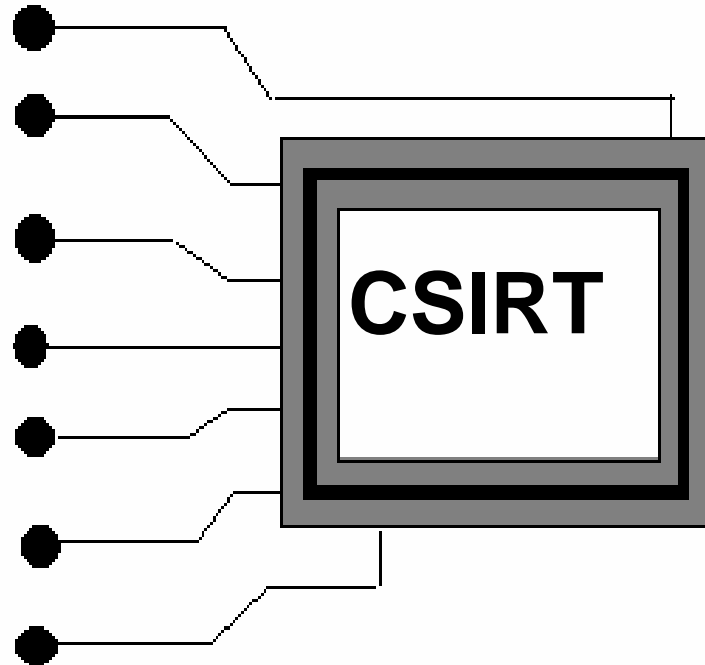
- Monitoreo de red.

- retroalimentación.

- Requerimiento de servicios.

- Reporte de incidentes.

- Preguntas generales.



¿Qué es lo que pasa con la información?

- ¿Qué análisis se hace o se debería hacer?
- ¿A dónde van los análisis de los resultados?
 - Informe de administración.
 - Reportar a la coordinación o centros de análisis.
 - Alertas y avisos.
 - Lecciones aprendidas y lo mejor de la práctica.
 - Documentos técnicos.
 - Informes de prensa.



Colaboración y coordinación

- ¿Quién más necesita verse involucrado?
- Otros expertos de seguridad.
- Otros CSIRT o centros de coordinación.
- Entorno de los Proveedores de Servicios de Internet.
- Otros grupos en tu organización:
 - Departamento IT.
 - Relaciones públicas.
 - Recursos humanos.
 - Departamento legal.



Modelos de CSIRT



Modelos organizacionales

- Cuando diseñas la visión de tu CSIRT, necesitas pensar acerca de cómo operará e interactuará el CSIRT con la organización y la constitución.
- Necesitas visualizar un modelo que pueda ser implementado.



Un dilema organizacional

- Érase una vez una gran compañía que estaba planeando crear un CSIRT...
- La compañía tenía diferentes localidades al alrededor del mundo. El equipo de planeación no podía determinar cómo tener un CSIRT trabajando a través de éstas diferentes áreas.....



Modelos alternativos de CISRT

- Equipos Locales.
- Equipos Virtuales.
- Equipos Centralizados.
- Equipos combinados (Virtuales y Centralizados).
- Centro de Coordinación.
- Centro de Análisis.
- Combinación de muchos Modelos.



Equipos locales

- Descripción:

- Existe un equipo de CSIRT identificado en cada sitio.

- Fortalezas:

- Grupos identificados para manejo de incidentes.
- El tiempo de respuesta puede ser mucho más rápido en el sitio.

- Debilidades

- Estrategias de respuesta inconsistente.
- No comparten información, por lo cual incidentes similares no pueden ser prevenidos en otros equipos.
- Análisis organizacional de bajo nivel.



Equipos Virtuales

- **Descripción:**

- Equipos locales con un equipo líder centralizado.

- **Fortalezas:**

- El compartir información genera la posibilidad de crear análisis completos a través de la organización.
- En los sitios de respuesta la reacción puede ser mucho rápida.

- **Debilidades**

- Los compromisos de tiempo pueden ser un problema.
- Es difícil crear sinergia de equipos.



CSIRT centralizado

- Fortalezas:

- Personal experto en el manejo de incidentes.
- Es un buen modelo para pequeñas organizaciones.

- Debilidades:

- Pueden existir retrasos en el desempeño de las repuestas (quizás ocasionados por tiempos de viaje).
- El CSIRT está centralizado, todos los miembros del equipo dedican 100% de su tiempo al manejo de incidentes.
- Reforzamiento y estandarización, difícil de llevar a cabo.



Equipo combinado

•Fortalezas:

- Lo mejor de modelos dedicados virtuales.
- Mecanismos para compartir la información, análisis y respuesta estandarizadas.

•Debilidades:

- Es necesario mantener dos estructuras.



Centro de coordinación

- Los Centros de Coordinación facilitan el análisis y el manejo de incidentes a través de los numerosos CSIRTs o unidades organizacionales.
- Facilitan la compartición de información y la diseminación de:
 - Tendencias de los incidentes, patrones y actividades.
 - Respuesta y migración de estrategias.
 - Análisis e investigación.
 - Nuevas herramientas y técnicas para el manejo de incidentes.



Centro de análisis

- Un centro de análisis se enfoca al análisis de las tendencias y los patrones para entender y prevenir futuros ataques.
- El centro de análisis no provee directamente un servicio de respuesta, sino ve la forma de responder con estrategias, cuyos efectos continúen por largo tiempo.



Quizá requieras de más de un modelo

- Algunas organizaciones quizás tengan diferentes necesidades que no puedan ser cubiertas por un solo modelo.
- Resulta necesario crear modelos multicapa.



Los modelos evolucionan

- Tus modelos quizás necesiten ser revisados a través del tiempo, basados en cambios en tu:
 - Misión.
 - Prioridades.
 - Servicios que se proporcionan.
 - Patrocinio.
- Se les exhorta a que periódicamente evalúen su modelo para determinar los cambios necesarios.



Puntos clave

- El modelo organizacional y la estructura de reporte deben de reconocer las necesidades de la organización y su entorno de trabajo.
- Tu modelo debe evolucionar a través del tiempo.
- El tamaño de tu CSIRT probablemente dependa de tu presupuesto disponible, recursos y número de servicios que se ofrecen.



Recursos Humanos e Infraestructura en la creación de un CSIRT



Recursos del CSIRT:

- Personal,
- Equipo e
- Infraestructura.



Propósito

- Identificar recursos iniciales requeridos en la creación de un CSIRT.
- Discutir elementos importantes en la consideración del personal inicial.
- Equipo e infraestructura necesaria para un nuevo CSIRT.



Las bases

- ¿Cuáles piensas que sean los recursos básicos necesarios para iniciar un CSIRT?
- Personal.
- Equipo.
- Infraestructura segura.



Selección de personal

- ¿Qué tipo de personal necesitarás?
- ¿Contratarás personal que se ajuste a los servicios?
- ¿Ofrecerás servicios que se ajusten al personal?



¿Dónde obtener personal para el CSIRT?

Las opciones incluyen:

- Contratar personal dedicado exclusivamente al CSIRT.
- Utilizar personal de sistemas y redes ya existente.
- Cubrir las necesidades de respuesta a los incidentes mediante Outsourcing.
- Por medio de contratistas.
- Alguna combinación de las de arriba.



Tipos de puestos en el CSIRT

- Jefe o líder de equipo.
- Asistente, supervisor o grupo de líderes.
- Oficinista, secretaria.
- Manejador de incidentes.
- Manejador de vulnerabilidades.
- Escritores técnicos.
- Administradores de redes o sistemas.
- Especialistas en diferentes plataformas.
- Personal de soporte.



Equipo para el CSIRT

- El personal del CSIRT necesitará tener acceso a equipo básico de cómputo y sistemas de comunicación para desarrollar sus funciones.
 - Piensa en equipo para la casa y la oficina.
 - El equipo en casa también debe de ser seguro.



La infraestructura del CSIRT

- La ubicación física del CSIRT también es importante.
 - No sólo para tener un espacio en donde trabajar sino para poder restringir el acceso al área del CSIRT.
- La ubicación o espacio de trabajo del CSIRT debería incluir:
 - Un área general de la oficina.
 - Un área segura (físicamente) para realizar reuniones o trabajo de incidentes.
 - Amueblado ergonómico.



Requerimientos de una infraestructura segura

- La infraestructura del CSIRT debe de incorporar todas las precauciones conocidas que sean física y financieramente posibles.
- Los CSIRT sirven como modelo a otras organizaciones.
- Por ello es importante asegurarse que sus operaciones son seguras y que todos los incidentes y datos sensibles están protegidos.



Protegiendo la información del CSIRT

- La información del CSIRT debería considerarse un elemento de la organización y debe ser protegida como tal.
- Considera todos los medios por los cuales esta información puede ser accesible.
- Asegúrate de que la información este protegida en cualquier caso:
 - Laptops.
 - Servidores.
 - Redes.
 - Cache, swap, áreas temporales.
 - Medios removibles.
 - Conocimiento humano.

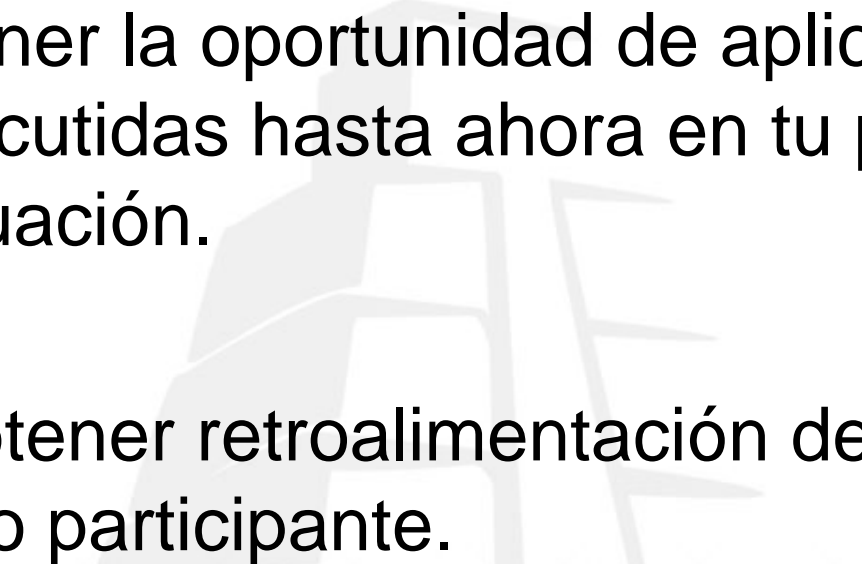


Implementación y Operación del CSIRT



Propósito



- Tener la oportunidad de aplicar las ideas discutidas hasta ahora en tu propia situación.
 - Obtener retroalimentación del instructor u otro participante.
- 



Tiempo para reflexionar

- ¿Cómo aplicar el material revisado hasta ahora?
- Acciones específicas que quisieras emprender, apenas regreses a tu organización.
- Información específica que deseas obtener.
- ¿A quién más necesitarías involucrar en el proceso de desarrollo del CSIRT?
- Ideas para tu diseño o plan de implementación.



Otros tópicos

- ¿Qué otros tópicos y tareas deben de ser tomadas en cuenta?



Puntos a corto plazo

- Desarrollar el plan de implementación del CSIRT.
- Anunciar el plan y obtener retroalimentación.
- Crear mecanismos de reclutamiento y contratación.
- Crear en plan de entrenamiento.
- Comprar equipo y sistemas.
- Construir la infraestructura del CSIRT.
- Obtener herramientas de manejo de incidentes para el personal.
- Comenzar a recibir y manejar de manera real incidentes.



Puntos a largo plazo

- Promocionar tu CSIRT.
- Establecer contactos y colaboración con otros equipos y otros grupos de seguridad.
- Construirle una buena reputación a tu CSIRT.
- Crear un mecanismo para el desarrollo del personal.
- Realzar y extender tus políticas y procedimientos de seguridad.
- Promover una cultura de la seguridad en tu organización y área de trabajo.
- Extender sus servicios.



Mejoras continuas

- Necesitarás evaluar tu progreso como nuevo CSIRT.
- Darte cuenta de qué funciona y qué no.
- Revisar tu diseño y planes de implementación en áreas y puntos que así lo requieran.
- Evaluar tus capacidades y servicios una vez que esté operado.
- Construir mecanismos de retroalimentación para revisar el desempeño de la constitución, tanto interna, como externamente.



Consejos de otros

- HACER HASTA LO IMPOSIBLE POR APRENDER EN CABEZA AJENA.
- Reutilizar (con los permisos pertinentes), es un buen hábito.



Información Adicional



Recursos que pueden ser de utilidad

- Organizational Models for Computer Security Incident Response Teams (CSIRTs)

- <http://www.cert.org/archive/pdf/03hb001.pdf>

- The CERT handbook

- <http://www.sei.cmu.edu/publications/documents/03.reports/03hb001.html>

- Expectations for Computers Security Incident Response

- <http://www.faqs.org/rfcs/rfc2350.html>

- Forming an Incident Response Team

- <http://www.uscert.org.au/render.html?it=2252&cid=1938>



Más fuentes

- Site Security Handbook
 - <http://www.faqs.org/rfcs/rfc2196.html>
- NSS Security Improvement Modules
 - <http://www.sei.cmu.edu/news-at-sei/features/2000/summer/feature-4-sum-00.pdf>
- Avoiding the Trial-by-fire Approach to Security Incidents
 - http://www.sei.cmu.edu/news-at-sei/columns/security_matters/1999/mar/security_matters.htm



Lecciones aprendidas

- La confiabilidad es primordial para alcanzar el éxito.
- Preparación y trabajo constante y no últimos sprints.
- Ten presente que todos los CSIRT son diferentes y respeta esas diferencias.



Gracias!!

Juan Carlos Guel López
cguel@seguridad.unam.mx

**Departamento de Seguridad en
Cómputo/UNAM-CERT**

<http://www.seguridad.unam.mx>

<http://www.cert.org.mx>

