Análisis del Desarrollo de un Centro de Respuesta Nacional para la República Oriental del Uruguay

Carozo, Eduardo; Martinez, Carlos; Vidal, Leonardo
Docentes.- Universidad de Montevideo

Betarte, Gustavo; Blanco, Alejandro; Rodríguez, Marcelo; Perez, Julion
Docentes.- Universidad de la República

Introducción

Un equipo multidisciplinario de ingenieros de distintas orientaciones bajo un convenio financiado por ANTEL trabajan desde hace varios años en proyectos de investigación y desarrollo en el área de Seguridad Informática. Dicho equipo ha realizado múltiples publicaciones entre las que se destaca la presente, que ha originado acciones reconocidas por (entre otros) la Organización de Estados Americanos y se ha constituido como referente internacional en la temática.

Resumen.

Se describen los modelos organizacionales identificados en [Kill03] con el objetivo de unificar la terminología y obtener conocimiento en las formas de organización más comúnmente utilizadas por CSIRTs establecidos. Asimismo se describen las principales ventajas y desventajas de cada modelo y se señalan las situaciones a las que mejor se adapta cada uno.

Los diferentes modelos organizacionales son presentados con diferente grado de profundidad y detalle. El detalle es mayor para el modelo Equipo de Seguridad, por ser una forma de organización de hecho muy difundida en nuestro medio, y para el modelo Coordinador por ser el que se ajusta a las características del futuro CERT nacional.

Finalmente se compara la canasta de servicios y otras características del futuro CERT nacional con los modelos descritos, verificándose que se ajusta al modelo de CSIRT Coordinador.

1 Modelos organizacionales más comunes

Esta sección resume la descripción de modelos organizacionales de CSIRTs presentada en [Kill03]. En dicho documento se identifican y describen en detalle cinco modelos organizacionales para equipos de respuesta a incidentes de seguridad informática:

- **Equipo de seguridad**: esta es la organización que se da de hecho cuando no existe un CSIRT constituido. No hay una asignación formal de responsabilidades respecto a los incidentes de seguridad. El personal existente, usualmente de TI, maneja los eventos de seguridad como parte de su actividad habitual.
- **Modelo distribuido**: una estructura central pequeña (al menos un gerente de seguridad) supervisa y coordina al personal del equipo distribuido en la organización. El personal del equipo distribuido es personal previamente existente en la organización. Se le asignan explícitamente responsabilidades relativas a seguridad, a las que se dedica parcial o totalmente. Este modelo se adecúa bien a organizaciones grandes en las que un equipo centralizado puede ser insuficiente.
- **Modelo centralizado**: un equipo centralizado de personal a tiempo completo toma responsabilidad sobre la seguridad en toda la organización.

- **Modelo combinado**: es una combinación de los dos anteriores.
- **Modelo coordinador**: es un equipo centralizado que coordina y facilita el manejo de incidentes de seguridad. Por lo general atiende a una comunidad objetivo formada por organizaciones externas múltiples y diversas.

En las siguientes secciones se describe más en detalle cada uno de estos modelos. En particular se analiza la estructura organizacional y la comunidad objetivo a las que mejor se adecua, los servicios que habitualmente brindan y los recursos necesarios para operar un CSIRT de esas características. Es notoria la diferencia en el grado de profundidad y detalle con que se presentan los diferentes modelos. Se ha puesto énfasis en la descripción del primero y el último de los modelos: el primero (equipo de seguridad) por ser una forma de organización de hecho muy difundida en nuestro medio, y el último (modelo coordinador) por ser el que se ajusta a las características del futuro CERT nacional.

Con respecto a los servicios brindados por los diferentes CSIRTs, se siguió la categorización de los mismos realizada en "Handbook for Computer Security Incident Response Teams (CSIRTs) " [West03] y "CSIRT Services List" [Kill02]. La descripción que sigue se limita a enumerar los servicios brindados en cada modelo y en algunos casos a señalar las características particulares de la forma en que se brindan los mismos en un CSIRT con ese modelo. Por una descripción completa de los diferentes servicios que puede brindar un CSIRT remitimos al lector a las referencias.

1.1 Modelo Equipo de Seguridad

Un equipo de seguridad ("security team") no es un modelo típico de CSIRT. Por el contrario, esta es la organización que se da más a menudo cuando no existe un CSIRT formalmente constituido.

En este modelo no existe una entidad centralizada a la que se le asigne explícitamente la responsabilidad de la coordinación del manejo de incidentes dentro de la organización.

Las tareas de manejo de incidentes son desarrolladas por administradores de sistemas y de la red, los mismos que normalmente mantienen y configuran las redes y equipos de la organización.

No existe una autoridad transversal a la organización que provea el manejo de incidentes de seguridad ni que recoja y analice información en forma centralizada. Por el contrario, en cada porción de la organización individuos o pequeños grupos son responsables localmente de la seguridad, conjuntamente con otras responsabilidades operativas. En caso de un incidente el gerente de cada una de esas áreas tiene autoridad plena para tomar acciones en su área de competencia. La coordinación para el manejo de incidentes es muy escasa, cada área actúa de acuerdo a sus necesidades y posibilidades.

En general, el objetivo primario en caso de un incidente en un equipo de estas características es restablecer el servicio afectado tan pronto como sea posible.

Si bien un equipo de seguridad no lo es formalmente, en muchos aspectos juega el rol de un CSIRT. Constituye además una forma de organización que se encuentra presente en un alto porcentaje de las organizaciones del medio nacional, que van a formar la comunidad objetivo de un futuro CSIRT nacional.

Comunidad soportada

Este modelo se encuentra en organizaciones con pocas necesidades en cuanto a administración de incidentes de seguridad. Si es necesario, se forman equipos pequeños para manejar aspectos específicos: Firewalls, VPNs, IDS, antivirus, mantenimiento e implementación de configuraciones de seguridad para hosts, etc.. Este modelo se encuentra usualmente en organizaciones de todo tipo (comerciales, gubernamentales, instituciones educativas).

Estructura Organizacional

No existe en este caso una estructura organizacional para el manejo de incidentes. Los reportes de incidentes se encaminan según la tecnología involucrada o las divisiones operativas de la organización que son afectadas.

La responsabilidad de cuestiones relacionadas con incidentes de seguridad es de los administradores de redes y de sistemas. Usualmente estos administradores no poseen una forma centralizada de comunicación y colaboración para coordinar los esfuerzos durante el manejo de incidentes.

En general no existen tampoco de información de incidentes que puedan ser utilizados para obtener una idea global de la actividad relativa a los mismos. Asimismo, es usual que no se disponga tampoco de personal con experiencia y enfocado a interactuar con grupos externos, actores legales u otros CSIRTs.

Triage

La función de triage en este modelo es manejada en forma ad-hoc. Los incidentes pueden ser reportados a través de múltiples puntos de contacto (escritorio de ayuda centralizado, escritorios de ayuda de diferentes divisiones, de manera informal a expertos en cada área, etc.).

Cada actor del equipo puede desarrollar su propio conjunto de procedimientos para procesar, ordenar y priorizar la información entrante.

En estas condiciones, difícilmente la información pueda ser consolidada y analizada, por lo que resulta muy difícil o imposible obtener una idea global sobre la actividad relacionada con el incidente en toda la organización. Ésta es una de las debilidades más importantes de este modelo.

Servicios

Servicios básicos

Los servicios básicos brindados en este modelo están alineados con el hecho de que la misión principal de los miembros del equipo es la de restaurar el servicio en los sistemas afectados.

- Análisis de incidentes.- Se realiza con el objetivo de determinar si ha ocurrido un incidente de seguridad, cuánto se ha expandido dentro del ámbito de acción del que realiza el análisis, y qué impacto se espera que tenga. A menudo este análisis incluye investigación y búsqueda de información existente sobre maneras de mitigar los efectos del incidente. El análisis se realiza en forma distribuida, por personal con diferentes niveles de experiencia y sin compartir los resultados. Es frecuente la repetición de esfuerzos y la propagación de problemas en partes de la organización cuando en otras partes el problema ya está diagnosticado y controlado.
- Respuesta a incidentes en sitio.- La respuesta a incidentes en sitio se da naturalmente en este modelo, ya que el personal del equipo de seguridad se encuentra distribuido en la organización y tiene como parte de sus responsabilidades mantener los servicios operativos.
- Coordinación de respuesta a incidentes.- Se realiza localmente dentro de cada grupo afectado. La coordinación entre grupos es mínima y es realizada expresamente en cada caso.
- Respuesta a Vulnerabilidades y artifacts, Configuración y mantenimiento de herramientas de seguridad, IDS. Realizados como parte de las tareas normales de los integrantes del equipo.

Servicios adicionales

Los servicios adicionales más comúnmente brindados por Equipos de Seguridad son la difusión de Alertas, el Análisis de vulnerabilidades y de artifacts y el desarrollo de herramientas de seguridad.

Recursos

Staff

Se utiliza el personal existente.

Las habilidades del equipo determinan el nivel y la calidad de la respuesta que se dará a los incidentes de seguridad.

Existe un potencial gasto de recursos en actividades duplicadas en diferentes partes de la organización o realizadas en forma ineficiente.

Equipamiento

No se requiere equipamiento adicional.

Infraestructura

Se utiliza la existente.

Resumen

Este modelo no define un verdadero CSIRT, sino que es la manera en que de hecho se procura resolver los problemas de seguridad en organizaciones con pocos recursos o pocos requerimientos en estos aspectos.

Un punto crítico para el buen desempeño de este modelo es contar con guías de seguridad, políticas efectivas y procedimientos detallados, todos correcta y precisamente escritos.

La comunidad debe confiar en estas medidas, ya que la capacidad de respuesta coordinada a incidentes de seguridad es mínima o inexistente.

Es necesario definir un método para contactar y notificar al resto de la organización, en el caso de ocurrir un incidente.

1.2 Modelo Interno Distribuido

En un CSIRT interno distribuido el equipo de trabajo está formado por personal de diferentes sectores dentro de la organización, que reportan a un gerente del CSIRT que opera centralmente junto con una pequeña estructura.

A diferencia del modelo anterior, un CSIRT distribuido es una entidad formalmente reconocida dentro de la organización, con asignación explícita de responsabilidades a sus miembros en lo que respecta a la seguridad informática.

En este caso, por lo general el CSIRT tiene autoridad completa para análisis, y compartida para responder a los incidentes cuando estos ocurren.

Comunidad soportada

Este tipo de modelo organizacional se encuentra en organizaciones grandes y distribuidas como puede ser una empresa multinacional o algunas organizaciones de gobierno. No se adapta bien para atender las necesidades de organizaciones pequeñas en las que resulta más eficiente un modelo centralizado.

Estructura Organizacional

Existen diferentes formas en que un CSIRT distribuido puede estar estructurado. La elección de la que se utilice está influida por el tamaño y la cantidad de instalaciones físicas de la organización, su distribución geográfica, la complejidad de su infraestructura informática, los servicios que ofrece el CSIRT y los conocimientos y experiencia del personal del mismo.

En todos los casos, el gerente del CSIRT es el que coordina el trabajo del equipo distribuido. Su oficina debe estar cercana a la alta gerencia, a la cual reporta. Junto con el gerente habrá una estructura central pequeña formada por integrantes del equipo y personal de apoyo. El gerente es el punto de contacto del CSIRT para interactuar con organizaciones externas y con otras partes de la propia organización. Debe tener un suplente designado con la capacitación adecuada para que el CSIRT pueda seguir funcionando correctamente cuando el gerente no esté disponible.

Los miembros del equipo son reclutados dentro del staff existente en la organización, para dedicar parte de su tiempo a tareas de manejo de incidentes, tanto activas como reactivas. El porcentaje de dedicación es negociado entre el gerente del CSIRT y el supervisor del miembro del equipo. Si no se logra una dedicación a tiempo completo para las tareas del CSIRT, entonces ese miembro del equipo reporta a dos supervisores: el gerente del CSIRT para las tareas relacionadas con seguridad y el gerente de su área o división dentro de la organización para las tareas operativas.

La asignación de responsabilidades a los miembros del equipo distribuido se realiza combinando diferentes criterios: ubicación geográfica, experiencia y conocimientos en las diferentes plataformas en uso, unidad de negocios o división dentro de la organización.

Es importante, para el correcto funcionamiento de este modelo, que todos los actores involucrados tengan claramente asumido que los integrantes del equipo distribuido deben poder abandonar sus tareas de rutina, cuando sea requerido para realizar el manejo de incidentes. Dado que, a menudo, los integrantes del equipo son expertos en los sistemas en los que trabajan diariamente, cuando se produce un incidente importante van a recibir fuertes requerimientos en forma simultánea desde el CSIRT para el manejo del incidente y desde su división de origen para combatir el impacto del incidente.

El equipo distribuido tiene un rol importante en fortalecer la presencia del CSIRT en las diferentes divisiones dentro de la organización. Esto es importante, para asegurar por un lado que los eventos y actividades inusuales sean reportados en tiempo, y por otro, para asegurar que las recomendaciones y las actividades de respuesta a un incidente sean realizadas.

La función de la oficina del gerente del CSIRT es analizar la información recibida desde las diferentes divisiones para ayudar a determinar el alcance y el impacto de un incidente, y para identificar tendencias y acciones correctivas que deben ser distribuidas dentro de la organización. El gerente es, además, el que coordina el trabajo de los integrantes del CSIRT.

Hay varios elementos importantes para posibilitar el buen funcionamiento de un CSIRT distribuido:

- debe existir un apoyo gerencial fuerte
- deben existir o desarrollarse: políticas, procedimientos y líneas de responsabilidad claras
- debe existir una infraestructura segura para que los integrantes del equipo puedan

comunicarse en forma ágil y puedan realizar el registro y seguimiento de incidentes

- deben fomentarse actividades que contribuyan a formar un espíritu de equipo entre los integrantes, a pesar de estar distribuidos geográficamente y en diferentes divisiones dentro de la organización.

Triage

Las principales alternativas para el ingreso, priorización y asignación de reportes de eventos son o bien utilizar si existe un Help Desk centralizado de la organización o bien recibir los reportes en forma distribuida en cada área o división.

En el primer caso el triage es llevado a cabo por el gerente del CSIRT, asignando la tarea al miembro del equipo que resulte más adecuado. En el segundo caso será un integrante del equipo distribuido el que realice la asignación.

Aunque se elija la opción distribuida para el ingreso de los reportes, toda la actividad debe ser registrada centralmente para facilitar el seguimiento por parte de los diferentes integrantes del equipo involucrados, y para poder realizar un análisis global de las actividades relacionadas con seguridad en toda la organización.

Servicios

En la sección Servicios Básicos se describen los servicios que brindan la mayoría de los CSIRTs de este modelo organizacional. Además de esos servicios básicos, muchos CSIRTs eligen ofrecer servicios adicionales, los que más frecuentemente aparecen se enumeran en la sección Servicios Adicionales.

Servicios Básicos

Los servicios básicos en este modelo son:

- Alertas y advertencias.- Recibidos en forma centralizada por el gerente o un miembro del equipo designado por él, se distribuyen a todos los miembros del equipo y de ahí a administradores de sistema y redes en cada sitio.
- Análisis de incidentes.- Realizado por cada miembro del equipo en su área de responsabilidad, siendo la oficina del gerente responsable de correlacionar la información de las diferentes áreas.
- Soporte en respuesta a incidentes.- Trabajando en conjunto con los administradores de sistema locales
- Coordinación de respuesta a incidentes.- Es responsabilidad del gerente o de personas designadas por él. Debe mantener informados a los integrantes del equipo distribuido y difundir estrategias de respuesta durante un incidente. Tambien es el principal punto de contacto con la gerencia superior y con otras áreas dentro de la organización.
- Coordinación de respuesta a vulnerabilidades y artifacts.- Se maneja en forma similar a la coordinación de respuesta a incidentes.
- Anuncios

Servicios adicionales

- Respuesta en sitio.- Facilitado por la presencia local de los miembros del equipo distribuido, que en algunos casos se desempeñan también como administradores de red y de sistema.

- Análisis y respuesta a vulnerabilidades y “artifacts”.
- Observatorio tecnológico.
- Auditoría o evaluación de seguridad.
- Configuración y mantenimiento de herramientas, aplicaciones e infraestructuras.
- Desarrollo de herramientas.
- Servicios de detección de intrusiones (IDS).
- Difusión de información.

Recursos

A continuación, se da una somera descripción de los recursos necesarios por este modelo organizacional en términos de personal, equipamiento e infraestructura.

Staff

- Gerente del CSIRT (y suplente designado).
- Uno o más administradores de sistema para la infraestructura del CSIRT (pueden ser de tiempo completo o formar parte del equipo de administración de sistemas de la organización).
- Uno o más administrativos.
- Uno o más analistas, dependiendo de los servicios ofrecidos. Cooperan en la elaboración de estadísticas de incidentes, de alertas de seguridad y otros documentos técnicos.
- Miembros del equipo distribuido, en cantidad a definir por la organización dependiendo del tamaño y distribución geográfica de la misma y de los servicios ofrecidos. Debe preverse personal suplente para cubrir licencias, asistencia a reuniones del equipo, etc..
- Otras funciones (redactores, instructores, relaciones públicas, legal, otros) ser requerirán a demanda, pero debe estar acordada previamente su disponibilidad.

Los servicios que brindará el CSIRT se seleccionan teniendo en cuenta los conocimientos y habilidades del personal disponible. Todo el personal necesitará capacitación y entrenamiento sobre el manejo de incidentes y sobre el funcionamiento y finalidades de un CSIRT.

Deben instrumentarse reuniones generales para fomentar el espíritu de equipo y aumentar el conocimiento y la confianza entre los miembros. Pueden aprovecharse para eso instancias de capacitación.

Equipamiento

Los miembros del equipo distribuido utilizarán el equipamiento existente para sus necesidades diarias. A menudo será necesario equipamiento adicional para realizar pruebas.

La oficina central del gerente del CSIRT requerirá también equipamiento:

- Espacio y equipamiento de oficina.
- Computadores, telefonía, pagers.
- Eventualmente “home equipment” y acceso remoto

Infraestructura

Se deberá tener acceso para todos los miembros del equipo a los siguientes recursos:

- Sistema seguro de seguimiento de reportes de incidentes

- Repositorio seguro para archivo de incidentes y "artifacts"
- Canales de comunicación seguros (e-mail, teléfonos, teleconferencia, intranet, ...)

Adicionalmente, puede ser bueno disponer de una infraestructura segura (acceso físico, energía, respaldos, virus, ...) recursos de red y servidores separados de los del resto de la organización con acceso VPN para miembros del equipo distribuido

Resumen

Los puntos fuertes de este modelo organizacional son:

- Una buena inserción en la comunidad objetivo a través de los miembros del equipo distribuido.
- Fuerte realimentación de información para la elaboración de políticas y procedimientos.

Las debilidades más importantes en cambio, son:

- Puede ser difícil mantener al día las habilidades del equipo. Importante reservar tiempo y energías para su actualización (evitar el "staff burnout").
- Pueden surgir problemas originados en la distribución geográfica: comunicaciones, inconsistencias en la implementación de las medidas de prevención, mitigación y recuperación de incidentes.
- Posibles conflictos de prioridades del personal part time.

1.3 Modelo Interno Centralizado

En este modelo organizacional hay un equipo central al que se le asigna la responsabilidad del manejo de incidentes en toda la organización.

Este equipo tiene autoridad completa para el análisis de los incidentes. Para la respuesta frente a los incidentes pueden darse diferentes situaciones, con autoridad completa o compartida con apoyo de la gerencia superior y eventualmente con participación de las divisiones afectadas.

Comunidad soportada

El modelo centralizado se adapta bien a organizaciones pequeñas, en las que un equipo central de tamaño moderado puede ser suficiente para atender las necesidades de la organización.

Se puede implementar también en organizaciones mayores y dispersas geográficamente siempre y cuando las entidades distribuidas tengan características y organización uniformes.

Estructura Organizacional

Es fuertemente deseable que el personal del equipo reúna experiencia y conocimientos en todos los sistemas soportados. Si esto no fuera posible, se deben identificar expertos en el resto de la organización que puedan trabajar junto con el CSIRT cuando sea necesario.

Las oficinas y el lugar físico asignado al CSIRT centralizado debe estar ubicado cerca del nivel gerencial superior, al cual reporta el gerente del CSIRT. Éste representa al CSIRT en la interacción con el resto de la organización.

Por lo general, el personal asignado a un CSIRT centralizado tiene una dedicación de tiempo completo al mismo. Sin embargo, en presencia de restricciones presupuestales en algunas organizaciones muy pequeñas, un régimen de dedicación parcial utilizado, es el de alternar períodos de dedicación al CSIRT con períodos de dedicación al resto de las tareas de, por ejemplo, administración de sistemas y redes.

Triage

Normalmente existe un mecanismo centralizado (dirección de e-mail o número telefónico) para contactar al CSIRT, ya sea para reportar un incidente o para solicitar otros servicios. Deben difundirse ampliamente los horarios de atención, los servicios disponibles y guías sobre cómo reportar incidentes para ayudar a la comunidad objetivo a interactuar con el CSIRT.

La función de recepción de reportes puede estar incorporada en el CSIRT en un escritorio de ayuda propio o se puede utilizar el escritorio de ayuda central de la organización que derive los reportes relacionados con seguridad al CSIRT.

Al reunir todos los reportes en un repositorio central se facilita su análisis para elaborar un panorama de las actividades relacionadas con incidentes de seguridad en toda la organización.

Servicios

En la sección Servicios Básicos se describen los servicios que brindan la mayoría de los CSIRTs de este modelo organizacional. Además de esos servicios básicos muchos CSIRTs eligen ofrecer servicios adicionales, los que más frecuentemente aparecen se describen en la sección Servicios Adicionales.

Servicios Básicos

Los servicios básicos presentes en la mayoría de los CSIRTs de este modelo son:

- Alertas y advertencias.- Se reciben centralmente desde el exterior, y redistribuyen según su gravedad a una lista de personas y unidades dentro de la organización, que deben ser notificadas, o a una lista de e-mail interna. Es importante mantener actualizada la lista de contactos a ser notificados.
- Análisis de incidentes.- La naturaleza centralizada del CSIRT hace que puedan encontrarse dificultades en el análisis, debido a desconocimiento por parte de los miembros del CSIRT de la operación diaria y las necesidades en cada unidad de negocio. Por eso, a menudo, debe involucrarse a las áreas operativas y de negocio en el análisis de incidentes que las afecten.
- Soporte y coordinación de respuesta a incidentes.- El CSIRT centralizado debe establecer una relación de cooperación con el resto de la organización. En una organización grande, el CSIRT centralizado es responsable de enviar información técnica y guías sobre como manejar la situación y recuperarse de un determinado incidente de seguridad. Esta información debe ser enviada también a los gerentes de las unidades de negocio para que estén informados. Puede ser una dificultad en este modelo determinar si las acciones correspondientes son tomadas en todas las divisiones de la organización, por lo que deben implantarse herramientas que aseguren la consistencia.
- Coordinación de respuesta a vulnerabilidades y "artifacts".- El CSIRT centralizado debe concentrar la recolección de información y distribuir las guías para detección y recuperación. Usualmente, esta actividad se realiza apoyándose fuertemente en otros CSIRTs con mayor desarrollo, o en información de fabricantes. De todos modos, el CSIRT debe funcionar centralizando la información y difundiéndola de manera adecuada dentro de la organización.
- Anuncios, Observatorio tecnológico, Difusión de información.- Un CSIRT centralizado con staff a tiempo completo está en mejores condiciones, que en los casos anteriormente analizados, para mantenerse al día en las diferentes tecnologías, recibir, clasificar y priorizar anuncios relativos a seguridad y distribuir la información relevante al resto de la organización.

Servicios Adicionales

- Respuesta en sitio.
- Análisis de vulnerabilidades y "artifacts".
- Auditorías o valoraciones de seguridad.
- Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras.
- Desarrollo de herramientas de seguridad.
- Servicios de detección de intrusiones (IDS).

Recursos

A continuación se da una somera descripción de los recursos necesarios para el modelo centralizado en términos de personal, equipamiento e infraestructura.

Staff

- Gerente del CSIRT y su suplente designado
- Un administrativo
- Personal técnico. La cantidad de personal técnico dependerá de factores como los servicios ofrecidos, los recursos disponibles y la amplitud del horario de atención cubierto. En algunos casos parte de las tareas se cubren con personal que realiza turnos rotativos, por ejemplo cada una semana.

Si hay recursos suficientes puede ser deseable incorporar también:

- uno o más administradores de sistema para el mantenimiento de la infraestructura informática del CSIRT. Esto puede eventualmente ser un cargo compartido con otra área dentro de la organización,
- una o más personas para las tareas de atención de llamadas y triage. El personal del CSIRT necesario para estas tareas depende de si se optó por utilizar el Help desk de la organización o montar uno propio del CSIRT.

Otras tareas son requeridas a demanda. Debe identificarse dentro de la organización personal para tareas de redacción técnica, relaciones públicas, asesoramiento legal, instructores, etc., y acordar previamente que estén disponibles cuando sea necesario.

Equipamiento

Se necesita equipo para apoyar al personal del CSIRT centralizado. Esto incluye:

- espacio y equipamiento de oficina
- equipamiento de computación para el trabajo diario
- instalaciones para laboratorio de test
- equipos para acceso remoto (casa, viajes, visitas en sitio)
- teléfonos, fax, celular, pagers, etc..

Puede ser necesario equipo adicional para la realización de pruebas. En algunos casos este equipamiento adicional puede obtenerse temporalmente en préstamo de otras secciones dentro de la organización.

Infraestructura

La infraestructura a utilizar debe brindar un ambiente seguro para la operación diaria del CSIRT debe incluir:

- seguridad de acceso físico
- energía
- red separada o firewall
- seguridad de red y servidores
- intranet, web
- sistema de seguimiento, repositorio de datos y reportes relativos a incidentes
- comunicaciones seguras
- respaldos, tecnologías de cifrado, antivirus, etc..

Resumen

El modelo centralizado se adapta bien a organizaciones pequeñas en las que un reducido grupo central puede atender en forma adecuada a toda la organización.

La mayor fortaleza de este modelo organizacional es que al disponer de un equipo de gente enfocado a la seguridad de la organización se tienen más oportunidades para llevar adelante actividades proactivas

Como contrapartida existe el peligro de que se produzca un aislamiento del resto de la organización: el staff del CSIRT se aleja de la operativa diaria con riesgo de no dominar los sistemas en operación, las unidades operativas se desentienden de los asuntos de seguridad transfiriendo toda la responsabilidad en el CSIRT.

1.4 Modelo Interno Combinado

Se establece un CSIRT central que interactúa con miembros del equipo distribuidos dentro de la organización.

El equipo central realiza el análisis de alto nivel y elabora recomendaciones y estrategias de recuperación y mitigación. Se encarga también de centralizar la recolección de información y de promover la toma de conciencia dentro de la organización de los problemas relacionados con seguridad.

Los miembros del equipo distribuido implementan las estrategias trabajando junto con administradores de red y sistema locales. Facilitan el análisis y la respuesta aportando conocimiento de los sistemas en operación en la organización.

El CSIRT combinado tiene autoridad completa para el análisis y es preferible que tenga autoridad compartida para la respuesta a un incidente. Con aprobación de la gerencia superior, el CSIRT puede requerir la implementación de acciones de mitigación o recuperación. Los gerentes de unidades funcionales son notificados de las acciones que deben tomarse y, es conveniente, que se los involucre en el proceso de toma de decisiones para determinar la respuesta a implementar.

Comunidad soportada

Funciona mejor en organizaciones distribuidas muy grandes. En organizaciones menores puede ser suficiente un equipo centralizado

Pueden surgir dificultades si cada parte de la organización tiene una autonomía importante, con diferente organización gerencial, políticas, procedimientos, etc. En este caso, puede ser mejor adoptar un modelo coordinador.

Estructura Organizacional

El modelo combinado incorpora características de los modelos analizados anteriormente: el modelo distribuido y el modelo centralizado.

El equipo central está formado por el gerente del CSIRT y un pequeño grupo de técnicos. Reside físicamente cerca de la gerencia superior a la que reporta.

Existen diferentes formas de distribuir las tareas y responsabilidades entre el grupo central y el equipo distribuido. Algunos ejemplos son:

- La función de triage y el análisis se realizan centralmente, asignándose tareas de respuesta a integrantes del equipo distribuido en su localidad o división dentro de la organización.
- Se reciben los reportes centralmente y cada reporte se asigna a un integrante del equipo para su análisis y respuesta con criterios de ubicación geográfica o conocimientos en la tecnología involucrada.

En forma similar al personal del Modelo Distribuido, el personal del equipo distribuido en un Modelo Combinado puede trabajar a dedicación completa o parcial en las tareas de seguridad.

Una práctica muy beneficiosa es la realización de pasantías de miembros del equipo distribuido para desempeñar tareas en el CSIRT central. Esto redunda en una mejor capacitación y comprensión de las políticas, procedimientos y procesos; y en un mejor conocimiento personal entre los miembros del equipo.

Triage

Para el triage en los CSIRTs con modelo combinado se observan dos posibles estructuras. En la primera de ellas todas las solicitudes y reportes ingresan al CSIRT central donde son clasificadas y priorizadas. En la segunda, las solicitudes ingresan en el sitio donde reside el miembro del equipo distribuido más cercano, que se encarga de atenderla inicialmente; las que no se pueden resolver se pasan al sitio central.

En cualquiera de los dos casos, el CSIRT central debe mantener una base de datos de incidentes accesible a todos los miembros del equipo distribuido, para que puedan ingresar o actualizar reportes y buscar actividades similares a las del reporte que estén atendiendo para ayudar a identificar posibles soluciones.

Al igual que en los otros modelos, es importante que existan y estén en conocimiento de la comunidad objetivo políticas y procedimientos para el reporte de incidentes y actividades anómalas y que la comunidad sea estimulada a reportar sin temor a consecuencias negativas posteriores.

Servicios

En la sección Servicios Básicos, se enumeran los servicios que brindan la mayoría de los CSIRTs de este modelo organizacional. Además de esos servicios básicos, muchos CSIRTs eligen ofrecer servicios adicionales, los que más frecuentemente aparecen se enumeran en la sección Servicios Adicionales.

Servicios Básicos

Los servicios básicos presentes en los CSIRTs combinados no son muy diferentes de los servicios brindados en los modelos distribuido y centralizado:

- Alertas y advertencias.- Son recibidos de diversas fuentes por el equipo centralizado y difundidos a los miembros del equipo distribuido y otras personas dentro de la organización.
- Análisis de incidentes.- Dirigido y coordinado por el equipo central, a menudo es realizado por miembros del equipo distribuido utilizando recursos (ambientes de test, experiencia en plataformas específicas) disponibles en un área de la organización.
- Soporte y coordinación de respuesta a incidentes.- En el modelo combinado el núcleo central y los integrantes del equipo distribuido trabajan en colaboración para desarrollar y clasificar material de soporte y distribuirlo a toda la organizaciónl. La coordinación es realizada principalmente por el equipo central, coordinando las actividades del equipo distribuido y oficiando de enlace con el resto de la organización y actores externos.
- Coordinación de respuesta a vulnerabilidades y "artifacts".- Como en el caso del CSIRT centralizado, el CSIRT combinado también concentra la recolección de información y distribuye las guías para detección y recuperación. Usualmente esta actividad se realiza apoyándose fuertemente en otros CSIRTs con mayor desarrollo o en información de fabricantes. De todos modos el CSIRT debe funcionar centralizando la información y difundiéndola de manera adecuada dentro de la organización.
- Anuncios, Observatorio tecnológico, Difusión de información.- Al igual que el CSIRT centralizado, un CSIRT combinado asigna recursos para estar al día en las diferentes tecnologías, recibir, clasificar y priorizar anuncios relativos a seguridad y distribuir la información relevante al resto de la organización.

Servicios Adicionales

- Respuesta en sitio. Este servicio es facilitado en este modelo por la presencia de los miembros del equipo distribuido trabajando conjuntamente con los administradores de red y sistemas en cada división.
- Servicios de detección de intrusiones (IDS).
- Análisis de vulnerabilidades y "artifacts".
- Auditoría o evaluación de seguridad.

Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructura.

- Desarrollo de herramientas.

Recursos

A continuación, se da una somera descripción de los recursos necesarios para el modelo centralizado en términos de personal, equipamiento e infraestructura.

Staff

En el CSIRT combinado el personal del equipo central usualmente dedica el 100% de su tiempo a tareas de seguridad, mientras que el personal distribuido puede dedicarse a tiempo completo o compartir su tiempo con tareas locales de administración de redes y sistemas.

El equipo central incluye los siguientes roles:

- un gerente y su suplente designado
- una persona de apoyo administrativo
- personal técnico (típicamente entre 4 y 6). La cantidad de personal técnico necesario

dependerá del tamaño y complejidad de la comunidad objetivo y de los servicios brindados

- uno o más administradores de sistema para soporte a la infraestructura, aporta también experiencia y conocimientos en las plataformas que administra. Puede ser compartido con otra división en la organización
- personal para atención telefónica y triage. Puede ser parte de un Help desk central.

El equipo distribuido, por su parte, incluye:

- personal técnico distribuido, con dedicación parcial o total, con suplentes identificados
- además a demanda pero acordado previamente: redactores técnicos, relaciones públicas, legal, instructores, especialistas en determinadas tecnologías.

La cantidad de personal necesaria queda determinada por el tamaño y la diversidad de ubicaciones geográficas y de plataformas en la organización.

Equipamiento

El equipamiento necesario para el equipo central incluye:

- espacio y equipamiento de oficina
- equipamiento de computación para el trabajo diario
- instalaciones para laboratorio de test
- equipos para acceso remoto (desde la casa, en viajes, visitas en sitio)
- teléfonos, fax, celular, pagers, etc..

Los miembros del equipo distribuido utilizarán equipamiento propio del CSIRT o equipamiento existente localmente. En cualquiera de los dos casos se deberá disponer de medios de comunicación seguros con el CSIRT central, incluyendo teléfono, e-mail, intranet.

Infraestructura (segura)

La infraestructura a utilizar debe brindar un ambiente seguro para la operación diaria del CSIRT, incluyendo:

- seguridad de acceso físico
- energía
- red separada o firewall
- seguridad de red y servidores
- intranet, web
- sistema de seguimiento, repositorio de datos y reportes relativos a incidentes
- comunicaciones
- respaldos, tecnologías de cifrado, antivirus, etc..

Resumen

El modelo combinado consta de un núcleo estable central trabajando en conjunto con una red de miembros insertos en las unidades operativas de la organización.

Este modelo se utiliza con ventaja en organizaciones muy grandes y con características no uniformes.

El núcleo central provee estabilidad, conocimiento y una estructura permanente. Los miembros distribuidos del equipo aportan conocimiento de las operaciones de la organización y conexión con las unidades de negocio a nivel local.

La principal debilidad es la dificultad de coordinar un equipo disperso geográficamente y en diversas unidades de la organización.

1.5 Modelo Coordinador

En este modelo el CSIRT está enfocado principalmente a coordinar y facilitar las actividades de manejo de vulnerabilidades e incidentes en una comunidad amplia, diversa y en general externa.

Este rol puede involucrar el compartir información, suministrar estrategias de mitigación y recomendaciones para la recuperación posterior a un incidente, analizar e investigar tendencias y patrones de la actividad de incidentes en la comunidad, proveer recursos para el manejo de incidentes, tales como recomendaciones, alertas, bases de datos de vulnerabilidades, herramientas, etc. o referencias a los mismos.

Existen diferentes situaciones en cuanto al nivel de autoridad del CSIRT sobre su comunidad objetivo. A menudo este nivel de autoridad es mínimo o nulo, como es el caso en un CSIRT coordinador nacional. En estos casos el CSIRT coordinador provee consejo y recomendaciones, pero son los integrantes de la comunidad objetivo los que deciden seguir o no esas recomendaciones. En base a su reputación el CSIRT puede influir positivamente en esa toma de decisiones.

Comunidad soportada

Un CSIRT coordinador atiende a una comunidad objetivo distribuida. En general esta comunidad está formada por múltiples entidades independientes. Algunas de estas entidades podrán contar con su propio CSIRT interno, en cuyo caso será el punto de contacto con el cual interactuará el CSIRT coordinador.

Usualmente estas entidades son organizaciones que tienen alguna característica en común por la que se define su pertenencia a la comunidad objetivo del CSIRT coordinador. Ejemplos de esto son:

- Conectividad a determinada red
- Ubicación geográfica, p. ej. un CSIRT nacional o regional
- Pertenencia a determinada organización o grupo de empresas

Estructura Organizacional

Por lo general un CSIRT coordinador funciona centralizado y con staff dedicado a tiempo completo.

Idealmente el personal del CSIRT debería reunir expertise en todas las plataformas y sistemas instalados en la comunidad objetivo. La gran diversidad de sistemas involucrados en la comunidad objetivo de un CSIRT coordinador hace que sea muy difícil dominar todas las posibles plataformas con staff propio. Resulta importante entonces identificar y contactar a expertos externos al CSIRT para incorporarlos cuando sea necesario.

Un CSIRT coordinador debe ser neutral para poder recibir y analizar información de toda la comunidad, y así ser capaz de elaborar y difundir un panorama global de la actividad de incidentes.

Triage

Es una función central para la operación de un CSIRT coordinador.

Debe existir un punto de contacto claramente definido.

Deben elaborarse y ser difundidas descripciones claras de los servicios que se brindan, horarios de atención y guías sobre qué y como reportar. Estas guías y referencias deben estar disponibles en línea para asistir al personal de las organizaciones de la comunidad objetivo al momento de reportar un incidente.

El personal encargado de la función de triage debe estar identificado. Para asistir a dicho personal deben elaborarse guías explícitas indicando qué requerimientos deben ser atendidos (y cuáles no).

Servicios

En la sección Servicios Básicos se describen los servicios que brindan la mayoría de los CSIRTs de este modelo organizacional. Además de esos servicios básicos muchos CSIRTs eligen ofrecer servicios adicionales, los que más frecuentemente aparecen se describen la sección Servicios Adicionales.

Servicios Básicos

- Alertas y advertencias

Desde la creación de los primeros CSIRTs, este servicio ha sido parte del conjunto básico de servicios ofrecido por CSIRTs coordinadores. En la operación diaria de un CSIRT se recibe y clasifica información de diversas fuentes, concentrándose en la información relacionada con riesgos que puedan afectar a la comunidad objetivo. Como parte del trabajo del CSIRT se reenvía a los puntos de contacto de las organizaciones de la comunidad objetivo todo lo relacionado con alertas y advertencias. Además el CSIRT puede elaborar y difundir sus propias alertas y advertencias, en base a información y análisis de actividad local.

A menudo los alertas y advertencias difundidos deben ser refinados o ampliados en base a respuestas desde la comunidad o a investigación posterior del propio CSIRT.

- Análisis de incidentes

Un CSIRT coordinador hace el análisis de los reportes de incidentes recibidos para determinar la naturaleza y el alcance de la actividad reportada y las estrategias de mitigación y recuperación más adecuadas para aplicar. El objetivo no es recuperar el sistema de un miembro en particular sino comprender lo que sucede con ese ataque y correlacionarlo con otras actividades detectadas en los sistemas y redes de la comunidad objetivo. En general el análisis en profundidad o un análisis forense detallado es realizado por el CSIRT o equipo de seguridad de la organización afectada.

El CSIRT realiza el análisis de incidentes para entender lo que está sucediendo en toda la comunidad y formarse una idea global de la actividad de incidentes. En base a eso elabora recomendaciones para reforzar la seguridad general cuando sea posible. Puede identificar tendencias y métodos de ataque y utiliza esa información para sugerir estrategias de defensa para los sistemas de la comunidad.

- Soporte de respuesta a incidentes

Como un CSIRT coordinador no tiene presencia en sitio y debe atender a múltiples organizaciones en su comunidad, su principal enfoque será de soporte o apoyo a las diversas organizaciones de su comunidad. Las actividades de soporte pueden incluir:

  - responder preguntas por teléfono o e-mail
  - investigar y analizar incidentes, vulnerabilidades y artifacts y proveer la información resultante colectivamente a la comunidad
  - mantener un archivo accesible por la comunidad con información de incidentes, vulnerabilidades y artifacts
  - crear y difundir recomendaciones y alertas con estrategias de respuesta y recuperación
  - crear documentos técnicos describiendo mejores prácticas
  - desarrollar materiales para concientización, educación y entrenamiento de su comunidad

La difusión de la información puede hacerse por sitios web, teléfono o listas de correo. Cada entidad de la comunidad determina quién será su contacto para recibir la información y asistencia y quién deberá seguir las recomendaciones y realizar las tareas de respuesta en caso necesario.

- Coordinación de respuesta a incidentes, vulnerabilidades y artifacts

La coordinación de respuesta a incidentes es una de sus principales funciones de un CSIRT Coordinador. Este CSIRT puede proveer a su comunidad el seguimiento, registro y difusión de información relativa a los incidentes. Consolidando la información recolectada, el CSIRT Coordinador está mejor capacitado para identificar ataques, tendencias y patrones similares en el ámbito de su comunidad. Pueden ser identificadas a tiempo potenciales nuevas amenazas, y pueden ser desarrolladas y difundidas las correspondientes estrategias de mitigación. El trabajo de coordinación en este modelo es principalmente de intercambiar información y facilitar la interacción entre las partes involucradas en la recuperación y análisis del incidente.

A pesar de ser deseable, es poco probable que el staff del CSIRT coordinador pueda reunir expertos en todas las plataformas y sistemas en uso en la comunidad. Por lo tanto será necesario convocar a expertos externos, que podrán provenir de organizaciones de la comunidad objetivo, proveedores u otros CSIRT, para cooperar en el análisis. El CSIRT coordinador puede actuar como facilitador o principal punto de contacto para reunir a todas esas organizaciones. Está en condiciones también de ser el principal punto de distribución para difundir rápidamente al resto de la comunidad las estrategias de respuesta que resulten de ese análisis.

Finalmente, como el CSIRT coordinador es un punto de contacto conocido para interactuar con su comunidad, seguramente recibirá advertencias y alertas de otras organizaciones o CSIRTs que deberán ser redistribuidas a las organizaciones involucradas.

Todo lo dicho para la coordinación de la respuesta a incidentes vale para la coordinación de la respuesta a nuevas vulnerabilidades y artifacts.

- Anuncios, Observatorio tecnológico, Difusión de información relacionada con seguridad

Dado que un CSIRT coordinador recibe información desde las organizaciones de su comunidad y de diversos expertos y grupos externos, está en una buena posición para elaborar y difundir un panorama de la actividad de incidentes en el ámbito de su comunidad. Puede hacer esto a través de anuncios generales destinados a mejorar el nivel de conciencia de su comunidad con respecto a nuevas tendencias que puedan afectar la seguridad de la misma. El CSIRT coordinador puede también ayudar a las organizaciones a defender sus activos críticos en forma proactiva haciéndoles llegar anuncios de vulnerabilidades y artifacts descubiertos recientemente para que puedan chequear y corregir sus sistemas antes que las vulnerabilidades sean explotadas.

En la medida que se liberen recursos se puede asignar a miembros del equipo del CSIRT la tarea de recolectar y sistematizar información sobre modalidades de ataque, amenazas y tendencias para las diversas tecnologías en uso en la comunidad. Esta información debe hacerse disponible en una primera instancia para el resto del staff del CSIRT mediante una intranet o algún repositorio similar. La información que sea de interés para la comunidad puede difundirse mediante listas de correo electrónico o sitios de discusión en Internet como forma de mantener actualizados a los miembros de la comunidad.

En forma similar, puede establecerse un repositorio web o ftp con información sobre buenas prácticas y herramientas de seguridad. En algunos casos un valor agregado importante puede ser la traducción de documentación originada en otros sitios para difundirla a la comunidad en su lengua nativa.

Concientización / Educación /Capacitación

La mayor parte de los CSIRTs coordinadores realizan actividades de educación o entrenamiento dirigida a mejorar la formación y el nivel de concientización de su comunidad objetivo.

Esto incluye la realización de cursos, tutoriales, charlas y elaboración de materiales. Estos pueden ser desarrollados en las instalaciones de los miembros de la comunidad o en instalaciones propias del CSIRT. La participación en estas actividades puede ser provista en forma gratuita para algún tipo de membresía o a través del pago de alguna tasa por cada servicio.

Servicios Adicionales

Cuando se dispone de una adecuada experiencia y del tiempo necesario por parte de los integrantes del equipo ("with the proper staff time and expertise") muchos CSIRTs coordinadores eligen brindar servicios adicionales a los descriptos en el apartado anterior.

Así es que a menudo realizan análisis de vulnerabilidades y "artifacts", en la mayoría de los casos enfocado a reportes que provienen de su propia comunidad o que potencialmente puedan afectar a la misma. En algunos casos (CERT/CC p. ej.) pueden asignar personal al análisis de vulnerabilidades trabajando en contacto con proveedores para determinar el status de determinada vulnerabilidad en sus productos. Son pocos los CSIRTs que cuentan con recursos suficientes para atacar actividades de este tipo, pero los resultados pueden ser compartidos por múltiples comunidades.

Como resultado de este análisis puede resultar información útil para mitigar o reparar vulnerabilidades o detectar y eliminar artifacts. Esta información puede difundirse a la comunidad a través de alertas, recomendaciones y documentos técnicos. Ejemplos de esto son la "Vulnerability Notes database" y el "Vulnerability Reports Catalog" elaborados por CERT/CC y la "Common Vulnerabilities and Exposures database" elaborada por MITRE.

Otra actividad adicional frecuente es la participación en el desarrollo de herramientas que puedan ser usadas por miembros de la comunidad u otros CSIRTs. Algunos grupos han desarrollado herramientas para la gestión de reportes de incidentes, otros han desarrollado "signatures" para antivirus o IDS, etc..

El resto de los servicios es menos frecuente que sea brindado por un CSIRT coordinador, pero si se cuenta con los medios y es una necesidad de la comunidad otros servicios pueden ser brindados, a menudo en base a un pago por servicio.

Recursos

A continuación se da una somera descripción de los recursos necesarios por este modelo organizacional en términos de personal, equipamiento e infraestructura.

Staff

Las funciones de un CSIRT coordinador son llevadas adelante por un núcleo central de personal a tiempo completo, con los siguientes roles:

- un gerente y su suplente designado
- personal administrativo y de soporte
- personal técnico. Varios, típicamente entre 3 y 10, dependiendo de los servicios ofrecidos y del tamaño y diversidad de la comunidad. Este personal realiza las tareas de análisis y manejo de incidentes y las tareas de formación y entrenamiento
- Administradores de sistema para dar soporte a la infraestructura
- personal de Hotline/triage/Help desk

Para tareas adicionales de soporte al trabajo del núcleo básico debe identificarse y acordarse con antelación la participación de redactores técnicos, asesores legales y en relaciones públicas. Asimismo deben identificarse y contactarse expertos en áreas y tecnologías usadas en la comunidad en las que no se tenga suficiente experiencia dentro del equipo para recurrir a ellos cuando sea necesario.

Equipamiento

El equipamiento necesario para el personal de CSIRT coordinador incluye:

- Espacio y equipamiento de oficina (escritorios, copiadoras, insumos)
- Equipamiento de computación para el trabajo diario
- Instalaciones que no esté utilizado en producción para laboratorios de test
- Equipos para acceso remoto (desde la casa, viajes, visitas en sitio)
- Teléfonos, fax, celular, pagers, ...

Infraestructura

La infraestructura necesaria para el trabajo diario del CSIRT incluye:

- Seguridad de acceso físico
- Energía
- Red separada o firewall
- Seguridad de red y servidores
- Intranet, web
- Sistema de seguimiento de reportes y repositorio de datos relativos a incidentes
- Comunicaciones seguras (e-mail, teléfonos, etc.)
- Respaldos, tecnologías de cifrado, antivirus, ...

Resumen

Este modelo es profundamente diferente de los descritos en las secciones anteriores de este documento. A diferencia de los anteriores, los CSIRTs coordinadores atienden los intereses de una comunidad amplia, formada por múltiples y diferentes entidades independientes.

Para poder realizar la función de coordinación con éxito, el CSIRT debe inspirar confianza en la comunidad objetivo, debe ofrecer valor agregado en los servicios que brinda y debe tener puntos de contacto y mecanismos de comunicación establecidos para interactuar con la comunidad. El tener una lista completa y verificada de puntos de contacto dentro de la comunidad ayudará a determinar quién debe ser notificado y reducirá el tiempo necesario para diseminar información de manera adecuada.

Restricciones, peligros y debilidades de este modelo

La principal restricción de este modelo es la dificultad para establecer comunicaciones efectivas con todas las entidades de la comunidad y de ganarse su confianza, de manera que los incidentes sean reportados y las recomendaciones de mitigación y prevención sean seguidas. El último punto es especialmente válido en este modelo ya que el CSIRT coordinador en la mayoría de los casos no tiene autoridad formal sobre la comunidad y actúa aconsejando y recomendando; no puede forzar a las entidades de la comunidad a cumplir las recomendaciones, ni siquiera en situaciones de ataques en gran escala.

Los miembros de la comunidad pueden elegir no seguir las recomendaciones. También pueden manejar los incidentes en forma autónoma y no reportarlo al CSIRT, limitando entonces la información que recibe el CSIRT y su capacidad para determinar el alcance, la naturaleza y el impacto de incidentes y actividades inusuales.

Otras limitaciones pueden provenir de la organización “madre” en la cual está inserto el CSIRT. Si esta organización no tiene una reputación confiable dentro de la comunidad esto puede afectar la forma en que el CSIRT es percibido y desmotivar a los miembros de la comunidad a reportar los incidentes.

Otro problema puede suscitarse cuando las expectativas de los miembros de la comunidad son superiores a los servicios realmente ofrecidos por un CSIRT coordinador. Algún miembro de la comunidad puede esperar o desear un nivel de servicio mayor que el que puede proveer el CSIRT (p. ej. podría esperar ayuda en sitio durante la respuesta a un incidente y la recuperación posterior).

Principales fortalezas del modelo

Una de las principales fortalezas de este modelo es que permite disponer de un núcleo estable de profesionales dedicado a tiempo completo a pensar en la seguridad de los sistemas en el ámbito de la comunidad objetivo definida.

Las otras ventajas provienen de la centralización de información y puntos de contacto. Así es que la centralización de reportes permite analizar información de todo el ámbito de la comunidad e identificar tendencias y elaborar información a distribuir en los miembros de la comunidad.

Brinda también un punto de contacto único para reportar desde fuera de la comunidad incidentes que involucren a alguna de las entidades de la misma.

1.6 Otros modelos identificados

Se describen someramente otros modos de organización para equipos de respuesta a incidentes de seguridad.

Vendor Team

Un equipo de estas características es interno a una empresa proveedora de productos y se concentra en las vulnerabilidades de los productos de dicha empresa. Recibe reportes de vulnerabilidades y problemas de seguridad de sus productos, trabaja para repararlos y genera y difunde alertas, recomendaciones y parches relacionados.

Managed Security Service Provider

Es un equipo que provee servicios de seguridad y manejo de incidentes por un pago mensual o por servicio. Puede presentar similitudes con varios de los modelos descritos en las secciones precedentes, pero la comunidad atendida es externa a la empresa del CSIRT.

2 Modelo para CERTuy

El modelo coordinador descrito en los apartados anteriores se ajusta a las características de un CSIRT de alcance nacional, y en particular con la misión y el conjunto de servicios que se están proponiendo para el CERTuy [Certuy06].

En [Kill03] se plantea las siguientes preguntas cuya respuesta afirmativa es una fuerte indicación de que determinado CSIRT responde al modelo coordinador:

- "Your team does not belong to the same organization as your constituency". Como CSIRT nacional, CERTuy va a atender a una comunidad objetivo amplia formada por múltiples entidades externas.
- "Your team coordinates incident response efforts and information exchanges across many different CSIRTs, security teams, and/or other external organizations". El texto preliminar para la Misión de CERTuy incluye a la coordinación como uno de sus ítems principales: "Coordinar las acciones entre los grupos de respuesta a incidentes informáticos (CSIRTs) o centros de cómputo nacionales que se vean afectados por incidentes de seguridad informática, con particular énfasis en aquellos que involucren redes de computadoras, de forma de facilitar una rápida resolución de los mismos".
- "Your main services are to coordinate information exchanges and facilitate discussions

of incident activity. You do not perform on-site incident response.". La canasta de servicios que se fue definiendo en el taller de discusión realizado en el marco del presente convenio no incluye en principio brindar soporte en sitio y, como se muestra a continuación, presenta enormes similitudes con el conjunto de servicios básicos (core services) identificados para el modelo coordinador.

La comparación de la canasta de servicios definidos para CERTuy con los servicios básicos de los diferentes modelos organizacionales se resume en la Tabla 1: Resumen de servicios por modelo organizacional. Puede verse claramente la similitud entre los servicios definidos para CERTuy y los servicios básicos del modelo coordinador.

En particular, los servicios de concientización y capacitación se encuentran como servicio básico solamente en el modelo coordinador y son una componente importante de los servicios definidos para CERTuy.

Un detalle a acotar es que el proceso de discusión en taller, en el cual se definieron los servicios para CERTuy, fue previo, y por lo tanto no fue influenciado, por el presente estudio de los modelos organizacionales.

La comunidad objetivo de CERTuy va a estar formada por una gran diversidad de organizaciones: grandes y pequeñas, públicas y privadas, y con grados muy diferentes de concientización con respecto a la seguridad. Es de esperar, entonces, que se encuentre en dichas organizaciones toda la gama de modelos organizacionales descritos. Sin embargo, y dado que en muchas organizaciones del medio la preocupación por problemas de seguridad es un fenómeno relativamente reciente, se espera que el modelo más frecuente que se va a encontrar al inicio será el Equipo de Seguridad.

Tabla 1: Resumen de servicios por modelo organizacional

	1	2	3	4	5	CERTuy
Alertas y Advertencias	+	√	√	√	√	√
Análisis de Incidentes	√	√	√	√	√	√
Respuesta al incidente en el lugar	√	+	+	+		
Soporte telefónico / e-mail		√	√	√	√	√
Coordinación de respuesta a incidentes	√	√	√	√	√	√
Análisis de vulnerabilidades	+	+	+	+	+	+
Respuesta a vulnerabilidades	√	+		+	+	+
Coordinación de respuesta a vulnerabilidades	+	√	√	√	√	√
Análisis de "Artifacts"	+	+	+	+	+	+
Respuesta a "Artifacts"	√	+		+	+	+
Coordinación de la respuesta a "Artifacts"	+	+	√	√	√	√
Anuncios		√	√	√	√	√
Observatorio tecnológico		+	√	√	√	+
Auditorías o Evaluaciones de Seguridad		+	+	+		+
Configuración y Mantenimiento de Herramientas, ...	√	+	+	+		+
Desarrollo de Herramientas		+	+	+	+	+
Servicios de Detección de Intrusiones	√	+	+	+		+
Difusión de Información Relacionada con Seguridad		+	√	√	√	√
Análisis de Riesgo		+	+	+	+	+
Planif. de cont. del negocio y recup. de desastres		+	+	+	+	+
Consultoría de Seguridad		+	+	+	+	+
Concientización		+	+	+	√	√
Educación/Capacitación		+	+	+	√	√
Evaluación y/o Certificación de Productos		+	+	+	+	+
Otros (Alertas personalizadas, Análisis forense)						√
	√	Servicio básico				
	+	Servicio adicional				
		Servicio rara vez brindado en ese modelo				

3 Referencias y Bibliografía

[Kill02] Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. CSIRT Services List. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002.

[Kill03] G. Killcrece et al, Organizational Models for Computer Security Incident Teams (CSIRTs), Handbook CMU/SEI-2003-HB-001, diciembre 2003.

[Kill03-2] G. Killcrece et al, State of the Practice of Computer Security Incident Response Teams (CSIRTs), Technical report, CMU/SEI-2003-TR-001, ESC-TR-2003-001, octubre 2003.

[West03] West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Handbook for Computer Security Incident Response Teams (CSIRTs) (CMU/SEI-2003-HB-002), 2003.

[Certuy06] Misión, Comunidad Objetivo y Servicios CERTUY (Taller-CERTUY-002), 2006